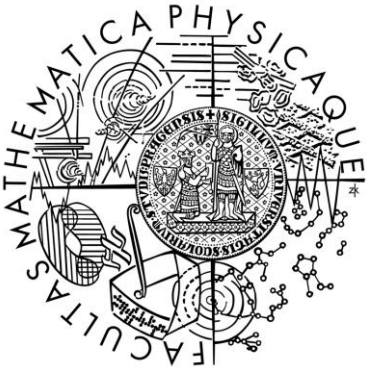
Univerzita Karlova v Praze

Matematicko-fyzikální fakulta

DIPLOMOVÁ PRÁCE



Bc. Petra Fritzová

Bezpečnost elektronického hlasování

Katedra algebry

Vedoucí diplomové práce: Mgr. Pavel Růžička, Ph.D.

Studijní program: Matematika

Studijní obor: Matematické metody informační bezpečnosti

Praha 2013

Na tomto místě bych ráda poděkovala Mgr. Pavlu Růžičkovi, Ph.D., který se mi ochotně věnoval a podnětně připomínkoval moji práci. Samozřejmě bych chtěla také poděkovat osobám z mého blízkého okolí, za podporu a porozumění, které mi během psaní práce projevovali.

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona.

V Praze dne 8. 4. 2013

Název práce: Bezpečnost elektronického hlasování

Autor: Bc. Petra Fritzová

Katedra: Katedra algebry

Vedoucí diplomové práce: Mgr. Pavel Růžička, Ph.D.

Abstrakt: Elektronické volby, také označované jako i-volby by mohly pomoci při odstraňování krize v naší demokracii, která se projevuje nespoluprácí při možnosti vyjadřování svého názoru na přímých volbách. Rozumným nastavením informačních a komunikačních technologií z technického i finančního hlediska by mohlo pomoci tomu, že voleb by se zúčastnilo více voličů. Implementací elektronických voleb by se mohlo docílit toho, aby způsob, jakým se vládne v demokratické republice, byl doopravdy reprezentován názorem valné většiny osob, které jsou v dané republice oprávněny k volbě. Zavedení elektronického volebního systému by se mohlo vyplatit i z finančního hlediska. Také by se mohlo v rámci volebního procesu snížit riziko lidské chyby, ale i riziko manipulace hlasů, protože většina procesů by byla automatizována.

Tato práce navrhuje definici základních požadavků na ideální elektronický volební systém, které porovnává s požadavky pro zaručení bezpečnosti dvou již navržených systémů elektronického hlasování. Díky hlubší analýze těchto dvou systémů se v práci dále popisují jejich nedostatky z hlediska bezpečnosti a nastoluje se možnost základních útoků, z důvodu nedokonalosti zabezpečení, na jednotlivé komponenty a vlastnosti systémů.

Klíčová slova: Bezpečnost, elektronický, hlasování

Title: Security of an Electronic Voting System

Author: Bc. Petra Fritzová

Department: Department of algebra

Supervisor: Mgr. Pavel Růžička, Ph.D.

Abstract: Electronic elections, also known as i-voting might help in removing the crisis in our democracy, which is reflected in non-cooperation in the opportunity of expressing their opinions during direct elections. A reasonable set up of information

and communication technologies in technical and financial terms could help that elections would be attended by more voters. The implementation of electronic elections could achieve that the way of governance in the democratic republic will be truly represented by the view of the vast majority of people who are authorized to elect. The introduction of the i-voting system could be efficient from the financial point of view. This electoral process could reduce the risk of human error as well as the risk of manipulation of votes since most of the processes would be automated.

Thesis proposes a definition of the basic requirements for an ideal i-voting system which compares the requirements for ensuring the safety of two previously proposed electronic electoral systems. Thanks to a deeper analysis of these two systems the thesis also describes the imperfection in safety and it raises the possibility of basic attacks on components and systems properties due to imperfections in security.

Keywords: Security, Electronic, Voting

Obsah

Úvod

Asi největší nevýhodou papírových voleb pro elektorát je lokalitní omezení. Voliči musí brát ohled na umístění a pracovní dobu volebních místností a na časová omezení stanovená pro vykonání volby. Co jim přináší vidina možnosti elektronického hlasování? Jednoznačně komfort, a tedy eliminaci fyzické interakce voliče s volebním systémem. Co ale voliči, kteří nemají potřebné vybavení pro provedení elektronické volby (nemají přístup k Internetu, počítač nebo chytrý telefon) anebo prostě zatím nedůvěřují takovému způsobu? Odpověď je jednoduchá, zavedení elektronických voleb by se mohlo prozatím provádět jako doplněk ke stávající možnosti volby klasickým papírovým způsobem. Jaké jsou další výhody? Z dlouhodobějšího hlediska by se mohly uvažovat finanční úspory; například úspory nákladů na tisk hlasovacích lístků, snížení počtu volebních místností a komisí (na počet privilegovaných osob potřebných pro fungování elektronického volebního systému) a také například prostorů pro uskladňování volebních lístků. Netřeba samozřejmě opomíjet fakt větší technické a procesní náročnosti, které by ale po rozumném navržení a po prvním úspěšném uvedení do provozu, měly být zastíněny finančními úsporami. Další výhodou je snížení náročnosti manipulace s odevzdanými hlasy, zvýšení rychlosti sčítání hlasů (i opakovaného sčítání hlasů) a celkové eliminace chyb lidského faktoru; možné je i snížení rizika manipulace s hlasy. Četnost referend by se dala také pozvednout bez zvýšení finančních nákladů a tím by mohli oprávnění voliči více ovlivňovat dění v republice.

Informační a komunikační technologie se neustále rozvíjí velkými skoky, mladí lidé si tento trend rychle osvojují a v podstatě stále očekávají další novinky. Když se podíváme například na bankovnictví, tak vidíme, jak se v průběhu několika let rozšířily možnosti komunikačních kanálů pro poskytování této služby. Stále se vedou diskuze ohledně bezpečnosti elektronického bankovnictví, ale mnoho lidí se denně přihlašuje do bankovních aplikací pomocí svých počítačů, tabletů nebo chytrých telefonů a mrknutím oka provádí různé finanční transakce. Co ale když se někde nastolí otázka elektronických voleb? Myslím, že většina z nás (možná vyjma mladé generace, která může vidět tento systém jako další skvělý nový trend) je vůči tomuto skeptická. Když opomenu lidi, kterým se to jenom prostě „nezdá“, protože se

například o tom prozatím mluví málo nebo to ještě není implementováno ve všech okolních zemích, tak druhá část lidí se ohání faktem nemožnosti dostatečného zabezpečení elektronických voleb. Tato skupina má v jistém smyslu slova pravdu, protože zabezpečení internetových voleb je složitější než například zabezpečení finančních transakcí prováděných přes Internet. Jednak proto, že v sázce je při volbách asi mnohem víc (než při jednotlivých finančních transakcích), takže si útočníci pravděpodobně najdou více času na uskutečnění takového útoku, nebo že mezi útočníky na elektronické volby budou pravděpodobně velké organizované skupiny, které mají jasný záměr, jako například ovlivnění volebních výsledků. Dalším důvodem by mohlo být to, že chyba při provedení elektronické volby je víceméně nevratná nebo například to, že nemožnost hlasování kvůli zahlcení volby přijímacího serveru může kompromitovat celé volby. To ale neznamená, že je nemožné uvést do provozu bezpečný elektronický volební systém; přece jenom, v Estonsku se to již podařilo.

Když se podíváme na celosvětové trendy v technologiích, je možné, že zavedení procesu elektronických voleb již není otázkou „jestli“, ale „kdy“; i proto je toto téma aktuální.

V první kapitole je připomenuta definice bezpečnosti a jiných techničtějších pojmů, se kterými se bude dále pracovat. Také je vysvětlen princip základních typů útoků, které představují pro elektronický volební systém hrozby a neměly by být při jeho navrhování opomíjeny.

Cílem druhé kapitoly je navržení základních definičních požadavků pro ideální volební systém, jaký by mohl vyhovovat celému elektorátu, protože by jim přinesl výhody, a přitom by mohli být spokojeni, že je dosažena alespoň taková bezpečnost, jaká se očekává od klasických papírových voleb.

Ve třetí kapitole je analyzován volební projekt SERVE z hlediska jeho komponent a jejich provázání, který byl navrhnut, ale v praxi se neuchytil, co již bude zřejmě vidět při popisu jeho architektury (proto se také používá označení projekt a ne volební systém).

Ve čtvrté kapitole je analyzován příklad robustnějšího, již fungujícího a v praxi zavedeného elektronického volebního systému v Estonsku, popis jeho komponent a jejich provázanosti.

Poslední kapitola obsahuje porovnání základních rozdílných vlastností ideálního volebního systému, systému SERVE a volebního systému EstEVS z hlediska bezpečnosti. Na základě těchto porovnání jsou nastíněné základní typy útoků, které tyto architektury svým návrhem umožňují.

1. Technický vstup

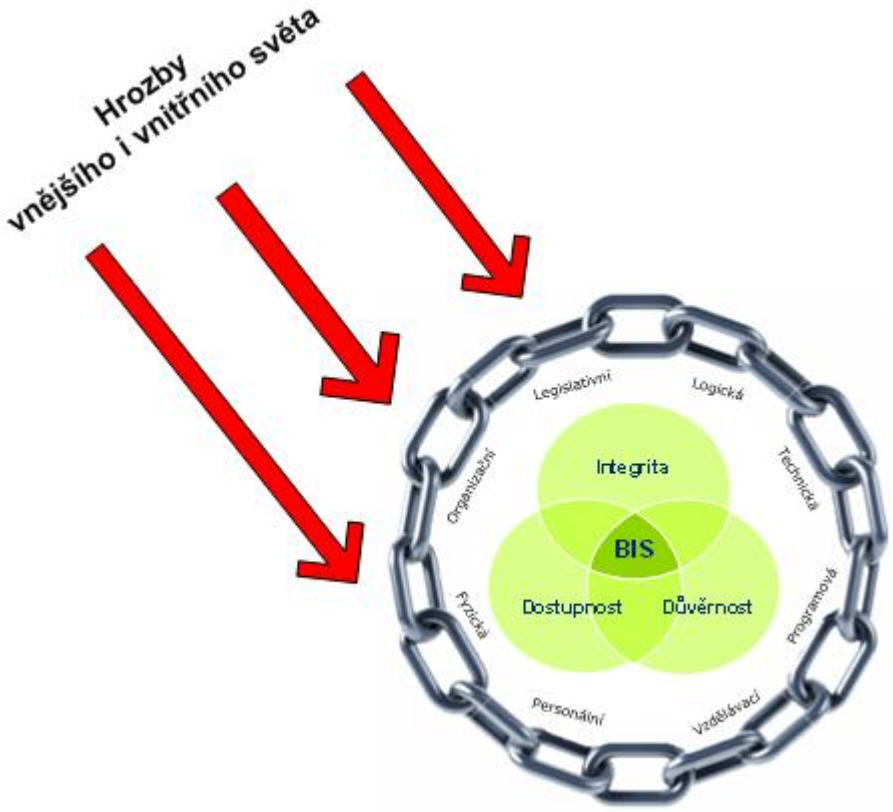
Před tím, než začneme definovat požadavky a vlastnosti pro ideální elektronický volební systém, shrneme technickou terminologii, s kterou budeme dále pracovat.

1.1 Informační bezpečnost

Celá tato práce pojednává o informační bezpečnosti elektronických voleb. Je tím myšleno zabezpečení informačního systému – jeho komponent (software, hardware), služeb, které má poskytovat (ve volebním systému službou může být možnost provedení volby, správné započtení volebního lístku, správné sečtení lístků a podobně) a dat, s nimiž systém pracuje, nebo které jsou v něm uloženy. Bezpečnost je jakýsi souhrn a soulad legislativních, organizačních, logických[1], technických, programových, fyzických, personálních a vzdělávacích opatření[2] namířených na zajištění správného fungování informačního systému, která musí působit proti narušení hlavních atributů bezpečnosti – důvěrnosti, integrity a dostupnosti. Tato zmíněná opatření, hlavní atributy bezpečnosti a hrozby, které ohrožují systém, jsou znázorněny na následujícím obrázku.

[1] Logická bezpečnost se zabývá návrhem a optimalizací systému s cílem dosažení co nejdokonalejšího filtru pro přístup k informacím v rámci tohoto systému – například zabezpečení kontroly přístupů, výběr a spolehlivost programového vybavení a jiné.

[2] Tato opatření jsou blíže popsána v kapitole 0.



Obrázek 1 Bezpečnost informačního systému - BIS

Naplnění těchto zmíněných základních atributů – důvěrnost, integrita a dostupnost – informačního systému nesmí určitě chybět ani v elektronickém volebním systému. Tyto atributy existují nezávisle na sobě a jejich průnik je dosahovanou mírou bezpečnosti informačního systému. Základní popis atributů je následující:

- Důvěrnost – Tento atribut bezpečnosti informačního systému znamená utajení při zpracování, přenosu a uchovávaní dat v systému a prevenci před jejich vyzrazením – aby se neoprávněná osoba nedostala k té části systému (informacím), ke které nemá právo.

  Typy útoků, které narušují důvěrnost, jsou například sledování síťového provozu (odposlech prováděný při komunikaci), odpozorování stisků kláves přes rameno či z dat na obrazovce nebo krádež vytištěných informací. Důvěrnost může být porušena například v případě, že jsou přes Internet poslána nezašifrovaná citlivá data, je vyzrazeno obchodní tajemství nebo jsou opomenuta potřebná zvláštní opatření při zpracování citlivých dat (například,

že citlivá data jsou uložena v takové části systému, ke které mají přístup i jiní uživatelé systému, než ti, kteří jsou k přístupu k takovým datům oprávněni).

Důvěrnost může být zajištěna například správným řízením přístupů k datům (přesné definování toho, kdo má přístup, k čemu má přístup – konkrétně k jakým souborům, datům, a jaký má přístup – čtení, editace, spuštění souboru a podobně; jakým způsobem je prováděna autentizace a jiné) nebo šifrováním při ukládání dat a při jejich přenosu (šifrování – tedy utajování smyslu dat převodem do podoby, která je čitelná jen s jistou znalostí – detailněji popsáno níže v kapitole 1.3.1).

- Integrita – Znamená to přesnost, celistvost a spolehlivost dat se zaručeným obsahem, prevence před jejich nežádanou modifikací. Bezpečný systém musí pracovat tak, aby byla data uchovávána a zpracovávána správně a přesně, přenášena bez nechtěných změn a aby falešná data, která útočník uloží do systému nebo pošle po síti, byla odhalena.

  Uživatelé mohou narušit integritu vlastní chtěnou nebo nechtěnou chybou, a to například editací důležitých souborů (což může být způsobeno nedostatečným vyškolením oprávněných osob nebo například nesprávným přidělením přístupových oprávnění – někdo, kdo neměl mít přístup pro editaci těchto souborů, jej měl), špatným zadáním dat do systému nebo nesprávným nastavením datových toků mezi databází a aplikací (data jsou při přenosu pozměněna nebo smazána). Malware je dalším způsobem pro narušení integrity - škodlivý kód způsobí změnu dat uložených v systému nebo vloží falešná data do systému (například do databáze nebo na souborový server) nebo způsobí změnu dat posílaných po síti (v průběhu komunikace). V některých případech se pozměnění dat projeví ihned, ale některé případy je téměř nemožné detekovat.

  Integritu některých přenášených dat lze zabezpečit například pomocí elektronického podpisu (podpisu dat v elektronické podobě; přesněji vysvětleno v kapitole 1.3.2). Narušení integrity ukládaných dat lze předejít správným nastavením zálohování a obnovy systému nebo například správným řízením přístupů k uloženým datům.

- Dostupnost – Spolehlivá dostupnost dat, systémů a jejich služeb (například provádění autentizace a autorizace uživatele a přijetí volebního lístku do systému) znamená přístupnost těm uživatelům, kteří na to mají právo, ale dostupností je také myšlena prevence před vyřazením informačního systému z provozu.

  Dostupnost dat může být ohrožena různými útoky na zahlcení serverů nebo komunikačních sítí, nedostupnost internetových stránek, na selhání operačního systému nebo například zničení hardware.

  Narušení dostupnosti může nastat, když útočník znepřístupní data – změní přístupová práva k souboru, ve kterém jsou data uložena, a soubor se stane nedostupným, nebo útočník data zašifruje tak, že uživatel není schopný je dešifrovat, nebo útočník zničí hardware, ze kterého již uložené informace nebude možné přečíst.

  Systémy a sítě, pomocí kterých tyto systémy komunikují, musí mít datovou kapacitu dimenzovanou tak, aby v určeném čase poskytovaly dostatečný výkon. Také musí být schopny rychlého zotavení se z výpadků tak, aby jejich produktivita byla ohrožena co nejméně. Přístup k datům je umožněn pomocí aplikací a databází, které běží na daném operačním systému a příslušném hardware. Dostupnost těchto dat může být zajištěna například rezervními zdroji, ale i robustností software a operačního systému, využitím replikací ve virtuálních prostředích[3] nebo například zvýšenou kapacitou sítě, pomocí které tento systém komunikuje. Také se pro dosažení dostupnosti používají IDS/IPS systémy (Intrussion Detection/Prevention system), které slouží na detekování útoků (IDP), například pomocí analýzy síťového provozu, a zastavení těchto útoků (IPS).

Jak již bylo zmíněno v popisu jednotlivých hlavních atributů bezpečnosti, s těmito atributy úzce souvisí řízení přístupu. Popis základních kroků pro přidělení přístupu je následující:

[3] Virtuální prostředí znamená několik jednotlivých pracovních prostředí na jediném počítači (serveru), kde na každém prostředí běží nezávislý operační systém

- Identifikace uživatele informačního systému – Identifikace je prvním krokem, kterým musí subjekt projít v procesu přidělování přístupu. Identitu udává každý uživatel sám za sebe. Je to tedy jeho tvrzení o své totožnosti, skupinové příslušnosti nebo schopnosti.

- Autentizace uživatele – Verifikační proces ověřující předloženou identifikaci uživatele, zajišťující ochranu před falšováním identity.

  Existují různé autentizační metody. Mohou být založené buď na něčem, co daný uživatel zná (PIN kód nebo heslo), něčem co daný uživatel vlastní (např. identifikační karta), nebo něčem čím daný uživatel je (jeho jednoznačná charakteristika, jako například otisk prstu). Na základě kombinace různých faktorů („zná“, „vlastní“, „je“) rozlišujeme autentizaci jednofaktorovou, dvoufaktorovou, nebo třífaktorovou [2]. Je zřejmé, že čím více faktorů použijeme, tím bude pro útočníka obtížnější zfalšovat identitu nějakého uživatele (při vícefaktorové autentizaci by nestačilo například uhodnout nebo získat jeho uživatelské jméno a heslo, ale potřeboval by jeho identifikační kartu nebo i jeho otisk prstu).

- Autorizace uživatele – Přiřazení oprávnění pro konkrétního uživatele pro konkrétní činnost po provedení úspěšné autentizace.

  Každý uživatel systému by měl mít správně nastavena přístupová práva, která mu budou při autorizaci přidělena. Tedy se mu zpřístupní taková část systému a taková data, které odpovídají jeho oprávněním. Ve volebním systému tomu není jinak. Jak volič, tak tzv. „privilegovaná osoba“ (osoba s právem administrovat nějakou část volebního systému – ne všechny privilegované osoby mají stejná práva v systému) musí projít procesem autorizace, kde jsou každému přidělena oprávnění, jaká mu náleží.

1.2 Hrozba, zranitelnost, riziko

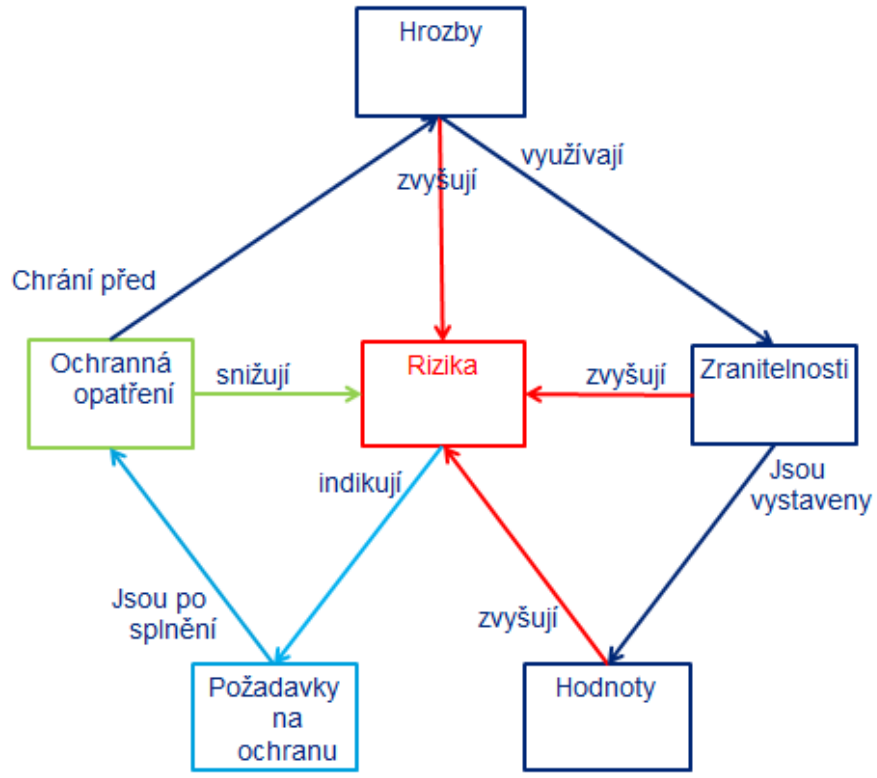
V dalších kapitolách budeme používat terminologii ohledně pojmů hrozba, zranitelnost a riziko. Tyto pojmy úzce souvisí z bezpečnosti informačních systémů, proto je jejich vysvětlení věnována tato část práce.

V rámci informačního systému, který chceme chránit, je nejprve potřeba identifikovat vše, co má pro daný systém nějakou hodnotu a mělo by být adekvátním způsobem chráněno (například který hardware, software, které služby a data) [3]. Důležitá je také identifikace hrozeb, kterým je informační systém vystaven. Dále je potřeba identifikovat slabiny systému (zranitelnosti) a určit, s jakou pravděpodobností může hrozba využít nějakou slabinu (pravděpodobnost vzniku hrozby se často určuje z toho, jestli a kolikrát již daná hrozba nastala) a jaký dopad by to mohlo mít (tedy důsledek nežádoucího incidentu; v praxi se určí vhodná škála, například od 1 do 5 a jednotlivým hrozbám se přiradí číslo, reprezentující míru dopadu vzniku této hrozby oproti ostatním hrozbám). Riziko (4, s. 90-100) je potenciální možnost, že daná hrozba využije zranitelnost a bude to mít nějaký dopad – může být vypočítáno například jako součin pravděpodobnosti vzniku hrozby a velkosti dopadu.

Hrozba je potenciální příčina nežádoucího incidentu, který může mít za následek poškození systému (např. narušení integrity, důvěrnosti či dostupnosti). Hrozby lze kategorizovat jako lidské hrozby (úmyslné – například odposlech, krádež, útok na systém; nebo náhodné – chyby, fyzické nehody) a hrozby prostředí (zemětřesení, povodeň, požár).

Ochranná opatření jsou postupy, které mohou poskytnout ochranu před hrozbou, snížit zranitelnost, omezit dopad nežádoucího incidentu, nebo je také například detekovat.

Následující obrázek znázorňuje vzájemnou provázanost výše zmíněných pojmů.



Obrázek 2 Hrozba, zranitelnost, riziko

1.3 Bezpečnostní mechanismy

Již jsme si uvedli, co je to informační bezpečnost a jaké má cíle, tedy co chce osoba odpovědná za bezpečnost informačního systému chránit. Při popisu ideálního elektronického volebního systému, volebního systému v Estonsku a volebního systému SERVE se budou používat pojmy, jako jsou šifrování, hašování, certifikát a jiné. Proto zde uvedeme popis těchto vybraných mechanismů [5], aby se s nimi mohlo dále pracovat.

1.3.1 Šifrování

Pro zajištění některých atributů informační bezpečnosti se používá kromě jiného šifrování dat. Uvedeme zde příklad způsobů, jak lze data šifrovat.

Šifra je kryptografický algoritmus, který (pomocí klíče) převádí čitelnou zprávu (otevřený text) na její nečitelnou podobu neboli šifrový text.

Klíč je informace, která se používá pro šifrování a následné dešifrování (v symetrické kryptografii se používá ten samý klíč[4] pro šifrování i pro dešifrování – zůstává v tajnosti; v asymetrické kryptografii se používá dvojice klíčů – jeden pro šifrování – veřejný neutajovaný klíč, a jiný pro dešifrování – tajný soukromý klíč, který je také nazýván privátní klíč). Z technického hlediska je klíč bitová sekvence určité délky (udávané v bitech). Kerckhoffsův princip říká, že bezpečnost šifrovacího systému nesmí záviset na utajení algoritmu, ale pouze na utajení klíče (proto by se mělo v elektronickém volebním systému myslet na utajení klíče, kterým budou elektronické volební lístky šifrovány).

Délka šifrovacího klíče zpravidla určuje "sílu" šifrovacího algoritmu, tj. odolnost proti prolomení šifry (např. klíč o délce pět bitů představuje $2^5 = 32$ různých kombinací pro klíče – prostor klíče).

Cílem návrhu šifrovacího algoritmu je to, aby se bez klíče dal tento algoritmus prolomit tak těžko, jak těžko je zhruba zjistit klíč prohledáváním celého prostoru klíče.

Následuje popis základních kryptografických schémat, která se využívají pro šifrování a hašování dat.

1.3.1.1 Symetrická kryptografie s tajným klíčem

Po vytvoření klíče se musí udržovat dvě kopie tohoto tajemství (tedy sdílení klíče oběma komunikujícími stranami), protože ten samý klíč se používá pro šifrování i dešifrování. Zásadní je ochrana tohoto klíče, což může být problém při jeho distribuci na druhý konec komunikačního kanálu z důvodu možného odchycení tohoto klíče třetí stranou (útočníkem). Útočník by po získání tohoto klíče mohl po odchycení zasílaných dat, která jsou tímto klíčem zašifrována, je číst i měnit bez toho, aby si toho komunikující strany povšimly.

Použití symetrické kryptografie představuje menší výpočetní náročnost, a tedy vyšší výpočetní rychlost ve srovnání s asymetrickou kryptografií (viz kapitola 1.3.1.2).

[4] Někdy se odvodí jeden klíč z druhého.

Nejznámější algoritmy symetrické kryptografie jsou DES (Data Encryption Standard – tato šifra již byla prolomena a není považována za bezpečnou), Triple DES, AES (Advanced Encryption standard – nástupce šifry DES).

1.3.1.2 Asymetrická kryptografie

V procesu asymetrické kryptografie je zásadní vytvoření páru klíčů: veřejný klíč pro šifrování a soukromý klíč pro dešifrování. Asymetrická kryptografie je také nazývaná „kryptografie s veřejným klíčem“ – šifrovací klíč může být zveřejněn, aniž by byla porušena bezpečnost zprávy nebo dešifrovacího klíče. Důležitá je ale ochrana soukromého klíče. Kdyby měl někdo další přístup k soukromému klíči, mohl by dešifrovat zprávy zašifrované odpovídajícím veřejným klíčem, ale také při jeho ztrátě například není možné data, jež byla jednou zašifrovaná odpovídajícím veřejným klíčem, dešifrovat. Komunikující strana, která vytvořila tento pár, distribuuje veřejný klíč (nebo jej uloží na dostupném místě), který může protější strana použít pro zašifrování dat. Takto zašifrovaná data lze dešifrovat pouze daným soukromým klíčem (tedy může si je dešifrovat jen ta komunikující strana, která tento pár klíčů vytvořila – oproti symetrické kryptografii zde není potřebné sdílení tajného klíče, což je pozitivní vlastnost z bezpečnostního hlediska – útočník má menší šanci na zjištění tohoto klíče, když je uložen v systému, než když se posílá po počítačové síti).

Druhým využitím asymetrické kryptografie je podepisování dat. Data se podepisují soukromým klíčem, ověření podpisu je možné odpovídajícím veřejným klíčem.

Co když například útočník podstrčí svůj veřejný klíč a uživatel, který chce poslat nějaká zašifrovaná data, použije namísto veřejného klíče příjemce, veřejný klíč útočníka? Příjemce si zašifrovaná data nebude moci přečíst, ale když tato data zachytí útočník, bude je moci dešifrovat. Blíže se tomuto typu útoku a příkladem jeho řešení budeme zabývat v kapitole 1.3.2.

Tento způsob kryptografie ale představuje znační výpočetní náročnost – až 1000 krát nižší výpočetní rychlost než u symetrické kryptografie.

Nejznámější asymetrické kryptografické algoritmy jsou RSA, ElGamal, kryptografie nad eliptickými křivkami.

1.3.1.3 Hybridní schéma

V praxi se často používá tzv. hybridní schéma, které v sobě slučuje rychlost symetrické kryptografie a bezpečnost asymetrické kryptografie. Při použití tohoto typu kryptografie se náhodně vygeneruje klíč pro symetrickou šifru. Tímto klíčem se zašifrují data, která je potřeba ochránit. Následně se zašifruje tento klíč asymetricky – tedy veřejným klíčem příjemce. Tento zašifrovaný klíč a zašifrovaná data se spolu odešlou příjemci. Ten si pomocí asymetrické šifry (pomocí svého privátního klíče) klíč dešifruje a pak pomocí něj dešifruje i samotná data.

Pomocí pomalé asymetrické šifry se tak šifruje pouze krátký klíč, zatímco samotná data, která mohou být velmi dlouhá, jsou šifrována rychlou symetrickou šifrou.

1.3.1.4 Jednocestné hašovací funkce

Hašovací funkce [6] je taková, že vstupní bitovou sekvenci převede na výstupní sekvenci, která je relativně krátká vůči délce vstupu; výstupem je takzvaný haš (také nazývaný otisk). Délka haše je fixní a je určena typem hašovací funkce. U hašovacích funkcí MD5/SHA-1/SHA-256/SHA-512 má výsledný haš délku 128/160/256/512 bitů (MD5 by se již neměla používat [7], neboť je od roku 2004 prolomena – byl nalezen takový algoritmus a použita taková výpočetní síla, že bylo umožněno najít kolizi v reálném čase). Ideální hašovací funkce je charakterizována jednosměrností (one-way) a bezkolizností (collission-free); jednotlivé hašovací funkce se snaží těchto vlastnosti dosahovat, což se daří jen do určité míry.

Jednosměrnost znamená, že ze vstupní hodnoty M lze jednoduše vypočítat $f(M)$, ale z dané hodnoty haše $f(M)$, je výpočetně nezvládnutelné najít původní hodnotu M (výpočetně nezvládnutelné znamená, že i když bychom věděli jak to vypočíst, nezvládli bychom to udělat v reálném čase).

Bezkoliznost (odolnost vůči kolizi) je druhá vlastnost, kterou chceme, aby měla dobrá hašovací funkce. Požaduje, aby bylo výpočetně nezvládnutelné nalezení takových dvou různých hodnot M, M', že by platilo $f(M)=f(M')$. Této vlastnosti se říká také bezkoliznost prvního řádu. Bezkoliznost druhého řádu (odolnost vůči nalezení druhého vzoru) požaduje, aby pro daný náhodný vzor M bylo výpočetně nezvládnutelné nalezení druhého vzoru M' (M' je různé od M), že $f(M)=f(M')$.

Je potřebné si uvědomit, že kolize existují už jenom z toho pohledu, že existuje mnoho různých zpráv ($1 + 2^1 + ... + 2^D = 2^{D+1} - 1$) pro maximální délku zprávy D.

Naproti tomu, existuje jenom málo možných výsledných hašů (u MD5 je různých hašů pouze 2^{128}). Existují tedy kolize, kterých je v tomto případě přibližně 2^{D-127}. Bezkoliznost ale hovoří o nereálnosti nalezení těchto kolizí v čase.

1.3.2 Elektronický podpis

Elektronický (digitální) podpis je aplikací asymetrické kryptografie. Nejprve je vypočten otisk dokumentu (kapitola 1.3.1.4). Tento otisk je poté podepsán autorovým soukromým klíčem (kapitola 1.3.1.2), čímž vznikne elektronický podpis (všimneme si rozdílu, že se podepisuje soukromým klíčem odesílatele, kdežto při šifrování se používá veřejný klíč příjemce).

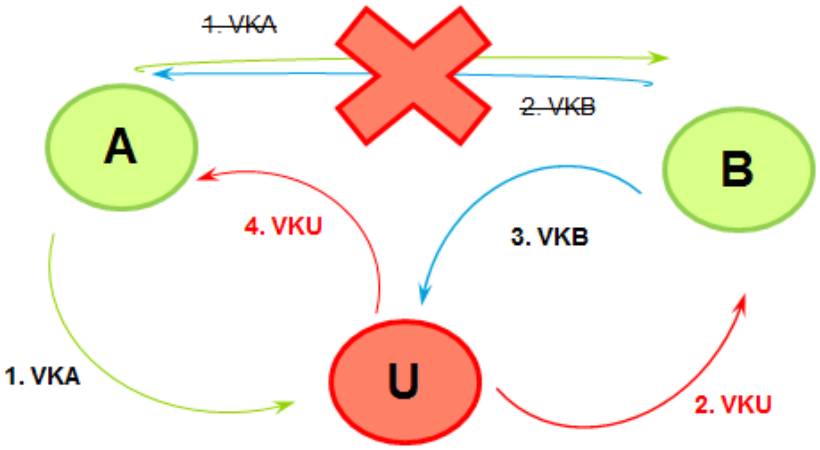
Je to způsob, kterým je možno zajistit autenticitu zprávy, tzn., že příjemce s určitostí ví, kdo je autorem dokumentu (podobně jako při klasickém podpisu papírového dokumentu) a integritu zprávy, tzn., že příjemce s určitostí ví, že obsah podepsané zprávy nebyl následně po jeho podpisu změněn.

Elektronický podpis lze uplatnit na elektronickém dokumentu. Z technického pohledu představuje elektronický podpis blok bytů určité délky, která je závislá na typu použitého hašovacího algoritmu.

1.3.3 Certifikát

Představme si, že spolu chtějí komunikovat strany A a B. Navážou spojení, sdělí si navzájem své veřejné klíče a potom si posílají zašifrované zprávy. Strana A šifruje zprávu veřejným klíčem strany B, ta si jej může dešifrovat svým privátním klíčem a naopak.

Představme si teď ale útočníka U, který má možnost vstoupit do jejich komunikace už při navazování spojení tak, že A i B jsou přesvědčeni, že hovoří spolu - ve skutečnosti ale komunikují prostřednictvím útočníka U.



Obrázek 3 Útočník uprostřed komunikace

Útočník má za cíl odchytit veřejné klíče A i B a nahradit je svým vlastním, aniž to A nebo B zjistí. To znamená, že (krok č.1) strana A pošle svůj veřejný klíč (VKA) straně B, v procesu posílání ale tento veřejný klíč odchytí útočník a ponechá si ho. Namísto něj pošle straně B (krok č.2) svůj veřejný klíč (VKU) a naopak (krok č.3 - strana B pošle straně A svůj VKB, ten je odchycen stranou U; krok č.4 – strana U pošle svůj klíč VKU straně A – strana A ho příjme v domnění, že přijala klíč VKB).

Strana A chce následně něco zašifrovat tak, aby to mohla přečíst jenom strana B, proto použije veřejný klíč od strany B (neví, a nemá se dozvědět, že tento klíč je z dvojice asymetrických klíčů od strany U), takže použije vlastně veřejný klíč strany U – zašifruje data a pošle je straně B. Tato data ale po cestě odchytí strana U, dešifruje je svým privátním klíčem (původní data pak může například pozměnit), zašifruje je veřejným klíčem strany B a pošle je dále straně B, ta si jej dešifruje pomocí svého privátního klíče a netuší, že tato data nepocházejí od strany A, ale od útočníka. Tento druh útoku se nazývá man in the middle – MITM (více viz kapitola 1.4.2).

Na stejný problém se naráží i při podepisovaní zpráv. Strana A pošle svůj veřejný klíč straně B, ten odchytí útočník U, a pošle straně B svůj veřejný klíč (nebo ho strana A na Internetu zveřejní – útočník nahradí veřejný klíč strany A svým veřejným klíčem – jako vlastník zůstane uveřejněna strana A). Strana A podepíše zprávu, pošle ji straně B, ale tuto podepsanou zprávu odchytí strana U (může ji například pozměnit), podepíše svým privátním klíčem a pošle straně B. Strana B

přijala od strany U její veřejný klíč, ale myslí si, že patří straně A. Ověření podpisu pomocí veřejného klíče strany U bude úspěšné, takže strana B si bude myslet, že přijatou zprávu podepsala strana A.

Problém je v tom, že strana A ani B nemají možnost, jak ověřit pravost zveřejněných veřejných klíčů. I proto se používají certifikáty.

Certifikát veřejného klíče je jakýsi elektronický průkaz (jistá datová struktura - nejrozšířenější je struktura certifikátu dle normy X.509[5]), který zaručuje vazbu subjektu a jí příslušejícího veřejného klíče (že se nejedná o falsifikát) – je to veřejný klíč spolu s informacemi o jeho majiteli. Tato datová struktura je elektronicky podepsána vydávající certifikační autoritou, jejíž veřejný klíč je dostupný (z bezpečných zdrojů).

Certifikační autorita (CA) vystupuje při komunikaci dvou subjektů jako třetí nezávislý důvěryhodný objekt, který vydává certifikáty. CA zaručuje, že deklarovaný veřejný klíč přísluší danému subjektu a potvrzuje planost vydaného certifikátu. Certifikační autorita je jedním ze způsobů, jak zajišťovat a řídit infrastrukturu veřejných klíčů PKI[6].

Certifikáty jsou obvykle vydávány na dobu určitou, tzn., že jejich platnost je omezena. Certifikát může ztratit svou platnost buď tak, že jeho nastavená platnost vyprší, nebo je zneplatněn, přičemž zneplatněn může být na základě žádosti vlastníka (myslí se vlastník privátního klíče, kterému náleží veřejný klíč – certifikát veřejného klíče) nebo na popud CA, která jej vydala.

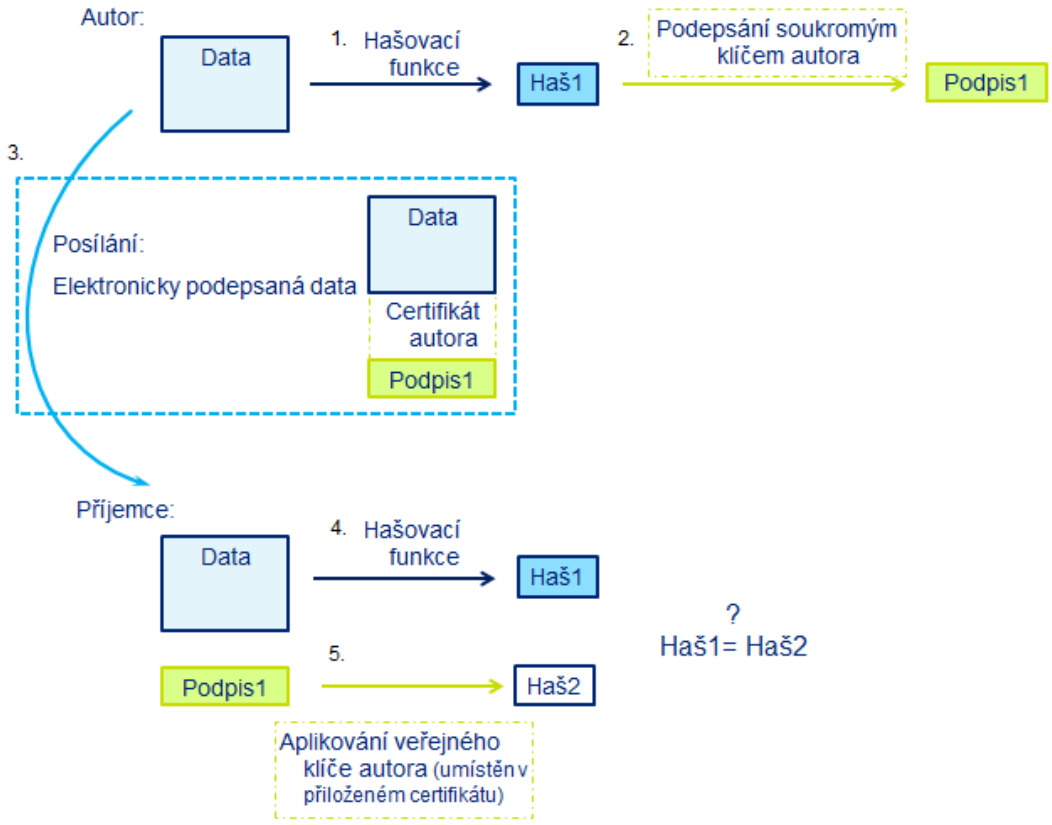
Ke zneplatnění na žádost vlastníka dochází v okamžiku, kdy došlo např. k prozrazení, nebo zcizení privátního klíče a hrozí tedy zneužití identity, nebo při změně údajů souvisejících s certifikátem. CA může certifikát zneplatnit v okamžiku, kdy ze strany vlastníka dojde k porušení certifikační politiky CA (např. jeho

[5] X.509 je standard pro systémy založené na PKI. Specifikuje mezi jiným formát certifikátů, seznamů zneplatněných certifikátů, parametry certifikátů a metody kontroly platností certifikátů.

[6] PKI (Public Key Infrastructure) je v asymetrické kryptografii označení infrastruktury správy veřejných klíčů. Pomocí veřejného klíče v podpisovém certifikátu lze ověřovat elektronický podpis vlastníka privátního klíče. Pomocí veřejného klíče v šifrovacím certifikátu lze šifrovat zprávu pro vlastníka privátního klíče.

nedovolené použití), při chybě způsobené CA. Zneplatněné certifikáty CA uveřejňuje v tzv. seznamu zneplatněných certifikátů – CRL (Certificate Revocation List), který je veřejně dostupný.

Pomocí obrázku 4 popíšeme, jak se certifikát používá a následně, jak se pomocí certifikátu ověří autenticita a integrita dat. Z kapitoly o elektronickém podpisu 1.3.2 již víme, jak se provádí elektronický podpis – vezmou se data jako vstup do hašovací funkce (krok 1), pak se výsledný haš podepíše (krok 2). Když pak uživatel pošle data s jejich elektronickým podpisem a příslušným certifikátem veřejného klíče (krok 3), tak příjemce po přijetí této struktury má možnost následujícího ověření. Vezme veřejný klíč z certifikátu a aplikuje jej na podpis, dostane tak haš – označme jej *Haš1* (krok 4). Na přijatá data použije stejnou hašovací funkci, jako použil odesílatel a dostane haš – *Haš2* (krok 5). Integrita dat nebyla při přenosu porušena, pokud platí, že *Haš1* = *Haš2*. A když je certifikát podepsán důvěryhodnou certifikační autoritou, tak máme i ověření autenticity.



Obrázek 4 Certifikát – elektronický podpis

1.4 Bezpečnostní hrozby

Tato kapitola uvádí příklad základních hrozeb a metod útoků, které by se daly využít proti elektronickému volebnímu systému, a předchází opisu jednotlivých systémů, pro dopředné pochopení hlavních myšlenek těchto útoků. Další kapitoly (hlavně kapitola 5) se na tyto útoky a hrozby odkazují a většinou je aplikují na jednotlivé zranitelnosti ve fungování volebních systémů.

1.4.1 Malware

Malware je hrozba, která se snaží využít různých zranitelných míst v rámci informačních systémů. Název této hrozby vznikl složením anglických slov „malicious“ (zákeřný) a „software“, což poukazuje na škodlivou činnost tohoto programu. S rozšířením Internetu vzniklo velké množství škodlivého softwaru tohoto druhu. Některé jsou vytvářeny se záměrem pouze obtěžovat uživatele, jiné jsou vyvinuty například pro zničení souborů na pevném disku, zapsání chybných dat do souborového systému (s cílem jeho poškození), dále k mazání, editaci či odposlouchávání dat, zobrazování nevyžádaných reklam, ovládání počítačů pro odesílání spamu nebo provádění DoS útoků (viz kapitola 1.4.3). Rozlišujeme několik druhů malware – základní rozdíly jsou například v různosti cílů útoků a způsobu šíření:

Počítačový vir

Je to kód, který je neschopný „samostatného života“, parazituje na jiných programech a dále se z nich (bez vědomí uživatele) šíří – autoreplikuje – vytváří ty samé nebo poupravené kopie sebe sama. Tyto hostitelské soubory se využívají pro rozšiřování virů přenosem po síti nebo pomocí fyzického média, tedy pro jejich šíření je potřebná jistá, obvykle neúmyslná, kooperace uživatele.

Podle toho, čeho chce autor viru docílit, tak napadené objekty pak například buď nefungují vůbec, fungují omezeně (například kvůli tomu, že virus svou reprodukcí zatěžuje systém) nebo například fungovat vůbec nepřestanou (aby se předešlo odhalení nákazy virem), ale virus přitom provádí nějakou skrytou zákeřnou

činnost. Dále může dojít například k blokování operačního systému, k editaci, či mazání dat na disku, provádění neautorizovaných změn v systému nebo k jiné činnosti, která je cílem počítačového viru. U některých virů se spustí jejich ničivý kód se zpožděním - například v určitý stanovený termín.

Jeden ze způsobů nákazy tímto malware je, že uživatel navštíví stránku na Internetu (odkaz na tuto stránku může uživateli přijít na e-mail, což může být přímo mířeno jako útok, nebo uživatel najde odkaz na jiné internetové stránce) a na pozadí se začne stahovat do počítače nějaký program, který obsahuje malware. Dalším způsobem pro nakažení počítače je například, když uživatel klikne na podvrženou chybovou zprávu nebo vyskakovací okno a spustí se tím stahování nějakého programu, který může být nakažen tímto malware.

Trojský kůň

Je jednoduchý program nebo aplikace – nebo jejich část, předstírající užitečnost, jako například počítačová hra, instalační soubor. Po spuštění často vykonává „legitimní“ funkci (jaká se od daného souboru očekává), v příhodný okamžik však vykoná nějakou škodlivou činnost – například destrukční (smaže soubory na disku), nebo prolomí nějaký zabezpečovací mechanismus, monitoruje stisky kláves (například pro odposlech hesla nebo čísel kreditních karet), umožní útočníkovi získání vzdálené kontroly nad počítačem (s cílem například vykonání DoS útoku – více v kapitole 1.4.3), umožní obejití standardního autentizačního mechanizmu, takže poskytuje jakýsi nestandardní vstup do systému – například obejití firewallu[7] (tento typ se nazývá backdoor – „zadní vrátka“ – a po spuštění může umožnit proniknutí viru do systému, zpřístupnění dat nebo například získání přístupu pro útočníka do systému). Další formou trojského koně může být spyware, který zasílá na určitou adresu citlivé informace o uživateli systému bez jeho vědomí - například osobní informace, informace o nainstalovaných programech, o navštívených internetových stránkách, o zaslaných e-mailech, přístupových heslech, číslech kreditních karet.

[7] Firewall je síťové zařízení/konfigurovatelný program, kterého nastavení určuje stupeň restrikcí, jež jsou uplatňovány na procházejících datových paketech. Je bariérou, která chrání síť před neoprávněnými přístupy a vlivy z vnějšího prostředí a také před vysíláním nežádoucích dat směrem ven. Musí ale umožňovat spolehlivý přenos povolených dat oběma směry.

Trojský kůň se nesnaží o replikaci. V Microsoft Windows využívá tento malware toho, že mnoho programů skrývá přípony souborů, takže uživatel v domnění, že otevře fotku nebo hru, spustí tento ukrytý kód.

Počítačový červ

Je to škodlivý kód – samostatný spustitelný program, který je schopen automatického rozesílání sebe sama na jiné počítače (nevyžaduje od uživatele zásah, aby se mohl rozšířit – na rozdíl od viru) a který se nesnaží vydávat za něco jiného (na rozdíl od trojského koně). Klasický červ využívá ke svému šíření počítačové sítě – vyhledává další počítače v síti a přenáší na ně své kopie (počítačový virus si existenci sítě neuvědomuje a k šíření používá soubory na daném počítači).

Kromě autoreplikace, vykonává tento malware v počítači i sekundární činnost, která je v případě červa označovaná jako „náklad“ („payload“). Touto škodlivou činností může například být vyřadění počítače z provozu, zapisování do registrů Windows a změna v něm uložených důležitých dat (nastavení), mazání souborů v počítači, získávání osobních dat, která jsou v počítači uložena, omezování kapacity počítačové sítě a jiné. V poslední době nejčastější varianta červa je taková, že antivirový program napadení počítače detekuje, ale neumí provést léčení.

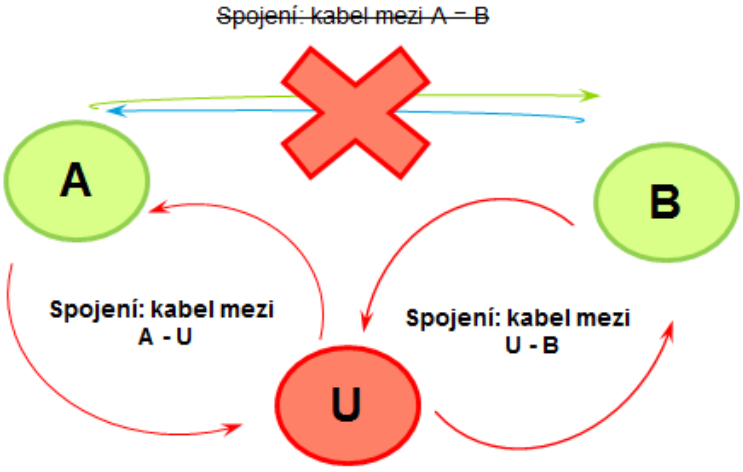
Když se malware dostane na počítač, může z něj vytvořit bot. Toto označení znamená, že daný počítač je donucen vykonávat příkazy útočníka přes Internet bez vědomí uživatele počítače. Útočníci typicky vytváří boty z více počítačů, čímž vzniká síť zvaná botnet. Botnet se může využít pro rozesílání nežádoucích e-mailových zpráv, šíření virů, může systém zpomalit nebo jej lze zneužít pro vykonání DoS útoku (blíže popsán v kapitole 1.4.3).

1.4.2 MITM útok

Útok MITM (Man in the middle) patří mezi nejznámější úmyslné hrozby v rámci informačních systémů. Jeho podstatou je snaha útočníka přesměrovat přenos dat mezi (současnými nebo budoucími) účastníky daného spojení tak, aby tato data procházela přes něj. Existuje mnoho způsobů, jak je možné provést takový útok –

aby útočník mohl odposlouchávat komunikaci (nebo ji dokonce měnit; ne pozdržovat) bez toho, aby to komunikující účastníci registrovali (kdyby útočník odposlouchávaná, případně pozměněná data neposílal dál, šlo by o DoS útok, protože by byla komunikujícím stranám odepřena služba přenosu dat – více viz kapitola 1.4.3).

Uvažme jednoduchou lokální síť (viz obrázek 5) se třemi počítači: A, B (oběti) a U (útočník), kde počítač A je spojen síťovým kabelem s počítačem B. Kdyby útočník U chtěl odposlouchávat komunikaci mezi A a B, mohl by rozpojit kabel spojující A a B a zapojil by jeden kabel mezi A a sebou, a druhý kabel mezi sebou a B. I toto je jeden z možných (i když zjednodušených) příkladů, jak je možné provést MITM útok.



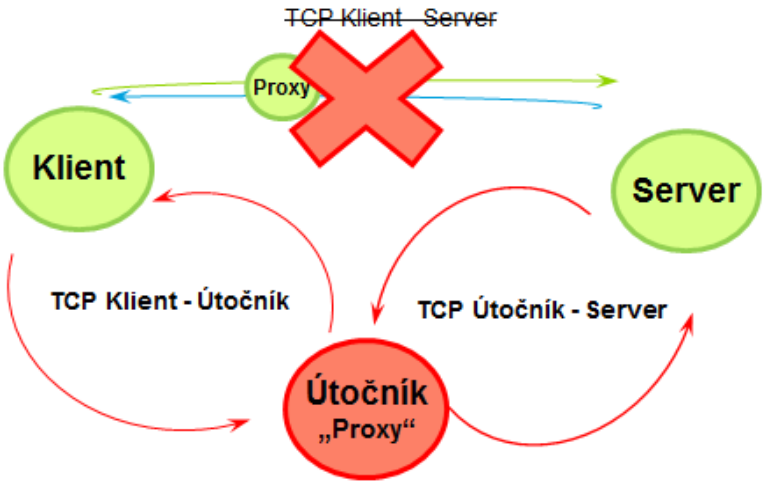
Obrázek 5 MITM – Kabel

Vezměme si jiný příklad. Klient (počítač A) a server (počítač B) chtějí spolu komunikovat klasicky přes HTTP[8] protokol. Cílem útočníka je dostat se do TCP[9] spojení zprostředkovávající tuto HTTP komunikaci mezi klientem a serverem. Pomocí různých technik útočník rozdělí původní zamýšlené TCP spojení (mezi klientem a serverem) na dvě nová spojení – jedno mezi klientem a útočníkem, druhé

[8] HTTP (Hypertext transfer Protocol) je protokol aplikační vrstvy pro přenos webových stránek.

[9] TCP (Transmission control protocol) je protokol transportní vrstvy, který navazuje spojení mezi klientem a serverem. Garantuje spolehlivé doručování a zachovává pořadí paketů (bloků dat).

mezi útočníkem a serverem. Jakmile je TCP spojení navázáno, útočník vystupuje v roli proxy[10] serveru – je schopen číst a měnit data v zachycené komunikaci.



Obrázek 6 MITM – HTTP

Je jasné, co je v tomto případě špatně - komunikující strany si nemohou ověřit navzájem svou identitu a data jsou posílaná v nezašifrované podobě. Pro řešení tohoto problému se aplikuje použití protokolů SSL (Secure Socket Layer, tzv. vrstva bezpečných soketů) a jeho nástupce TLS (Transport Layer Security) – mezi protokoly SSL 3.0 a TLS 1.0 jsou jenom drobné rozdíly. Tyto protokoly poskytují zabezpečení komunikace proti odposlouchávání či nechtěné změně dat v průběhu komunikace šifrováním dat, která se přenáší, a autentizací komunikujících stran. Komunikace má pak tři základní fáze – dohoda komunikujících stran na podporovaných algoritmech (které se budou dále používat), výměna klíčů (šifrování veřejným klíčem přijímatele; autentizace za pomocí certifikátů) a šifrování dat.

Protokol HTTPS je zabezpečenou verzí (nadstavbou) protokolu HTTP – pro přenos používá protokol HTTP, ale přenášená data šifruje pomocí protokolu SSL (TLS). Použití tohoto protokolu funguje na principu asymetrické kryptografie (viz kapitola 1.3.1.2) a s pomocí certifikátů (viz kapitola 1.3.3).

[10] Proxy server funguje jako aktivní prostředník mezi klientem a cílovým počítačem (serverem), překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Může analyzovat obsah komunikace, případně ji pozměňovat.

1.4.3 DoS a DDoS

DoS - Denial of Service (odmítnutí služby) je technika útoku na internetové služby, stránky, uzly či sítě, při níž dochází k zahlcení požadavky a pádu, nefunkčnosti, či nedostupnosti dané služby pro ostatní uzly. Existuje mnoho způsobů, využívajících různé zranitelnosti, jak je možné provést DoS útok s tímto cílem.

Lokální DoS útok znamená, že pro provedení tohoto útoku musí mít útočník přístup k uzlu, na který chce útočit. Existují ale i vzdálené útoky, kde není potřeba mít přístup k uzlu, na který se útočí, ale lze jej napadnout vzdáleně.

DDoS je zkratka pro distribuované DoS útoky (podmnožina DoS útoků). Jedná se o útoky, které jsou charakteristické tím, že se jich účastní více než jeden počítač (počítač inicializující útok).

Dříve tyto útoky vypadaly zhruba tak, že útočníci se museli domluvit a útočili ze svých počítačů nebo počítačů, ke kterým měli přístup. Postupem času se způsob provádění těchto útoků velice změnil. Většina útoků probíhá pouze s jedním útočníkem. K útoku používají takzvané zombie[11] počítače, jež útočníci ovládají pomocí botnetů. Tyto uzly pak vykonávají příkazy útočníka a spolu způsobí DDoS útok.

1.4.4 ARP cache poisoning

Jedná se o techniku využívající slabiny v ARP protokolu, který se stará o překlad IP[12] adresy na MAC[13] adresu [8]. Adresování počítačů v lokální síti je totiž

[11] Zombie je v informatice označení pro počítač připojený k Internetu, který je napaden (např. počítačovým virem nebo trojským koněm) a může být použit pro další počítačové útoky. Mnoho zombie počítačů může tvořit síť nazvanou botnet, která slouží například k zahlcení cílového serveru. Mnoho vlastníků těchto nakažených počítačů mnohdy ani neví, že je jejich počítač zombie.

[12] IP (Internet Protocol) je základní protokol síťové vrstvy používaný v rámci počítačových sítí a Internetu. IP je zodpovědný za směrování paketů ze zdrojového do cílového zařízení. IP adresa – je číslo, které se používá na identifikaci síťových zařízení v sítích, které používají IP protokol. Označením IP se v praxi často myslí IP adresa.

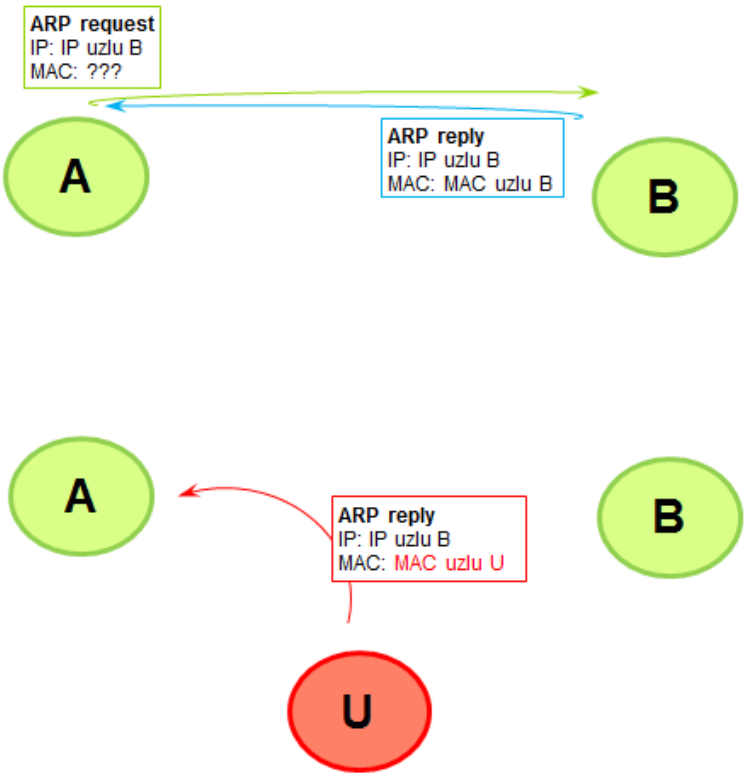
ve skutečnosti realizováno pomocí adres na linkové vrstvě – MAC adres (takže pro doručení dat nám nestačí vědět IP adresu příjemce, potřebujeme vědět jeho MAC adresu).

Při ARP protokolu jsou důležité dva typy paketů – *ARP request* (posílá se na zjištění MAC adresy) a *ARP reply* (posílá se jako odpověď na *ARP request* s vyplněnou MAC adresou).

Komunikace počítačů v lokální síti za pomoci ARP protokolu vypadá následovně: uzel A chce komunikovat s uzlem B, ale zná jenom jeho IP adresu (MAC adresu nezná). Tady přichází na řadu ARP protokol. Uzel A pošle *ARP request* paket s vyplněnou IP adresou uzlu B broadcastem na všechny počítače ve svém okolí. Když dojde tento paket k počítači B (ostatní počítače tento paket ignorují, protože v něm není vyplněna jejich IP adresa jako adresa příjemce), tak odpoví uzlu A. Pošle mu paket *ARP reply*, kde vyplní svou MAC adresu. Když tento paket dorazí zpět k uzlu A, tak ten si přiradí tuto MAC adresu k IP adrese vyplněné v *ARP request* a uloží si toto provázání do vlastní paměti (cache) pro případnou následující komunikaci.

Problémem tohoto protokolu je, že paket *ARP reply* může útočník podvrhnut – tedy pošle uzlu A paket *ARP reply*, ve kterém mu sdělí, že MAC adresa uzlu B je MAC adresa útočníka. Když pak bude chtít uzel A něco odeslat uzlu B, tak to ve skutečnosti odešle útočníkovi U na jeho MAC adresu (vidíme, že je to další možný příklad provedení MITM útoku).

[13] MAC (Media Access Control) je podvrstva linkové vrstvy, která řeší přístup ke sdílenému médiu. MAC adresa - identifikátor zařízení v rámci informačních sítí. Označením MAC se v praxi často myslí MAC adresa.



Obrázek 7 MITM – ARP cache poisoning

Kde nastala chyba? *ARP reply* paket je možné odeslat bez toho, aby mu předcházel *ARP request* paket – při přijímání *ARP reply* paketu se nekontroluje, jestli si ho vůbec někdo vyžádal. Tato „vlastnost“ ARP protokolu je velice nebezpečná a kromě výše zmíněného MITM útoku může být také zneužita pro útoky typu DoS. Při DoS útoku by útočník mohl posílat *ARP reply* pakety uzlu, na který chce provést tento útok, kde by v těchto paketech byla informace, že například IP adresa gateway je provázána s nějakou neexistující MAC adresou. Když by tento uzel chtěl komunikovat přes Internet (tedy přes gateway), tak by posílal pakety na tuto neexistující MAC adresu, čímž by se stal nedostupným.

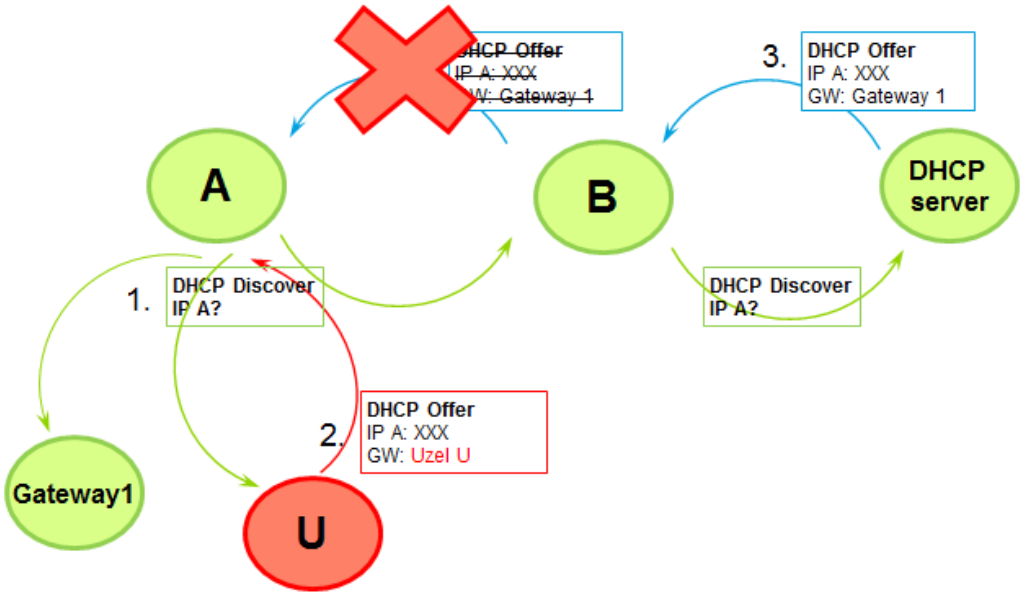
1.4.5 DHCP spoofing

DHCP[14] spoofing [9] je další z MITM technik, pomocí které útočník nastaví oběti jako gateway[15] sebe, čímž si zajistí, že veškerá odchozí komunikace oběti

[14] DHCP (Dynamic Host Configuration Protocol) je protokol, který je určený k dynamickému přidělování síťových parametrů koncovým zařízením.

s Internetem bude probíhat skrz útočníka. Kdyby útočník podstrčil sebe jako DNS server[16], mohl by zachytit oba směry komunikace a sloužil by v podstatě jako proxy server bez toho, aby o tom oběť věděla.

Princip spočívá v tom, že v momentě, kdy se oběť připojí do sítě, nemá přidělenou žádnou IP adresu. K tomu, aby ji získal, rozešle broadcastem *DHCP Discover* paket (krok 1 – viz obrázek 8) a čeká na odpověď od nějakého DHCP serveru[17], který mu IP adresu přidělí (spolu s ostatními parametry). Takových serverů může být na síti víc a platí pravidlo, že klient příjme ten *DHCP Offer* paket, který k němu dorazí jako první.



Obrázek 8 MITM – DHCP spoofing

Toho může využít útočník, když odpoví *DHCP Offer* paketem (v něm uvede jeden z parametrů sítě, který bude udávat falešnou gateway – parametr útočníka – krok 2) rychleji než skutečný DHCP server (krok 3). To, aby útočníkův paket dorazil k oběti dřív než *DHCP Offer* paket od skutečného DHCP serveru, se dá zaručit různými způsoby. Kromě toho, že DHCP servery jsou obvykle trochu pomalejší,

[15] Gateway (brána) je aktivní síťové zařízení, které spojuje sítě – při komunikaci mezi sítěmi je provoz směrován přes ni.

[16] DNS (Domain Name System) je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.

[17] DHCP server přiděluje počítačům pomocí DHCP protokolu síťové parametry (zejména IP adresu).

útočník může být fyzicky blíže k oběti, než je skutečný DHCP server. Útočník by mohl také provést DoS útok na DHCP server a způsobit tak jeho dočasnou nedostupnost.

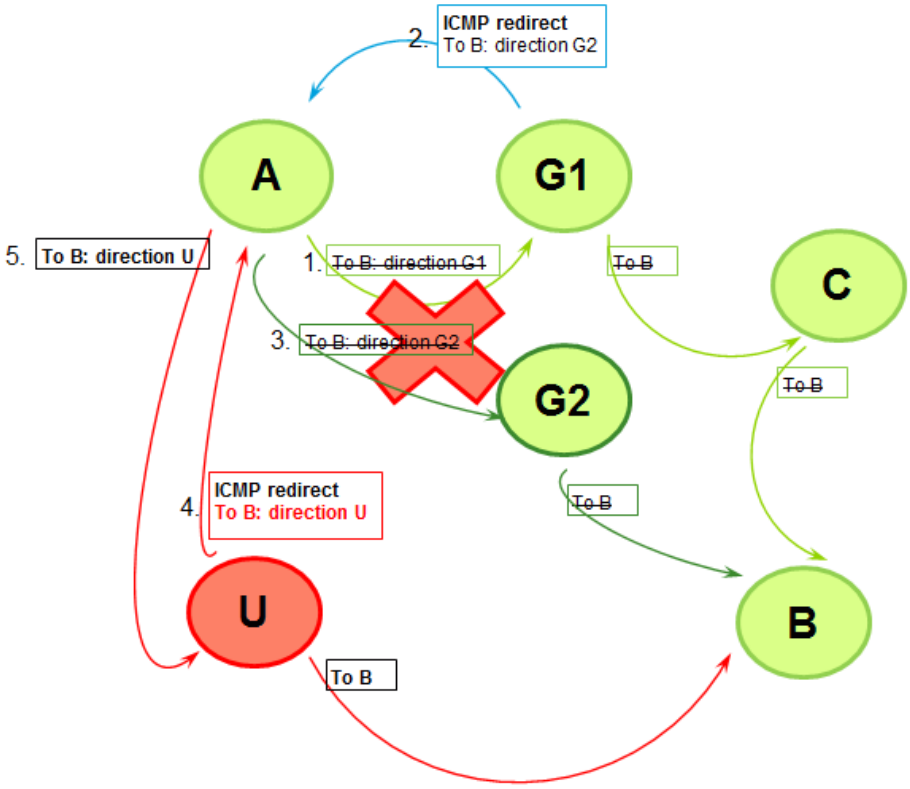
1.4.6 ICMP redirecting

ICMP[18] protokol pomáhá IP protokolu vypořádat se s jeho nespolehlivostí.

Jak víme, IP protokol je nespolehlivý, a proto se občas stává, že se mu nepodaří doručit paket na požadované místo (kvůli fyzickému rušení signálu nebo nespolehlivé síti apod.) a když taková situace nastane, tak se ji nepokouší aktivně řešit (nevyžádá si porušený paket znovu). Co však udělá, je to, že odesílatele paketu alespoň informuje o tom, že se doručení nezdařilo. Tato notifikace se realizuje právě ICMP protokolem. ICMP protokol [9] implementuje různé typy zpráv, které označují jednotlivé chyby - Time Exceeded (došlo k zacyklení nebo paket je na cestě příliš dlouho), Destination unreachable (nedostupná síť nebo počítač, výpadky uzlů), Redirect a další.

Zpráva Redirect upozorňuje na to, že existuje vhodnější cesta mezi dvěma uzly, než ta, která byla zvolena. Když chce například uzel A odeslat zprávu (paket) uzlu B po síti, tak typicky existuje několik cest, kterými se může tento přenos uskutečnit. V případě, že zvolená cesta není nejoptimálnější – řekněme, že gateway G1, přes kterou zpráva právě prochází (krok 1 – viz obrázek 9), má někde poznačeno, že uzel A může komunikovat s uzlem B kratší cestou (tedy přes jinou gateway – G2), gateway G1 odešle uzlu A paket ICMP Redirect (krok 2). V tomto paketu sděluje optimálnější cestu k uzlu B – přes G2. Uzel A si tuto informaci poznačí a příště, když bude chtít kontaktovat uzel B, udělá to přes nově poznačenou gateway G2 (krok 3).

[18] ICMP (Internet Control Message Protocol) protokol primárně neslouží k přenášení dat, ale k přenášení informací o chybách, upozorněních a jiných.



Obrázek 9 MITM – ICMP redirecting

Podle RFC[19] specifikace (RFC 1122) by měly být ICMP Redirect pakety odesílané jenom gatewayemi, avšak nelze to technicky vynutit.

MITM útok by se dal inicializovat například i právě pomocí ICMP redirecting útoku. Kdyby totiž pomocí *ICMP Redirect* paketu útočník sdělit uzlu A, že k uzlu B vede nejkratší cesta přes něj (útočníka – krok 4), a uzlu B by sdělil, že nejkratší cesta od něj k uzlu A vede přes útočníka, tak by veškerá komunikace šla přes útočníka (krok 5).

Pro provedení DoS útoku by se mohly například zneužít ICMP Redirect pakety tak, že by je útočník rozesílal dalším uzlům a nasměřoval je na oběť, čímž by ji zahltil, protože všechny uzly by komunikovaly přes ni.

[19] RFC (Request For Comment) je souhrn doporučení ohledně protokolů (popisu komunikace) Internetu.

1.4.7 Port stealing

Port stealing představuje další formu MITM útoku v síti se switchem. Tento útok je založený na faktu, že switch, který pracuje na linkové vrstvě, a tedy adresuje uzly pomocí MAC adres, si ukládá MAC adresy s příslušným portem v CAM tabulce (Content Addressable Memory table). Aktualizace CAM tabulky nastává při přijímání paketů.

Uzel A odešle zprávu uzlu B a v momentě, kdy tato zpráva prochází switchem, si switch aktualizuje svou CAM tabulku a poznačí si, na kterém portu k němu zpráva od uzlu A přišla (poznačí si tedy provázaně daný port a MAC adresu uzlu A). Následně tento switch prohledá svou CAM tabulku a zkusí v ní najít port, na kterém se nachází uzel B. V případě, že ho najde, přepošle na něj zprávu od uzlu A. V případě, že uzel B ještě poznačený nemá, přepošle zprávu na všechny své porty (kromě portu ze kterého mu zpráva přišla). Když pak uzel B odpoví uzlu A, switch si poznačí port a MAC adresu uzlu B, a protože uzel A již poznačený má, tak zprávu odešle na příslušný port.

Port stealing útok spočívá v tom, že útočník může odeslat zprávu (s libovolným adresátem), ve které nastaví MAC adresu odesílatele na MAC adresu uzlu B. Tím pádem upraví CAM tabulku switche a všechny zprávy, které budou adresovány uzlu B, dorazí ve skutečnosti útočníkovi. Aby se však zpráva nakonec dostala také k uzlu B, musí útočník po získání paketu znovu aktualizovat CAM tabulku switche, aby mohl uzlu B zprávu přeposlat. To může útočník zajistit například odesláním ARP request paketu s IP adresou uzlu B, na který uzel B odpoví ARP reply paketem, který znova projde přes switch, a ten si poznačí jeho novou adresu. Útočník může následně odeslat odposlechnutou zprávu uzlu B.

Samozřejmě, kdyby uzel B mezičasem odeslal nějakou zprávu, tak se CAM tabulka přepíše dřív, a aby tomu útočník zabránil, musel by falešné zprávy na upravení CAM tabulky posílat poměrně často. Taktéž, když uzel B komunikuje s uzlem A příliš frekventovaně, může být pro útočníka velice náročné nepozorovaně odposlouchávat komunikaci vzhledem k častému přepisování CAM tabulky switche.

1.4.8 CSRF, XSS

Cross-site request forgery (CSRF) je rozšířený typ útoků, který zneužívá slabiny internetových prohlížečů a skriptů (v dnešní době typicky Javascript). Útok spočívá v tom, že do aplikace přichází příkazy od uživatele, které ve skutečnosti uživatel nezadal, ale zadal je škodlivý skript (kód – program) na pozadí.

Když uživatel používá nějakou internetovou aplikaci, do které se přihlásí přes internetový prohlížeč, ta využívá k uchování stavu svá cookies s nějakou dobou platnosti.

Pojmem cookies jsou v rámci protokolu HTTP označována data, která posílá server prohlížeči, a ten si je uloží. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Zpravidla se vyměňují informace o typu přenášených dat, o délce platnosti vytvořené relace, apod. Cookies také často slouží k identifikaci aktuální relace, tedy informace o tom, že uživatel je k dané službě (aplikaci) aktivně přihlášen. Relace je permanentní síťové spojení a představuje prostředek, jak mezi jednotlivými přístupy zachovávat a předávat data. Někdy je potřebné uchovávat pro každého uživatele specifické údaje. Například uživatel ve formuláři vyplní své jméno a heslo pro přihlášení do nějaké internetové aplikace. Po úspěšné autentizaci se vytvoří relace a do ní se uloží informace identifikující daného uživatele. Po celou dobu, po kterou je uživatel přihlášený, má aplikace přístup k informacím v dané relaci a když se uživatel odhlásí, relace je zrušena. Takže když se jednou uživatel do aplikace přihlásí, může ji využívat, dokud se neodhlásí, anebo dokud mu nevyprší platnost cookie identifikující relaci.

Lze předpokládat, že útočník tuto aplikaci zná (útočník může taktéž mít účet v této aplikaci, ale jeho cílem je přihlásit se do ní pod účtem oběti), a tedy zná příkazy, kterými se aplikace ovládá – zná například adresu stránky na změnu hesla apod. Aby si uživatel aplikace změnil heslo, potřebuje si v prohlížeči otevřít příslušnou stránku s formulářem na změnu hesla, zadat potřebné parametry (nové heslo) a potvrdit formulář, který se odešle dané aplikaci ve jménu daného uživatele, neboť on je do ní přihlášen (relace je identifikována pomocí uživatelova cookie).

Kdyby útočník chtěl nějakému uživateli změnit heslo oběti, potřeboval by tedy odeslat formulář na změnu hesla s novým heslem na definovanou adresu ve jménu daného uživatele. Při tomto útoku tuto změnu hesla neprovede přímo útočník, ale

nějaký program (skript), který spustí daný uživatel, který o tomto útoku neví. Útočník totiž může naprogramovat nějakou vlastní internetovou stránku (která může vypadat úplně neškodně), do které ale vloží skript, který způsobí to, že po načtení této útočníkovy stránky v prohlížeči uživatele odešle formulář na změnu hesla (i s vyplněným novým heslem, které tam skript vloží) do dané aplikace ve jménu daného uživatele. Bude to fungovat díky tomu, že uživatel má stále uloženu cookie pro přístup do své aplikace, a tedy když do aplikace přijde požadavek na změnu hesla, tak si aplikace myslí, že přišla skutečně od daného uživatele. Takto může útočník například změnit uživateli heslo (anebo upravit nějaká práva, anebo vykonat nějakou jinou operaci) bez toho, aby se o tom uživatel věděl.

Cross-site scripting (XSS) patří spolu s CSRF mezi nejrozšířenější bezpečnostní slabiny internetových aplikací. K XSS útoku dochází, když útočník vloží do aplikace jako uživatelský vstup kus škodlivého kódu a aplikace na to není připravena (tedy tento vstup přijme). Typickým příkladem může být, když aplikace nabízí uživatelům možnost přidávat komentáře, ale nekontroluje, jestli se uživatelé nepokouší vložit do komentářů škodlivý kód. Útočník takto může vložit do komentáře kus kódu v Javascriptu, který se potom při každém zobrazení stránky vykoná. Útočník by takto mohl například vložit do komentáře kód, který aktuálně přihlášenému uživateli změní heslo a nové heslo odešle útočníkovi (podobně jako při CSFR).

2. Ideální elektronický volební systém

Elektronický volební systém je takový, kde se vyjádření voličovy vůle provádí pouze elektronickou formou. V tomto textu budeme za elektronický volební systém považovat volby přes Internet. Jak již bylo zmíněno v úvodu, protože se práce nezabývá přesnou definicí a technickým řešením elektronického volebního systému, můžeme si v tomto případě představit jak volby přes webový prohlížeč, tak volby přes nějakou desktopovou aplikaci. Blíže se budeme tímto rozdílem zabývat v Tezi 2 této kapitoly.

Kapitola 2 podává návrh požadavků pro elektronický volební systém, poukazuje na jejich provázanost a v podkapitole 2.3 poukazuje na to, že bezpečnost volebního systému se nemá řešit jenom z technického pohledu, jako je například šifrování, ale i z organizačně-procesního hlediska, které tato podkapitola popisuje.

V následující tabulce shrneme základní společné a rozdílné vlastnosti papírových a elektronických voleb.

Vlastnosti voleb	**Papírové volby**	**Elektronické volby**
Přesně definovaný čas, kdy může oprávněný volič uplatnit svoje právo volit v daných volbách.	X	X
Existence definice oprávněného voliče a seznamu oprávněných voličů[20].	X	X
Existence seznamu kandidátů voleb (jasně definovaný předmět voleb, například i body referenda).	X	X
Existence seznamu privilegovaných osob[21].	X	X
Volič musí hlasovat sám za sebe, a aby mu bylo umožněno vykonat volbu, musí prokázat svou totožnost.	X	X
Volby jsou tajné.	X	X
Hlasy se nesmí falšovat, špatně započítat.	X	X
Musí být zabráněno možnosti kupování hlasů.	X	X
Volební systém započítá jenom poslední správně provedenou volbu od daného voliče.	X	X
Existence definice způsobu práce s volebními lístky, kdy jsou neplatné a přesně definovaný způsob hlasování.	X	X
Musí být stanovena přesná definice toho, za jakých podmínek a jakým způsobem je voličovi umožněno hlasovat. I mimo volební místnost nebo mimo volební okrsek v místě svého trvalého pobytu.	X	X
Přesně definované místo pro provedení volby.	X	-
Přímá kontrola průběhu volby oprávněnými osobami.	X	-
Možnost provedení opakované volby.	-	X
Definovaní jestli, kdy, jakým způsobem a za jakých podmínek má volič možnost kontroly stavu svého	-	X

[20] Pro různé volby v různých státech může pojem oprávněný volič znamenat něco jiného, ale uveďme si příklad definice oprávněného voliče pro volbu prezidenta České republiky v lednu 2013, kterou uvádí Ministerstvo Vnitra České republiky: „Voličem pro volbu prezidenta České republiky je státní občan České republiky, který alespoň druhý den volby, tj. 12. ledna 2013, dosáhl věku nejméně 18 let. Ve druhém kole volby může volit i státní občan České republiky, který alespoň druhý den druhého kola volby, tj. 26. ledna 2013, dosáhl věku 18 let.“

[21] Jsou to osoby s jistými, přesně definovanými, přidělenými pravomocemi v rámci volebního systému, v papírových volbách tzv. volební (okrsková) komise.

volebního lístku (uložen/ započten/ zneplatněn).		

Tabulka 1 Vlastnosti voleb

Tato tabulka nás přivádí do problematiky papírových a elektronických voleb – vidíme, že většina zmíněných vlastností je podobná. Některé z těchto vlastností jsou problematické pro naplnění – například zabránění kupování hlasů. Určitě bychom chtěli, aby byla tato vlastnost zachována v obou typech voleb, což je ale náročné, protože jak při papírových volbách, když můžete být donuceni nahrát si na video celý proces volby, který se odehrává za volební plentou, nebo vynesení zbývajících volebních lístků ven z volební místnosti, tak i při elektronické volbě nemusí být tato vlastnost naplněna. To ale neznamená, že to nepovažujeme za vlastnost volebního procesu, kterou chceme, aby volební systém měl.

Možnost provedení opakované volby v rámci elektronických voleb znamená, že volič, který má právo volit, může provést volbu víckrát s tím, že každá správně provedená nová volba (správně provedenou se myslí v analogickém významu vzhledem ke klasické papírové volbě – provedena v souladu s předpisy a zákony týkajícími se voleb – například provedena ve správném časovém rozmezí, volič má právo volit, volba byla přijata volebním systémem) anuluje volbu předchozí. Do sčítání hlasů bude započtena poslední správně provedená volba.

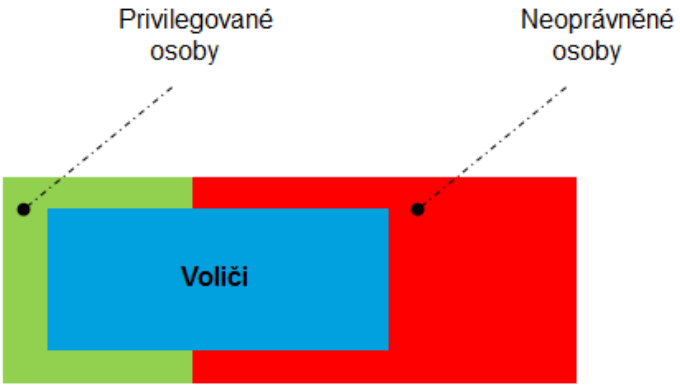
Fungování elektronického volebního systému vychází ze stejného principu jako je ten, na kterém funguje klasický „papírový" volební systém, na jaký jsme v České republice zvyklí. Důvod je zřejmý, a to úspěšné provedení elektronických voleb alespoň na stejné úrovni bezpečnosti, jaká provází proces stávajících klasických voleb. Bezpečnost je velmi důležitý faktor, který se musí analyzovat v celém průběhu tvorby, implementace a udržování elektronického systému.

2.1 Požadavky na elektronický volební systém

S definicí požadavků volebního systému úzce souvisí identifikace jednotlivých subjektů, které mají jednoznačně určená svá práva (co daný subjekt smí), záruky (co je danému subjektu zaručeno) a omezení (co daný subjekt nesmí). Následující výčet můžeme považovat za seznam požadavků, které vytváří charakteristické vlastnosti

volebního systému a určují míru jeho bezpečnosti. Ideální systém tak můžeme definovat jako takový, který splňuje všechny následující požadavky.

Rozlišujeme tři subjekty, a těmi jsou volič, privilegovaná osoba a neoprávněná osoba. Následující obrázek znázorňuje vzájemné vztahy mezi jednotlivými subjekty. Privilegované a neoprávněné osoby v tomto pojetí tvoří disjunktní množiny. Volič (ten, kdo má právo volit) může být buď privilegovaná, nebo neoprávněná osoba. Ti, kteří nemají právo volit, mohou být také buď privilegované, nebo neoprávněné osoby (kdo nemá právo volit, je ale pravděpodobně neoprávněná osoba).



Obrázek 10 Subjekty voleb

Definujme tedy jejich práva, záruky a omezení v rámci procesu elektronických voleb, které definují základní požadavky na volební systém:

Volič

Definice subjektu oprávněného k volbě je stanovena před každou volbou, která se chystá. Tato definice může být různá pro různé státy a různé typy voleb.

1. Práva voliče

1.1 Volič má právo vykonat volbu, a to opakovaně – víckrát elektronickým způsobem a jednou papírovým způsobem (započtení volby řeší sekce Záruky voliče).

1.2 Volič má právo kontroly stavu svého volebního lístku (uložen/započten/zneplatněn).

2. Omezení voliče

2.1 Volič musí volit sám za sebe.

2.2 Volič musí mít pro odevzdání volby příslušné vybavení nebo se musí nacházet v takové lokalitě, kde je toto vybavení k dispozici nebo kde může vykonat volby klasickým "papírovým" způsobem[22]. Toto omezení je ale v souladu se zárukou pro voliče 3.5 (nenáročnost provedení volby bez zvláštních znalostí).

2.3 Co se týče administrace volebního systému nebo přístupu k informacím v něm uložených, je volič považován za neoprávněnou osobu, tedy vážou se na něj omezení neoprávněných osob, s výjimkou toho, kdy je nějaký volič určen, že v rámci volebního systému mu jsou přidělena práva privilegované osoby.

3. Záruky voliče

3.1 Voličovi je zaručeno utajení jím provedených voleb.

3.2 Voličovi je zaručeno, že jeho správně provedená volba se započte a započte se jenom jeho poslední správně provedená volba. Změna volby daným voličem je zaručena v případě, že předchozí volba byla vykonána elektronickým způsobem. Volba vykonána klasickým „papírovým" způsobem je neměnná a nahrazuje případnou předchozí elektronickou volbu.

3.3 Voličovi je zaručeno, že jeho poslední správně provedená volba se započte správně.

3.4 Voličovi je zaručeno, že pod nátlakem jakékoli osoby k vykonání volby se buď voličova volba nezapočte, nebo se započte, ale v takovém případě má volič právo pro provedení opakované volby (1.1) a záruku, že se započte jeho poslední správně provedena volba (3.2).

3.5 Voličovi je zaručeno nenáročné provedení volby bez nutnosti zvláštních znalostí[23].

---

[22] Jestliže volební systém dovoluje volbu i papírovým způsobem.

[23] Tento požadavek je sice relativní, protože pro lidi, kteří vůbec nepoužívají (neumí používat) počítač, bude provedení elektronické volby v podstatě nemožný úkol (v tomto případě by stálo za uvážení ponechat jako možnost volbu klasickým papírovým způsobem). Nicméně by se při návrhu systému mělo dbát na to, aby bylo jeho použití co nejméně náročné. Je rozdíl, jestli si bude nutné pořídit certifikát od důvěryhodné certifikační autority, nebo si koupit čtečku karet a obdržet čipovou identifikační kartu, nebo zadat kromě jména a hesla vygenerovanou sekvenci čísel, kterou volič obdrží na e-mail nebo přes SMS.

3.6 Voličovi je zaručeno, že jeho volební lístek, který chce odeslat do volebního systému k započtení, bude zašifrován pomocí bezpečného šifrovacího schématu a zůstane zašifrován minimálně po dobu sčítání hlasů.

3.7 Voličovi je zaručeno, že jeho zašifrovaný volební lístek, který chce odeslat do volebního systému k započtení, bude podepsán pomocí volební aplikace, a že podepisovací schéma je bezpečné.

3.8 Voličovi je zaručena nemožnost prokazatelnosti toho, jak volil.

3.9 Voličovi je zaručeno, že logovací systém v rámci volebního systému je bezpečný a loguje vše, co je potřebné pro dohledatelnost jakékoli události, potřebné pro řešení bezpečnostních incidentů nebo pro kontrolu procesu v zpracování hlasu (souvisí s právem pro voliče 1.2 a pro privilegované osoby 1.3).

Privilegovaná osoba (volební komise)

Je osoba určena pro administrování, kontrolu auditních logů nebo má jiný, přesně definovaný, přístup do volebního systému.

1. Práva privilegované osoby[24]

1.1 Privilegovaná osoba má právo určit oprávněnost subjektu k volbě[25].

1.2 Privilegovaná osoba má právo provést sečtení volebních lístků opakovaně.

1.3 Privilegovaná osoba má právo kontroly, jestli byly všechny správně odevzdané hlasy správně započteny[26].

1.4 Privilegovaná osoba má právo administrovat volební systém v souladu s bezpečným rozdělením jednotlivých povinností, pravomocí a přístupových práv.

2. Omezení privilegované osoby

[24] Práva privilegované osoby – myslí se tím práva, která mohou být přidělena privilegovaným osobám. Tato práva pro různé privilegované osoby mohou být různá.

[25] Oprávněnost subjektů k volbě například při provádění registrace nebo při případné papírové volbě.

[26] Například auditor, který nemá jinak přístup k administraci – spravování systému, může být definován jako privilegovaná osoba s právem této kontroly.

2.1 Privilegovaná osoba smí administrovat jen tu část systému, na kterou se vztahují její privilegia.

2.2 Privilegovaná osoba nemůže zneužít svých pravomocí k získání neautorizovaného přístupu do jiné části volebního systému než k té, na kterou má právo (a ke které jí volební systém přístup umožňuje) nebo získání tajných informací souvisejících s volbami.

2.3 Privilegovaná osoba nesmí pomoct neoprávněným osobám získat přístup do volebního systému nebo získat tajné informace související s volbami.

Neoprávněná osoba (třetí strana)

Vůči volebnímu systému je pojem neoprávněná osoba ve smyslu všech osob, které nejsou privilegované osoby.

1. Omezení neoprávněné osoby

1.1 Neoprávněná osoba nemá žádný přístup do volebního systému nebo k informacím v něm uložených.

1.2 Neoprávněná osoba není schopna se dozvědět o provázanosti mezi voličem a jeho hlasem.

1.3 Neoprávněná osoba není schopna se dozvědět průběžný výsledek sečtení hlasů před jeho oficiálním zveřejněním nebo seznam voličů, kteří volili.

1.4 Neoprávněná osoba nesmí odposlechnout, modifikovat, mazat nebo duplikovat odevzdané nebo odevzdávané volební lístky. Kdyby došlo k takové situaci, musí být toto včas odhaleno a musí být definován postup, jak v dané situaci pokračovat ve volebním procesu.

1.5 Neoprávněná osoba nemá možnost přístupu k většímu množství podepisovacích klíčů voličů (k takovému množství, že by to mohlo ovlivnit výsledek voleb).

1.6 Neoprávněná osoba nemá možnost přístupu k privátnímu klíči volebního systému (privilegovaná osoba nemá možnost tento klíč kompromitovat).

Všechny tyto tři subjekty mají právo dozvědět se finální výsledek voleb.

2.2 Provázanost požadavků

Zmíněné požadavky jsou navzájem provázány a různě se ovlivňují. Podívejme se na pár příkladů, jak lze pracovat s plněním jednotlivých požadavků a jak například docílení jednoho požadavku v některých případech může znamenat rozpor s jiným požadavkem.

Teze 1

Požadavek pro voliče 3.2 říká, že se započte jenom poslední voličem správně provedená volba (úzce souvisí s požadavkem pro voliče 1.1 o právu na vykonání opakované volby), a požadavek pro voliče 1.2 mluví o voličském právu ověřit si stav svého volebního lístku.

Řešení 1.1

Požadavky z Teze 1 mohou implikovat potřebu jistého provázání identifikačních údajů voliče a jeho volby. Toto provázání existuje, ukládá-li se někde ve volebním systému hlas voliče spolu s identifikací daného voliče. Na základě těchto informací, které jsou uloženy v systému provázaně, je možno zaručit, že když oprávněný volič bude volit vícekrát, tento záznam se v systému najde a zneplatní se (nebo vymaže), a nová volba se zapíše stejným způsobem, tedy také s provázáním na identifikační údaje voliče.

Důsledek 1.1.1

Tedy kdyby se požadavky pro voliče 3.2, 1.1 a 1.2 naplnily tímto způsobem, tak by v jistém slova smyslu kolidovaly s požadavkem pro voliče 3.1 a pro neoprávněné osoby 1.2, které mluví o uchování voličovy volby v tajnosti a o nemožnosti se dozvědět o provázanosti voličovy volby a jeho identifikačních údajů, což je ohroženo, existuje-li toto provázání v systému.

Řešení 1.2

Zkusme upustit od myšlenky provázání voličovy volby s jeho identifikačními údaji, jak je nastoleno v Řešení 1.1 a uvažujme zabezpečení například na

algebraicko-kryptografické úrovni. Zabezpečení takové, že by jenom oprávněný volič byl schopen zjistit ze zašifrovaného hlasu uloženého v systému, jestli se jeho hlas započetl bez toho, aby s tímto zašifrovaným hlasem byly provázány identifikační údaje voliče v kterékoli části volebního systému, a že by volební systém byl schopen provedenou volbu nahradit, po zjištění, že volič už jednu volbu provedl. Kdyby se implementace podle daného návrhu podařila, bylo by to velmi přínosné pro volební systém (protože bychom se obešli bez uvedeného provázání a přitom bychom zachovali možnost opakované volby), samozřejmě nám zůstává otázka, jestli je vůbec možné takovým způsobem prakticky řešit tento návrh.

Důsledek 1.2.1

Zřejmě bychom tak implementací Řešení 1.2, vyhověli požadavkům pro voliče 1.1, 1.2, 3.1 a 3.2 a pro neoprávněné osoby 1.2.

Řešení 1.3

Požadavkům z Teze 1 by se dalo vyhovět i tak, že by se provázání identifikačních údajů a uskutečněné volby voliče provedlo sofistikovaněji - zašifrováním těchto identifikačních údajů. Tím pádem by v systému byly uloženy záznamy, které sestávají ze zašifrovaného hlasu voliče a ze zašifrovaných identifikačních údajů voliče, obě informace by byly zašifrované veřejným klíčem volebního systému. Takže jenom dedikovaná část volebního systému by mohla v případě potřeby dešifrovat identifikační údaje jednotlivých voličů.

Zde by se dal například implementovat kryptografický algoritmus Shamirovo schéma pro sdílení tajemství - mluví o rozdělení informace o tajemství na několik částí a odhalení těchto částí jistým osobám, tajemství se rozluští při kooperaci určeného počtu osob, kterým byla část tajemství vyzrazena. Informace pro použití privátního klíče by se tedy mohla rozdělit na několik částí a každou bychom odhalili nějaké privilegované osobě. Následně bychom určili přesný počet těchto částí, které budou potřebné pro rekonstrukci původní informace (mohly by to být třeba všechny privilegované osoby, kterým byla sdělena tato dílčí informace pro snížení rizika zneužití tohoto privilegia).

Důsledek 1.3.1

Systém by Řešení 1.3 tedy mohl využívat v případě, že by zjistil, že daný volič už svou volbu provedl a potřeboval by jeho hlas vymazat a nahradit ho novým a také kdyby se uživatel dotázal, v jakém stavu se nachází jeho volební lístek. A přitom jsme se přiblížili i k naplnění požadavků pro voliče 3.1 a pro neoprávněné osoby 1.2. Požadavky z Teze 1 (tedy požadavky pro voliče 1.1, 1.2 a 3.2) jsou splněny z předpokladu Řešení 1.3.

Řešení 1.4

Zamysleme se nad tím, jak by šlo provést vylepšení Řešení 1.3. Řešení 1.3 navozuje otázku, co kdyby se náhodou podařilo útočníkovi zjistit privátní klíč volebního systému (šlo by tedy dešifrovat jak ID voliče, tak jeho volební lístek). To by se mohlo ale vyřešit tak, že by se nešifroval identifikační údaj voliče (v otevřené podobě), ale jenom jeho haš[27], který by byl vytvořen nějakou bezpečnou hašovací funkcí. Hašování by se mohlo provádět ve volebním systému nebo ve volební aplikaci. Tím by se zvýšilo zabezpečení, že i v případě odhalení privátního klíče volebního systému by nebylo tak jednoduché zjistit jednotlivé identifikační údaje voličů, díky jednosměrnosti hašovací funkce (i kdyby se útočníkovi podařilo dešifrovat volbu), protože údaj, který by dostal po dešifrovaní, by nebyla identifikace voliče, ale jenom otisk této informace. Útočník by musel znát hašovací funkci systému, musel by znát identifikační údaje voliče ve správném formátu (jak vstupují do hašovacího algoritmu) a musel by zkoušet hašovat tyto údaje a porovnávat je s ostatními zahašovanými identifikátory.

Ale tomuto zkoušení by mohlo být zabráněno například požadavky pro neoprávněné osoby 1.1 (omezení přístupu do systému a k informacím) a omezeními pro privilegované osoby.

Je potřebné připomenout, že systém by v případě povolení opakované volby musel být schopen sám porovnávat haše identifikačních údajů voličů, takže použitá

[27] Jak již bylo zmíněno v kapitole 1.3.1.4, čím více je dat, které chceme hašovat tou samou funkcí, tím je vyšší pravděpodobnost, že narazíme na kolizi, tedy že dvě výsledné haše budou stejné. Pravděpodobnost je stále malá a nemusí být pro volební systém zajímavá, protože když kolize nastane ve dvou případech, nemuselo by to hned znamenat narušení bezpečnostních atributů systému, díky velkému počtu voličů.

hašovací funkce by měla jako sůl[28] používat bezpečně uložený náhodný prvek (pro každého voliče jiný).

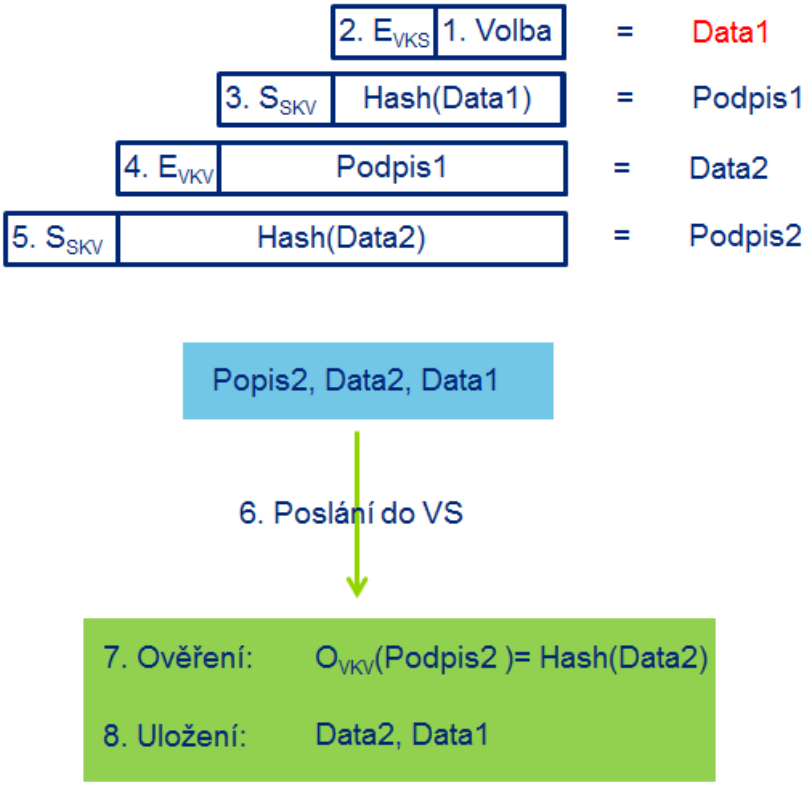
Důsledek 1.4.1

Tímto hašovaním a šifrováním identifikačních údajů voliče pomáháme kromě naplnění požadavků z Teze 1 (pro voliče 1.1, 1.2 a 3.2) navíc naplnění požadavků pro voliče 3.1 a pro neoprávněné osoby 1.2, tedy tajnosti voleb.

Řešení 1.5

Ještě by se to dalo řešit možností (viz obrázek 11), kde by volič odvolil (1), jeho volba by se zašifrovala veřejným klíčem volebního systému E_{VKS} (2), pak by se udělal elektronický podpis soukromým klíčem voliče S_{SKV} (3), elektronický podpis by se zašifroval veřejným klíčem voliče (toto by se stalo nečitelným pro každého kromě daného voliče) E_{VKV} (4), tyto data by se následně podepsala opět soukromým klíčem voliče S_{SKV} (5) a poslala do volebního systému (6). Volební systém by ověřil elektronický podpis O_{VKV} (7), zjistil, jestli volič má oprávnění k volbě. Elektronický podpis by mohl zahodit, čím by se ztratilo další nechtěné provázání identifikačních údajů voliče a jeho volby. Zůstal by zašifrovaný elektronický podpis veřejným klíčem voliče (nemá žádnou vypovídající hodnotu pro toho, kdo nevlastní privátní klíč voliče) a zašifrovaný volební lístek veřejným klíčem systému (8). Tyto dvě informace by se mohly uložit provázaně.

[28] Sůl v terminologii hašování znamená jistý přídavek k hašované hodnotě; může být stejný, ale většinou se používá jiná hodnota soli pro každou hašovanou hodnotu. Použitím soli se předchází útokům s cílem uhodnutí hašované hodnoty.



Obrázek 11 Řešení 1.5

V případě, že volič provede druhou volbu, ověří se, jestli zašifrovaný elektronický podpis voliče Data2 již je uložen v databázi, a jestli je, tak se hodnota zašifrovaného volebního lístku nahradí novou volbou. Nikdo není schopen se dozvědět, kdo je daný volič, jemuž patří zašifrovaný elektronický voliče Data2. Kdyby se někdo pokoušel o falzifikaci, tak by potřeboval přístup k soukromému klíči voliče určenému pro podepisování.

Problém by ale mohl být v tom, že by si aplikace uživatele nebo uživatel museli pamatovat, jakou volbu provedl volič posledně – Data1 (protože další podepisování a šifrování navazuje na data „1. Volba"). Při opakované volbě by se tedy poslala do volebního systému taková volba, jako minule, tím by se vyhledal správný záznam (Data2), pak by volič provedl novou volbu a záznamy Data1 i Data2 z minulé volby by se nahradily novými záznamy.

Možná by tedy stálo za úvahu přidělit jednotlivým voličům nějaké jednoznačné identifikátory (ve volebním systému by nebylo známo žádné provázání mezi voličem a tímto identifikátorem), které by muselo být zadáno při každé volbě. Ve volebním systému by se pak ukládal místo identifikátoru voliče (například jeho elektronického podpisu), jež by mohl být zneužit pro kompromitaci tajnosti voleb, právě tento

identifikátor spolu s hlasovacím lístkem voliče Data1, který by nedával zpětnou vazbu na voliče.

Důsledek je podobný jako při předchozím řešení.

Řešení 1.6

Co by se ale stalo, když by se daný počet privilegovaných osob z Řešení 1.3 sešel. Mohly by si nějaký volební lístek dešifrovat a volbu změnit. Takže by bylo asi vhodné, kdyby se například v systému dal použít klíč pro dešifrování jenom v určitou dobu a jenom jedenkrát. Ověřování, jestli volič volil, by se neprovádělo při každé volbě. Jednoduše by se uložil každý platný volební lístek, který by byl přijat volebním systémem. Nakonec by se v určitou, přesně stanovenou, dobu použil dešifrovací klíč, hlasovací lístky by se dešifrovaly, zneplatnily by se ty, které jsou duplicitně nebo neplatné, a ponechal by se poslední platný volební lístek od každého voliče. Samozřejmě privilegované osoby, které mají přístup k aktivaci dešifrovacího klíče, by neměly možnost jakýmkoli způsobem měnit hlasovací lístky.

Teze 2

Nastolme si otázku, jakým způsobem provést identifikaci uživatele před samotnou volbou, aby došlo k naplnění následujících tří požadavků, které se jistým způsobem vzájemně rozporují – požadavky pro voliče 1.1 (souvisí s požadavkem pro voliče 3.2), 3.1 a pro neoprávněné osoby 1.2. Ty říkají, aby každý volič, který je způsobilý, mohl provést svou volbu opakovaně a aby se správně započetla poslední správně provedená voličova volba, aby tato volba zůstala v tajnosti, tedy aby se neporušila důvěrnost provázání mezi voličovou identifikací a tím, jak hlasoval.

Řešení 2.1

V případě, že by se toto řešilo tak, že volič se za účelem volby přihlásí do systému přes nějakou webovou volební aplikaci, narážíme na fakt, že v momentě, kdy se uživatel takovým způsobem přihlásí a následně hlasuje, tak zde existuje virtuální provázání mezi jeho hlasem a identitou. Podívejme se tedy na to jinak.

Řešení 2.2

Zkusme to například vyřešit tím, že by se volič nemusel přihlašovat do on-line aplikace, ale využila by se nějaká off-line (desktopová) aplikace a systém dvou obálek.

Aplikace by mohla provést zašifrování hlasu (obsah vnitřní obálky) a digitální podpis podpisovým certifikátem (obsah vnější obálky), který slouží k identifikaci voliče. Kdyby se tato dvojitá obálka zaslala například e-mailem na volby přijímající server, mohla by se provést identifikace voliče až přímo na tomto serveru. Po úspěšném ověření identifikačních údajů z vnější obálky by server provedl jednu z následujících možností. V případě, že volbu poslal volič, který není oprávněn k volbě (například není v seznamu oprávněných voličů, který je v systému uložen), server by zapsal do logu tuto událost a voliči by poslal zprávu (například e-mailem), že není oprávněn k volbě. V druhém případě a to, že by ověřená identita patřila voliči, který je oprávněn volit, server by oddělil vnitřní a vnější obálku a do dedikovaného úložiště by uložil zašifrovaný hlas (tedy obsah vnitřní obálky) a digitální podpis by mohl zahašovat, zašifrovat a uložit s daným zašifrovaným volebním hlasem v provázanosti (následně by si zapsal voliče do seznamu voličů, kteří již úspěšně svou volbu provedli).

Důsledek 2.2.1

Využití systému dvou obálek, kde ve vnitřní obálce je zašifrovaný hlas a vnější obálka obsahuje digitální podpis voliče, nám řeší požadavky pro voliče 1.1, 3.1 a pro neoprávněné osoby 1.2.

Na druhé straně přináší použití desktopové aplikace jisté komplikace. Může to být méně pohodlné pro voliče, kteří si musí aplikaci stáhnout, nainstalovat a musí ji aktualizovat. Tato aplikace by se neměla provozovat na zařízení, které nedosahuje jistou úroveň zabezpečení (systém by měl umět zakázat instalaci aplikace na zařízení, které nesplňuje jistou předem definovanou normu). Bylo by vhodné, aby zařízení měla vhodný antivirový program, antispyware (který blokuje spyware vysvětlen v kapitole 1.4) a jiné bezpečnostní prvky. Je potřebné myslet i na zabezpečení toho, aby voličovi nebyla podvržena nějaká aplikace, která se tváří, že je ta pravá volební, ale je škodlivá a buď získává citlivé údaje od voliče, nebo zjišťuje, jak volil, nebo například jeho volbu před zašifrováním pozmění.

Dále by byla potřeba řešit informovanost uživatelů ohledně managementu klíčů – jak používat certifikáty, jak je uskladňovat a podobně.

Webová aplikace může tedy působit vhodněji, protože nevyžaduje od uživatele žádný servis (tedy kromě správného operačního systému, webového prohlížeče a jeho nastavení). Samozřejmě i tady existují útoky, které podvrhnou jinou stránku, která vypadá jako opravdová volební aplikace, ale je škodlivá a narušuje atributy bezpečnosti.

Teze 3

Zkusme například upustit z požadavků v Tezi 1 a to z požadavku pro voliče 1.1 (oprávněnost pro provedení opakované volby) a z požadavku 1.2 (ověření voličem, stavu jeho volebního lístku).

Důsledek 3.1

Toto upuštění od požadavků by znamenalo, že by se identifikace voliče nemusela ukládat nikde v rámci volebního systému provázaně s hlasovacím lístkem voliče. Byl by udržován v lokální databázi systému jenom seznam voličů, kteří provedli úspěšnou volbu, čím by se docílilo vyššího utajení voličova hlasu, které je představováno požadavky pro voliče 3.1 a pro neoprávněné osoby 1.2.

Důsledek 3.2

Upuštění od požadavku pro voliče 1.1 (možnost provedení opakované volby), by zkomplikovalo docílení části požadavku pro voliče 3.4 – nemožnosti opravy volby, která byla vykonána pod nátlakem a tedy provedení opakované volby. Protože kdyby někdo donutil voliče hlasovat za to, co by nebylo v souladu s jeho osobním názorem a volič by po vykonání této vynucené volby, neměl možnost tuto volbu změnit, bylo by to v rozporu jednak s principem voleb a jednak by to kolidovalo s omezením pro voliče 2.1 (volič musí volit sám za sebe).

Je ale nutné, aby byl základní požadavek pro voliče 1.1 (a s ním související požadavek pro voliče 3.4) o možnosti provedení opakované volby brán jako nutný požadavek v rámci každého elektronického volebního systému? Zamysleme se nad tím, kdy je vhodné, aby volič měl možnost provést volbu opakovaně v případě, že jeho volba se započte správně. Co může voliče vést k tomu, aby svou již provedenou

volbu změnil? Je asi logické uvažovat to, že volič asi nezmění názor za relativně krátký čas (v případě papírové volby tato možnost ani není a klasický volební systém funguje) takže když volič vykonává opakovanou volbu, je možné že byl k první volbě (nebo právě je k této volbě) donucen. Když někdo donutí voliče provést volbu pod nátlakem, tak jaká je pravděpodobnost, že pak přijde za ním ještě jednou (pro jistotu) a donutí ho zase volit, protože si myslí, že volič pozměnil již vykonanou nucenou volbu? Pakliže volební systém dovoluje provedení papírové volby, která ruší započtenou elektronicky provedenou volbu a je již neměnná, tak volič který volil pod nátlakem, má možnost nakonec všechno dostat do svých rukou, protože papírový systém u nás funguje[29].

Je právě načrtnuta úvaha například hodná pro uvažování v takových situacích, kde při sčítaní hlasů jsou pro výsledky voleb doopravdy rozhodující jednotlivé hlasy a tedy kdyby byl jeden hlas volen pod nátlakem, mohlo by to zvrátit celý výsledek voleb, anebo stojí za to implementovat tento požadavek jako vlastnost elektronického volebního systému i v případě, že změna pár hlasů pod nátlakem nemá pravděpodobně žádný vliv na výsledky voleb. Ale zase, tam, kde je voličů oprávněných volit relativně málo, oplatí se vůbec implementovat elektronické volby? Nestačí provádět jenom jednoduché a zaběhnuté klasické papírové volby?

Kdybychom totiž opomněli nutnost dvojí volby (požadavek pro voliče 1.1 a 3.4), tak bychom pravděpodobně navrhovatelům volebního systému ulehčili mnoho práce a také bychom snížili riziko odhalení spojitosti mezi voličovým identifikátorem a jeho hlasem (požadavek pro neoprávněné osoby 1.2), protože již by nebylo nutné ukládat toto provázání. Když by lístek přišel do systému, tak by se jednoduše započetl a mohl by se smazat (volič by se zapsal do seznamu, že provedl úspěšnou volbu, která byla započtena). Žádné komplikované zabezpečení již není nutné. Tak dostáváme naplnění požadavku pro neoprávněné osoby 1.2 o neschopnosti dozvědět se provázání mezi voličovou identitou a jeho odevzdaným hlasem.

Teze 4

[29] Elektronický volební systém je ale vhodné uvažovat tak, že v budoucnosti by úplně nahradil papírové volby. Proto není velkým argumentem spoléhat se na papírové volby. Diskuze nad touto myšlenkou je ještě rozvedena dále v Tezi 4.

Kdybychom chtěli jít jinou cestou, než nám nastoluje Důsledek 3.2 a chtěli bychom tedy splnit požadavky pro voliče 1.1 a 3.4 (opravy volby, která byla vykonána pod nátlakem a tedy provedení opakované volby), dalo by se to vyřešit i následující návrhem řešení.

Řešení 4.1

A to například tak, že by se každý volič šel zaregistrovat před začátkem voleb na určené místo, na které by mu v průběhu registrace bylo sděleno unikátní číslo. Toto číslo by bylo vyžadováno volební aplikací v momentě šifrování hlasu. Systém by mohl fungovat tak, že kdyby uživatel zadal číslo správně, tak by se jeho volba normálně započetla. V případě, že by ho volič zadal například odzadu, tak to by bylo upozorněním pro volební systém, aby danou volbu vůbec nezapočítal a voliče nezapsal do seznamu subjektů, kteří již provedli úspěšnou volbu. Samozřejmě by volební systém poslal uživateli zprávu, že hlasování proběhlo v pořádku a jeho hlas byl započten (aby si subjekt, který donutil volit voliče pod nátlakem, myslel, že tato volba byla započtená správně). Takže volič by pod nátlakem mohl zadat své heslo odzadu a v případě opakované volby (již ne pod nátlakem) by zadal své heslo správně a jeho hlas by se započetl.

Důsledek 4.1.1

Toto není ale v souladu s částí požadavku pro voliče 2.2 a to s lokalitou voliče. Protože kdyby byl volič například v zahraničí, nebyl by schopen přijít se zaregistrovat a odnést si své heslo (ale s tímto problémem se setkáváme i při papírových volbách a není neřešitelný).

Také to představuje jistý rozpor s požadavkem pro voliče 3.5 (záruka nenáročného provedení volby). To, že si volič musí zajít pro PIN kód, by se možná dalo zvládnout (možná by systém vyžadoval nějakou registraci předem), ale zapamatovat si ten kód již nemusí být příjemným požadavkem pro voliče.

Řešení 4.2

Teze 4 by mohla být vyřešena i tak, že by heslo mohlo přijít prostřednictvím e-mailové zprávy nebo textové správy do mobilního telefonu voliče. Záleží, kdy by mu tato informace přišla. Kdyby to bylo při provádění volby, tak by to mohl útočník

zneužít a mohl by voliče donutit vykonat volbu pod nátlakem. Je možné, že kdyby si mohl to číslo vygenerovat volič v jakoukoli chvíli, tak by to útočník nemusel vědět zneužít.

Řešení 4.3

Dalším způsobem dosažení požadavku pro voliče 3.4 by mohlo být použití čipových karet (s digitálním podepisovacím certifikátem) a s PIN kódem, ale tím pádem je nutné použití čteček karet a znalost PIN kódu, který by se ale zase dal použít například tak, že by se zadal odzadu v případě, kdyby byl volič nucen volit pod nátlakem.

Důsledek 4.3.1

Toto ale zase koliduje s požadavkem pro voliče 2.2 na jednoduchost volby, ale řeší to požadavek pro voliče 3.4.

Teze 5

Zamysleme se nad tím, jak zabezpečit tajnost voleb i v průběhu sčítání, tedy zaručení požadavku pro voliče 3.1 a požadavku pro neoprávněné osoby 1.3 (neoprávněná osoba není schopna se dozvědět průběžný výsledek sčítání hlasů).

Řešení 5.1

Dalo by se zaručit například s pomocí homomorfního šifrování (11, s. 5) - využití takové kryptografické funkce (aplikované při šifrování volebních lístků voliče), aby se dali veškeré voličské hlasy sečíst bez nutnosti dešifrace jednotlivých hlasů a tedy bez narušení atributů bezpečnosti. Tato homomorfní šifra dovoluje pracovat se zašifrovanými daty. Dešifrovalo by se až výsledné sečtení.

Důsledek 5.1.1

Kromě dosažení požadavků pro voliče 3.1 bychom dále dosáhli zaručení požadavku pro neoprávněné osoby 1.3, že tato osoba není schopna se dozvědět průběžný výsledek sčítání hlasů.

Řešení 5.2

Aby se nebylo možné dozvědět průběžné výsledky voleb, mohly by se například hlasovací lístky ukládat do různých databází. Bylo by určeno, jaké lístky patří do jaké databáze na základě nějakých dat, anebo by se mohlo určit omezení na počet záznamů v jedné databázi. Když by se tento počet naplnil, data by se začala ukládat do jiné databáze. Každá databáze by byla samostatně zašifrována jiným klíčem.

Teze 6

Vezměme si požadavky pro omezení privilegovaných osob a omezení neoprávněných osob. Týkají se přístupu do systému a k informacím. Jak můžeme zabezpečit to, aby privilegovaná osoba nezneužila svých pravomocí a neoprávněná osoba neměla možnost porušit svá omezení?

Řešení 6.1

Před tím než by se kdokoli pustil do implementace volebního systému, je potřebné nastavit si, jakou úroveň bezpečnosti chceme v systému dosáhnout. Ať by byla jakákoli, stále zůstává pár základních věcí, které by v procesu řízení přístupu do systému a k informacím neměli chybět.

Například bychom se měli určitě držet pravidla takzvaného SoD (Segregation of Duties = rozdělení pravomocí). Zjednodušeně řečeno, každá úloha, která se může vykonat ve volebním systému, by se měla rozdělit na několik dílčích podúloh a každá tato podúloha by měla být splnitelná jinou privilegovanou osobou. Tím bychom mohli například snížit riziko úniku informací, protože aby nějaká osoba dostala přístup k citlivým datům, tak by například potřebovala svolení jiných osob a tak podobně.

Dalším principem, kterým by se mělo řídit je, že každá privilegovaná osoba by měla mít jasně stanovený popis práce a odpovědností, toto by mělo být schváleno a na základě toho by měli být stanoveny, jaké přístupové pravá k různým částem volebního systému tato osoba potřebuje. Například kdyby měla osoba na starosti jenom kontrolu, jestli má volič oprávněnost k volbě, tak by měla mít přístup jenom k seznamu oprávněných voličů, nepotřebuje mít přístup například k dílčím výsledkům voleb. Samozřejmě při definování toho, kdo má mít jaké povinnosti a jaké přístupové práva, musíme uvažovat to, že do procesu administrace volebního

systému by nemělo být zahrnuto zbytečné více privilegovaných osob, než je doopravdy nutné. Protože každou osobou navíc se zvyšuje zase riziko selhání lidského faktoru.

Aby se zabránilo tomu, aby se mohla neoprávněná osoba nějakým způsobem vydávat za privilegovanou osobou, mohli bychom implementovat vícefaktorovou autentizaci a zakázat vzdálený přístup. Tedy každá privilegovaná osoba, by pro přihlášení do systému musela použit lokální přístup, kde by pro úspěšnou autentizaci kromě znalosti osobního PIN kódů, byla nutnost vlastnění identifikační karty, a navíc byl požadován také například otisk prstu, nebo jiná lidská charakteristická črta.

Také by asi stálo za uvážení časové omezení možnosti přístupu do systému pro jednotlivé privilegované osoby. Tedy kdyby se nějaká privilegovaná osoba pokoušela přihlásit do systému v dobu, v kterou to má zakázané, byl by automaticky vyvolán poplach a samozřejmě by jí byl přístup odepřen.

Teze 7

Jedním z nutných požadavků na zavedení procesu elektronického hlasování je to, aby voliči vůbec mohli, chtěli a věděli, jak provést svou volbu elektronickým způsobem. Nelze jenom předpokládat, že někteří lidé se v technických záležitostech vědí rychle zorientovat. Musíme předpokládat, že existují voliči, kteří nevědí úplně dobře, jak používat internet nebo jak si stáhnou volební aplikaci. Jak tedy vynaložit s poučením voličů o volebním procesu?

Řešení 7.1

Nejdřív bychom asi potřebovali zvýšit povědomí oprávněných voličů ohledně smyslu, výhod a záruk elektronického volebního systému (záruk například i na základě bezpečnostního auditu elektronického volebního systému nezávislým auditem). Před prvními elektronickými volbami bychom mohli také vytvořit elektronické nebo i klasické školící systémy, které by srozumitelnou formou popisovali, jak provést elektronickou volbu a demonstrovat voličům, jak bude jejich volební aplikace vypadat a jak s ní mají pracovat.

Důsledek 7.1.1

Teze 7 a její Řešení 7.1 ale trochu rozporují s požadavkem pro voliče 3.5, který zaručuje voličovi nenáročné provedení volby bez nutnosti zvláštních znalostí, protože říkají o nutnosti jisté znalosti voliče, aby mohl elektronickou volbu provést. Prakticky se tento požadavek asi nedá naplnit do detailu, protože jistá znalost práce s počítačem například, s internetem a volební aplikací je nutná. Samozřejmě by se dizajnéři volební aplikace měli snažit o co nejvíce snadno a intuitivně ovládatelnou volební aplikaci. I pro provedení papírové volby je ale nutná jistá znalost a to znalost čtení například. Záleží, co definujeme jako zvláštní znalost a jestli se nám podaří i navzdory nutnosti těchto znalostí přesvědčit voliče, aby volili takovým způsobem.

Jak je vidět, definice požadavků pro volební systém je velmi variabilní. Celková požadovaná úroveň bezpečnosti systému je dána tím, které požadavky určíme jako definiční a jakým způsobem je budeme chtít implementovat v rámci daného volebního systému. Díky této variabilitě a tomu jak jsou jednotlivé požadavky vzájemně provázané, není zabezpečení systému snadnou úlohou.

2.3 Návrhy pro zvýšení bezpečnosti

Zvýšení úrovně bezpečnosti lze dosáhnout zavedením preventivních i reaktivních protiopatření. Je potřebné kontinuálně zvyšovat efektivitu a rozsah všech bezpečnostních opatření (definována v kapitole 1.1). Sice se tato práce zaměřuje hlavně na technickou část informační bezpečnosti, uvedeme si zde výčet několika základních bodů pro jednotlivá organizačně-procesní opatření, které by se měly zvážit při návrhu, implementaci a provozu elektronického volebního systému.

Při návrhu elektronického volebního systému by se měly jasně specifikovat požadavky na udržení stanovené úrovně bezpečnosti. Pro dosažení požadované bezpečnosti by se mělo alokovat dostatečné množství kvalitních personálních interních či externích zdrojů a zvolit vhodný přístup k realizaci tohoto projektu, zejména v oblastech:

- Definování klíčových rolí v kontextu reakce na řízení rizik plynoucí z identifikovaných hrozeb.
- Nastavení systému pro efektivní řízení pravomocí a odpovědnosti pro klíčové role.
- Revize a nastavení efektivního způsobu řízení a rozsahu případné externí podpory pro provoz a rozvoj bezpečnostních technologií.
- Formy řízení a zajištění realizace organizačních a technických opatření a způsob jejich financování.

V rámci následujících opatření je potřebné řídit vyjmenované základní oblasti.

Legislativní a organizační opatření

- Definice a řízení schématu a klasifikace informačních aktiv a zacházení s citlivými informacemi v rámci systému.
- Definice a řízení bezpečnostní politiky, která bude definovat a řídit bezpečnost v rámci informačního systému. Pro jednotlivé oblasti se v ní budou nacházet odkazy na konkrétní standardy/politiky, které se zabývají již detailně danými částmi systému.
- Definice a řízení (správa, aktualizace, distribuce) procedur a směrnic pro oblasti:
  - základních bezpečnostních opatření při zpracování a výměně informací a při denním provozu informačního sytému,
  - dávkových úloh, kontroly dávkového zpracování,
  - zálohování,
  - monitoringu sítě,
  - bezpečnostního monitoringu,
  - řízení incidentů,
  - správy uživatelských přístupových oprávnění na základě správného definování a aktualizaci:
    - matice konfliktních oprávnení – SOD (Segregation of Duties - viz kapitola 1.8 Řešení 6.1),
    - autorizační matice (tabulka přirazení uživatelských oprávnění v rámci jednotlivých aplikací/systémů),
  - problematiky podpory uživatelů a provozu service desku,

- změnového řízení na všech úrovních (například i aplikační a databázové),
- správy, provozu a zabezpečení datového centra,
- testování, správu a implementaci software,
- správu hardware,
- aplikačního, databázového a procesního managementu,
- havarijního plánování (BCP – Business Continuity Plan) a obnovy systému (DRP – Disaster Recovery Plan),
- kontrolu servisních služeb od externích dodavatelů.

- Kontrola zajištění shody s legislativou a provádění pravidelného nezávislého bezpečnostního auditu informační bezpečnosti.
- Kontrola plnění a zajištění shody s právními regulacemi bezpečnostních opatření, jako je šifrování či elektronický podpis.

Logická, technická a programová opatření

- Logická bezpečnost se zaobírá návrhem a optimalizaci systému s cílem dosažení co nejdokonalejšího řízení přístupů (identifikaci, autentizaci, autorizaci) k informacím uloženým v daném systému, včetně vzdáleného přístupu, definování a správy přístupových práv, rozdělení pravomocí uživatelů, sledování a záznam činností systému a uživatelů.
- Výběr, spolehlivost a licencování hardwarového a softwarového vybavení, včetně záložních výpočetních center.
- Návrh architektury systému s aktivními i pasivními prvky – definování zabezpečení a řízení všech prvků, včetně koncových bodů (včetně mobilních zařízení).
- Dostatečně účinné potvrzovací, šifrovací a hašovací funkce a procedury na veškerých komunikačních vazbách v rámci informačního systému i komunikace s okolím, jako jsou např. telefonní linky, připojení k Internetu.
- Bezpečnost přenosu a komunikace.

Fyzická opatření

- Definovat a udržovat úroveň fyzické spolehlivosti prostředí, v němž funguje informační systém.

- Definovat plány pro případ neoprávněného vniknutí, poškození nebo zničení prostor a technických zařízení informačního systému a nosičů informací.
- Definovat a udržovat úroveň služeb ochrany a ostrahy objektů.
- Využívání automatizovaných systémů kontroly vstupu a pohybu osob v objektech – např. EZS (Elektronická Zabezpečovací Signalizace), využívaní kamerového systému.
- Ochrana proti aktivním i pasivním odposlechovým prostředkům- šumové generátory, paměťový radiový analyzátor, rušička mobilního signálu, šifrované volání.
- Způsoby ničení již nepotřebných informací nebo médií s informacemi.
- Ochrana proti požáru, ochrana proti vodě, plánování havárií a řešení krizových situací.

Personální opatření

- Zajištění personální bezpečnosti - zaobírá se především eliminací hrozeb způsobených lidským faktorem. Jde například o ochranu pracovníků jako součásti informačního systému, ale také o ochranu IS před důsledky událostí způsobených nekorektním jednáním pracovníků. Dále se zaobírá neúmyslnou i úmyslnou škodlivou činnosti osob, a to z vnějšku i zevnitř, např. chyby, krádeže, podvody nebo nesprávné užití či zneužití informací a informačního systému (poskytování informace získané v rámci pracovního zařazení třetí straně nebo směrování činnosti "své" společnosti ve prospěch třetí strany).
- Personální management – správný výběr managementu, koncových uživatelů, správců a administrátorů informačních a komunikačních systémů, vývojových pracovníků, zadavatelů veřejných zakázek a auditorů.
- Správné definování činností, odpovědností a pravomocí pracovníků informačního systému (viz kapitola 1.8 Řešení 6.1).

Vzdělávání

- Návrh bezpečnostně právního, procesního a technicko-organizačního modelu pro odborné vzdělávání managementu, koncových uživatelů, správců a administrátorů informačních a komunikačních systémů, vývojových pracovníků a auditorů.

3. Experiment volebního systému – SERVE

Tato kapitola popisuje fungování systému SERVE, kterého posouzení je nastoleno v kapitole 5.

Elektronické volby představují v tomto kontextu volby přes Internet. Vzhledem k tomu, že se tento volební systém neuchytil ve Spojených státech amerických tak, jak to bylo cílem, a tedy není používán, budeme elektronický volební systém SERVE (Secure Electronic Registration and Voting Experiment) dále označovat jen jako systém SERVE nebo projekt SERVE (15, s. 17-20).

Tento projekt byl vyvinut v roce 2004 pro primární a všeobecné volby ve Spojených státech (12, s. 5). Byl nástupcem projektu VOI (The Voting Over the Internet Pilot Project), který pro něj byl základním modelem. Projekt VOI, jako i jiné projekty, které byly určené pro elektronické hlasování, a které postupně vznikaly ve Spojených státech, nedosáhli úspěchů, jaké se od volebních systémů čekají (v projektu VOI byly zapojeny 4 státy a prvních voleb v rámci tohoto projektu se zúčastnilo jenom 84 voličů). Po zveřejnění bezpečnostních problémů projektu SERVE byl v lednu 2004 ukončen.

Důvod, proč se vznikající elektronické hlasovací systémy neujaly, je jednoduchý – je to jeden z nejzávažnějších důvodů, proč se mnoho lidí i v této době bráni používání elektronických volebních systémů. Tímto důvodem je nedosažení dostatečné úrovně zabezpečení a tedy ani spolehlivosti, které by volební systém měl svou definicí a implementací poskytovat. Žádný projekt pro elektronické hlasování, který nebyl dostatečně zabezpečen, nedosáhl úspěch a neuchytil se v praxi.

Projekt SERVE byl určen pro hlasování v celkem sedmi volebních státech, kterými byly: Florida, Washington, Hawaii, Severní Karolina, Jižní Karolína, Utah a Arkansas.

Bezpečností analýza (12, s.13) vykresluje SERVE jako systém s závažnými bezpečnostními problémy a zdůrazňuje jeho zranitelnost vůči různým útokům (např. DoS, kupování hlasů, útoky virovými nákazami), kterých využití by mohlo vést k vážným následkům v rámci procesu voleb, jako například zbavení práva hlasovat, narušení tajnosti voleb, prodávání a kupování hlasů, změna hlasů, což by také mohlo vést ke změně výsledku hlasování. Analýza uvádí, že zranitelnosti, kterými tento

systém disponuje, jsou tak fundamentální, že by se zabezpečení tohoto systému dalo pravděpodobně provést jenom celkovým re-designem nebo výměnou většiny hardwaru a softwaru, které jsou částí tohoto systému (analýza a její závěr z roku 2004). Autoři na základě své analýzy doporučovali okamžité ukončení vývoje systému SERVE.

V systému SERVE je možné hlasovat jakýkoli den v průběhu 30 dnů před dnem voleb až po stanovený čas v den voleb, kdy se volby končí. Tato delší doba pro možnost vykonání volby může působit pozitivně pro voliče, protože mají pro vykonání volby větší rozmezí. Systém má dále následující vlastnosti:

- Každý subjekt, který chce (a má právo) provést volbu v rámci projektu SERVE elektronickým způsobem, se musí nejdříve přihlásit do programu.
- Po přihlášení má subjekt povinnost se zaregistrovat jako volič a při této příležitosti je voličovi přiděleno identifikační číslo a PIN (chce-li volič provést volbu).
- Každý oprávněný volič má po provedení úspěšné registrace právo provést hlasování pouze jednou.
- V rámci tohoto systému neexistuje možnost změny již jednou úspěšně provedené volby a to dokonce ani volbou provedenou papírovým způsobem.
- V případě útoku či proniknutí do volebního systému má určená privilegovaná volební komise právo volby ukončit a všechny již odevzdané hlasy zrušit.

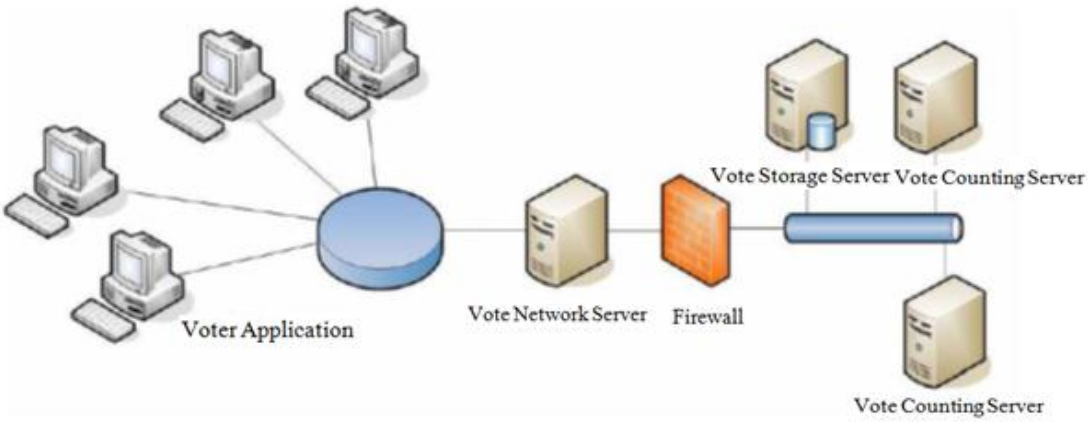
3.1 Systémová architektura

Systémová architektura systému SERVE (15, s. 17-20) pozůstává z několika vzájemně provázaných komponent. Volební server je přímo přístupný z Internetu, ale Úložní server a sčítací server jsou umístěny za firewallem. Všechny komponenty jsou zapojeny online do sítě. Hlavní prvky systémové architektury SERVE jsou následující:

- volební aplikace (Voter Application),
- centrální systém,

- volební server (Vote Network Server),
- úložní server (Vote Storage Server),
- sčítací server (Vote Counting Server).

Na následujícím obrázku jsou znázorněny jednotlivé komponenty systému SERVE a jejich vzájemné komunikační vazby.



Obrázek 12 Architerkura SERVE

BERGER, Josef. Elektronický systém voleb a hlasování (E-voting) [online]. 2012 [cit. 2013-03-02]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/bergejos_2012dipl.pdf. Diplomová práce. České vysoké učení technické v Praze. Vedoucí práce Ing. Leoš Boháč, Ph.D

Bližší popis fungování jednotlivých komponent systému SERVE je následující.

3.1.1 Volební aplikace

První komponentou, které funkčnost a význam si přiblížíme, je volební aplikace. Je to jediná komponenta v rámci této systémové architektury, která je používána širokou veřejností. Je to webová aplikace, která je spouštěna na počítači voliče a která tedy pracuje s uživatelem interaktivně.

Šifrování a autentizace se provádí prostřednictvím SSL protokolu, který zabezpečuje komunikaci mezi volební aplikaci a volebním serverem.

Volební aplikace systému SERVE může běžet jenom na počítačích s operačním systémem Microsoft Windows. Není tady žádná multiplaformnost, což

by mohlo pro voliče znamenat jisté omezení. Proč by měli voliči ve volbách, kde by byl zaveden tento systém, být omezení tímto operačním systémem a těmito prohlížeči?

Dále je nutno použít webový prohlížeč Internet Explorer[30] (IE) nebo Netscape.

Internet Explorer je sám o sobě zranitelný. Kromě toho, že je znám laxním dodržováním webových standardů (což se poslední dobou zlepšuje), jeho doplňky jsou založeny na prvku ActiveX. Jde o malé soubory kódu, které lze stáhnout a spustit na počítači. Jsou často zneužívány k virovým útokům. Po stažení se stávají součástí operačního systému se schopností manipulace s hardware i software počítače. To, že je architektura IE kritizovaná a náchylná k chybám, je vidět i na celkovém průběhu její vývoje, kde se každým rokem objevují nové a nové zranitelnosti.

Netscape měl svého času dominantní postavení ve světě webových prohlížečů, ale neudržel krok s konkurencí a jeho podíl časem klesl na minimum. Kvůli útlumu vývoje, je zabezpečení proti moderním hrozbám nedostačující, což činí tento prohlížeč v dnešní době prakticky nepoužitelným.

Aby mohl volič správně využít volební aplikace, musí být daný webový prohlížeč nakonfigurován tak, aby povoloval Javu nebo ActiveX prvky a Javascript. Také musí být povolené cookies. Tyto technologie jsou považovány za zranitelné a mohou představovat riziko pro bezpečnost voličova zařízení.

Javascript je moderní a stále více používaný programovací jazyk WWW stránek, obvykle používán pro ovládání různých interaktivních prvků (tlačítka, textová políčka) nebo animací, či obrázkových efektů. Kvůli své dynamické povaze a expresivní síle, kterou disponuje, si čím dál tím více utužuje své postavení v internetovém světě. Při práci s Javascriptem je nutná opatrnost. Umožňuje útoky, jako jsou Cross-site scripting a Cross-site request forgery (popis jak by takový útok pomocí Javacsriptu a cookies mohl probíhat lze nalézt v kapitole 1.4.8).

Když má volič k dispozici veškeré výše zmíněné vybavení (a nastavení), potřebné pro provedení elektronické volby, pak by měl být schopen přihlásit se přes internet do volební aplikace pomocí přiděleného identifikačního čísla a PIN kódu

[30] Internet Explorer je webový prohlížeč společnosti Microsoft integrován do operačních systémů Windows.

(přiděleno při registraci, kterou musí podstoupit každý volič, který chce provést volbu). Autentizace voliče probíhá ověřením jeho jména vůči příslušným registračním záznamům.

Po úspěšné autentizaci je voličovi zobrazen na obrazovce seznam kandidátů voleb a on je oprávněn provést svou volbu zvolením jím vybraného kandidáta. Volební aplikace pak zvoleného kandidáta, tedy voličův hlas, zašifruje asymetrickou funkcí pomocí veřejného klíče systému SERVE. Spolu s hlasem voliče se zašifruje i náhodné číslo – to je kvůli tomu, že kdyby si útočník zašifroval pomocí volebního klíče systému SERVE všechny možné volby (které mohou voliči provést), a kdyby se někde v rámci systému dostal k zašifrovaným volebním lístkům voličů, tak by porovnáním těchto zašifrovaných lístků s těmi, které si vytvořil sám, mohl zjistit, který volební lístek vznikl zašifrováním které volby. V případě, že by útočník zjistil provázání daného volebního lístku s voličovým identifikátorem, znamenalo by to narušení tajnosti voleb. Kdyby měl možnost útočník například mazat tyto lístky, tak by věděl, které má vymazat, aby to bylo podle jeho preferencí.

Aplikace následně pošle volebnímu serveru tento zašifrovaný volební lístek a identifikační údaje voliče.

3.1.2 Centrální systém

Centrální systém se skládá z následujících částí.

3.1.2.1 Volební server

Volební server (Vote Network Server) je webový server a je přímo přístupný z Internetu. Komunikuje s volební aplikací a s úložním serverem.

Má na starosti zpracovávání autentizačních požadavků. Přijímá tedy identifikační údaje o voličích. Volební server dále přijímá od voličů zašifrované hlasovací lístky a ověřuje korektnost všech přijatých dat. Po ověření tato přijatá data (identifikační údaj a volební lístek) zašifruje soukromým klíčem systému SERVE a přeposílá na úložní server.

Když úložní server zjistí, že volič nemůže volbu vykonat (volič již provedl jednu úspěšnou volbu nebo volič nemá oprávnění provést volbu), přepošle tuto informaci volební aplikaci, která ji zobrazí voliči.

V případě úspěšné autentizace volební server zobrazí voliči seznam kandidátů voleb, aby mohl provést svou volbu.

3.1.2.2 Úložní server

Úložní server (Vote Storage Server) přijímá od volebního serveru zašifrovaná data a následně je dešifruje pomocí soukromého klíče systému SERVE a oddělí identifikační údaje voliče od volebního lístku voliče.

Úložní server ověřuje právo k vykonání volby, tedy jestli je volič registrován a jestli ještě neprovedl úspěšnou volbu a na základě toho přiděluje právo přístupu. Opatření proti vykonání dvojí volby od toho samého oprávněného voliče probíhá na základě seznamu identifikačních údajů voličů, kteří již volbu provedli, který si tato komponenta udržuje aktuální v průběhu celého trvání elektronických voleb. V případě, že volič již hlasoval, informuje úložní server voliče o tomto faktu zprávou prostřednictvím volebního serveru – pošle voličovi tzv. *Response* s potřebnou informací a ukončí volební proces (zruší přijatý volební lístek). V případě, že se volič nezaregistroval, je proces podobný. Úložní server tedy pošle uživateli *Response* s potřebnou informací a ukončí volební proces.

V případě, že se volič zaregistroval a ještě neprovedl úspěšnou volbu, úložní server informuje voliče zprávou *Response* s příslušnou informací o tom, že byl jeho hlasovací lístek úspěšně přijat a uložen. Pak ukončuje komunikaci.

Po dešifrování přijatých dat se tato citlivá data (volební lístek a identifikační údaje voliče) nachází po krátkou dobu na úložním serveru v nezabezpečeném formátu, až dokud server volební lístek znova nezašifruje pomocí veřejného klíče příslušného sčítacího serveru.

Dalším krokem je, že si úložní server uloží zašifrovaný hlasovací lístek, zašifrovaný veřejným klíčem takového sčítacího serveru.

Takto zašifrované hlasovací lístky a seznam voličů, kterým patří tyto hlasovací lístky, se posílají online po zabezpečeném komunikačním kanále sčítacím serverům. Přenos jednotlivých volebních lístků a seznamu voličů probíhá opakovaně a komunikaci zahajují jednotlivé sčítací servery.

3.1.2.3 Sčítací server

V systému SERVE se nachází několik sčítacích serverů. Jsou nazývané také Lokální volební úřady (Local Election Offices). Každý sčítací server přímo

komunikuje s úložním serverem a přijímá od něj potřebná data (volební lístky a seznamy voličů, kterým tyto volební lístky patří).

Každý volební okrsek (například stát, nebo nějaký menší celek), který se účastní daných voleb, má vlastní sčítací server. Každý sčítací server si vygeneruje pro účely voleb jeden pár volebních klíčů - veřejný a soukromý klíč sčítacího serveru. Veřejný klíč sčítacího serveru používá úložní server pro zašifrování volebních lístků voličů z daného volebního okrsku (kapitola 3.1.2.2). Tím se zaručí, že daný volební lístek voliče z daného volebního okrsku bude moci být dešifrován pomocí soukromého klíče jenom sčítacím serverem v daném volebním okrsku.

Úkolem každého sčítacího serveru je pravidelné připojování se zabezpečeným komunikačním kanálem k úložnímu serveru a následné dotazování se na seznam voličů a nové zašifrované volební lístky. Tyto data jsou danému sčítacímu serveru po úspěšné autentizaci zaslány. Po přijetí dat sčítací server ověří jejich totožnost, potvrdí úložnímu serveru jejich příjem a ukončí s ním komunikaci.

Každý sčítací server si udržuje seznam voličů, který dostal od úložního serveru.

Pro sčítání hlasů je potřebné, aby si úložní server dešifroval přijaté volební lístky pomocí svého privátního klíče a následně ověřil korektnost dat ve volebním lístku. Nesprávné hlasy jsou pak vyřazeny a správné hlasy jsou započteny (proces sečtení je možné provádět opakovaně, aby se minimalizovalo riziko vzniku chyb v průběhu sčítání hlasů).

3.1.3 Logování a audit

V procesu elektronických voleb v rámci systému SERVE se nevytváří žádné auditní logy. Na jedné straně se takovým způsobem nevytváří provázání mezi identifikačními údaji voliče a jeho volebním lístkem, ale na druhé straně to znemožňuje jakoukoli propracovanější auditovatelnost. Tedy vystopování toho, co se v daném systému s volebním lístkem děje není možné. Nelze například ověřit, jestli se hlas určitého voliče zúčastnil sčítání hlasů.

Co se v rámci systému dá dohledat, jak již bylo načrtnuto výše, je to, že úložní server i jednotlivé sčítací servery si ukládají seznamy voličů, kteří volbu provedli. Je tedy možné ověření, jestli volič již volbu provedl a jestli se jeho volební lístek

nachází jenom na úložním nebo již i na sčítacím serveru (neznamená to ale, že byl započten, jenom že byl přenesen). Toto je umožněno díky tomu, že každý sčítací server dostane od úložního serveru volební lístky i s příslušným seznamem voličů, kteří volbu provedli. Jednotlivé volební okrsky jsou tedy schopny zkontrolovat seznam voličů, kteří mají uložen lokálně vůči tomu seznamu voličů, který je uložen na úložním serveru.

4. Elektronické volby v Estonsku

Tato kapitola popisuje fungování elektronického volebního systému v Estonsku, kterého posouzení je nastoleno v kapitole 5.

Elektronické volby zůstanou i nadále pod pojmem voleb přes Internet (ne voleb pomocí speciálního volebního elektronického přístroje). Takové volby představují v Estonsku (15, s. 9-16) v praxi zavedenou možnost volby jiným způsobem, než papírovým.

Tyto volby jsou v Estonsku úspěšně již 7 let a tato země byla první, která realizovala elektronické volby v takovém rozsahu (17, s. 2-5). V roce 2003 se začal v Estonsku postupně vyvíjet volební systém přes Internet označovaný jako Estonian E-Voting System (dále jen EstEVS). Elektronické volby byly poprvé zavedeny v roce 2005 v lokálních volbách. Více než 9000 voličů vyjádřilo svou volbu přes Internet (byly to přibližně dvě procenta z celkového počtu zúčastněných voličů v těchto volbách).

Doposud proběhlo v Estonsku 5 elektronických voleb přes Internet – lokální volby v roce 2005, parlamentní volby v roce 2007, volby do Evropského parlamentu a lokální volby v roce 2009 a parlamentní volby v roce 2011. Ze statistik ohledně počtu zúčastněných voličů vyplývá, že každým rokem tento počet rostl. Například ve volbách v roce 2011 bylo již 140 tisíc hlasů odevzdáno elektronicky, což tvoří 24,3 procent ze všech odevzdaných hlasů v průběhu těchto voleb.

Můžeme říct, že elektronický volební systém v Estonsku představuje možnost volby jednodušším způsobem, než je papírový způsob. Tento volební systém zaručuje soulad s volebními principy a volební legislativou.

Elektronické volby jsou tajné, spolehlivé a auditovatelné. Další požadavky pro volební systém EstEVS jsou následující - oprávnění voliči mají možnost provést elektronickou volbu (zde vidíme souvislost s požadavkem pro voliče 1.1 z kapitoly 2.1), každý oprávněný volič má jeden platný voličský hlas (zde máme souvislost s požadavky pro voliče 3.2 a 3.3), volič provádí volbu sám za sebe (to je požadavek pro voliče 2.1), svobodně a bez nátlaku (požadavek pro voliče 3.4), volič nesmí být schopen prokázat, jak volil (volby jsou tajné; souvislost s požadavkem pro voliče 3.1 a pro neoprávněné osoby 1.2). Použití cizích identifikačních karet (nebo mobilních

ID) pro volební účely je zakázáno (požadavek pro voliče 2.1). Podněcování voliče k elektronickému hlasování nabízením počítače pro tento účel, nebo ovlivňování voličů jiným způsobem je zakázáno. Také se zakazuje organizování kolektivních volebních akcí (např. otevření takzvaných „e-hlasovacích“ kanceláří), protože to může být považováno za porušení svobody hlasování. Myslí se tím pravděpodobně to, že by se tyto kanceláře mohly nést v duchu preferencí určitého volebního názoru a mohly by tak přímo nebo nepřímo na poslední chvíli ovlivnit osobní voličský názor jednotlivých voličů, kteří by do takové kanceláře přišli volit (možná že by totiž neměli jinou možnost, protože například nevlastní zařízení, ze kterého by mohli elektronickou volbu provést). Toto omezení na nabízení zařízení pro provedení volby mohlo být stanoveno i kvůli tomu, že tato zařízení by mohla být úmyslně, či neúmyslně poškozena/infikována/nezabezpečena (mohl by nastat rozpor se zárukami pro voliče 3.1, 3.2, 3.3 nebo 3.4). V procesu EstEVS je rovněž stanoveno, že Estonská národní volební komise má právo zastavit proces elektronické volby a zneplatnit výsledek voleb (zde vidíme vazbu na požadavky pro privilegované osoby 1.4 na administraci volebního systému).

Dle Estonské volební legislativy (14, s. 7-9) je délka průběhu elektronických voleb stanovena na 7 dní (rozdíl oproti projektu SERVE – 30 dní – je poměrně marginální). Volby začínají 10 dní před začátkem definovaného dne voleb, končí 4 dny před stejným dnem a jejich základní popis je následující:

- V dny učené pro elektronické volby má volič možnost volit elektronickým způsobem na webové stránce Národní volební komise.
- Volič musí volit sám za sebe.
- Volič se musí autentizovat pomocí svého certifikátu.
- Po úspěšné identifikaci se voličovi zobrazí konsolidovaný seznam kandidátů.
- Volič zvolí ze zobrazeného seznamu kandidátů jméno toho, kterého si přeje volit a potvrdí svou volbu elektronickým podpisem (zvýšená bezpečnost z hlediska integrity, protože podepsaná data je nereálné změnit pro útočníka, když nezná voličův privátní klíč).
- V případě, že všechno proběhlo v pořádku, zobrazí se voličovi zpráva, že jeho volba byla započtena.

- Pro zvýšení pravděpodobnosti toho, že volič při volbách vyjádří svou vůli, má volič právo na změnu svoji elektronicky provedené volby dvěma způsoby s tím, že se započte poslední správně provedená volba.

  Způsoby změny již podaného volebního hlasu:
  - Provedení nové volby elektronickým způsobem (elektronická volba musí být provedena v čas určený pro provádění elektronických voleb, a to je 10 až 4 dny před dnem voleb).
  - Provedení nové volby papírovým způsobem v termínu 6 až 4 dny před dnem voleb.
- Po ukončení možnosti provádění elektronické volby se na volební okrsky zašlou ucelené a konečné seznamy voličů, kteří provedli úspěšnou elektronickou volbu. Je důležité, aby přenos tohoto seznamu byl dostatečně zabezpečen, tedy aby byla zaručená hlavně integrita dat při přenosu. V případě úspěšného přenosu na jednotlivé volební okrsky odešlou potvrzení s důkazem o přijetí. Na těchto stanicích se pak připravují takzvané výzvy ke zrušení elektronické volby pro ty voliče, kteří volili elektronicky a také volili papírově. Tento proces vytváření výzev se končí nejpozději ve 12 hodin v den voleb. Informace o dvojí volbě se zasílá Národní volební komisi, která zruší dané elektronicky vykonané volby.

Estonský volební systém je koncipován tak, že nemá speciální registrační fázi. Tedy voliči, kteří chtějí hlasovat elektronicky, nejsou povinni se jít zaregistrovat na určené místo. Stačí, když požádají elektronickou volební službu o hlasování. Při požádání je každý uživatel identifikován a autorizován, a to jedním z následujících způsobů možné identifikace voliče v rámci EstEVS:

1. Identifikace ID kartou - Potřebné vybavení pro voliče, který se rozhodl volit elektronickým způsobem, touto formou identifikace, je následující:
   - počítač s přístupem na Internet (volič přistupuje přes Internet k aplikaci, prostřednictvím které provede svou volbu),

- ID karta (v nové nebo staré verzi – toto pravděpodobně nedělá problém občanům Estonska, protože k datu 08.03.2013 bylo téměř 1,2 milionů aktivních karet, což je více než 90% občanů Estonské republiky [18],
- podpisový certifikát (obsahuje veřejný klíč, určen pro podepisování; je součástí ID karty; v případě neplatnosti certifikátu si jej volič může obnovit přes Internet),
- čtečka ID karet (znamená pořídit si tuto čtečku – nemusí to na voliče působit komfortně),
- specializovaný software pro možnost použití ID karty (lze jej nainstalovat pomocí Internetu – hrozba stáhnutí škodlivého kódu),
- a PIN kód (v případě potřeby si může volič požádat o nový PIN na místech k tomu vyhrazených - což je zase nevýhoda, protože to snižuje komfort pro voliče, na druhou stranu to ale můžeme považovat za jistý bezpečnostní prvek, který je pravděpodobně na místě).

Tyto ID karty jsou občany v Estonsku běžně používány pro ověřování identity (např. při vyřizovaní půjček nebo hypoték). To znamená, že kromě občana, který vlastní tuto kartu, s ní pracuje i mnoho dalších lidí, kteří tuto identitu ověřují. To může znamenat riziko odcizení citlivých dat – například certifikátů, která jsou uložená na této kartě).

2. Identifikace pomocí Digi-ID. Je to dokument, kterým se volič identifikuje v elektronickém prostředí a je pomocí něho schopen vytvořit elektronický podpis. Vypadá jako ID karta, ale bez fotky (není tedy možná vizuální identifikace subjektu na rozdíl od ID karty, což ale v procesu elektronické volby nevadí). Potřebné vybavení je stejné jako v případě provádění elektronické volby pomocí ID karty zmíněné výše.
3. Mobilní ID (umožněno v rámci EstEVS od roku 2011) - Potřebné vybavení pro voliče, který chce volit elektronickým způsobem, touto formou identifikace, je následující:
   - počítač s přístupem na Internet (volič přistupuje k aplikaci, prostřednictvím které provede svou volbu),
   - mobilní telefon (pomocí SMS se doručí voliči potvrzující PIN kódy),
   - Mobilní ID SIM karta,
   - podpisový certifikát,

- a PIN kód.

Není potřebná instalace čtečky karet ani žádného speciálního software. Mobilní telefon zastupuje funkci ID karty i čtečky karet, což může působit na voliče velmi komfortně. Na druhé straně nemáme žádný firewall nebo jinou SMS filtrovací ochranu. Je patrně těžké předvídat SMS útok a nesmíme zapomínat na velkou dávku nejistoty v tom, jestli byla SMS zpráva doručena svému příjemci či nikoli, nebo jestli mu byla doručena zpráva od odesilatele, nebo od útočníka, který zprávu od odesilatele pozdržel a například pozměněnou původní zprávu poslal příjemci. Ne jenom neznámý útočník, ale také mobilní operátoři mají možnost pozdržet nebo pozměnit SMS zprávu, která se posílá. Nebo by útočník například mohl odpojit mobilní telefon od telefonní sítě.

Chytré telefony v dnešní době nemůžeme celkově považovat za bezpečné, protože trend je zatím takový, že chytrý telefon s připojením na Internet se sice používá v každodenním životě, ale uživatele na ně zatím neaplikují žádná nebo nedostačující speciální bezpečnostní pravidla, nemají nejnovější verzi operačního systému, který může obsahovat nové bezpečnostní prvky, nebo vlastní zařízení, které samo o sobě obsahuje mnoho zranitelností. Uživatele stahují různé aplikace a tak by pravděpodobně nebyl problém pro útočníka naprogramovat nějakou aplikaci, která bude působit nevinně, ale po instalaci na mobilní telefon by mohla napomoct útočníkovi v naplnění jeho zájmů neslučitelných s cílem voleb.

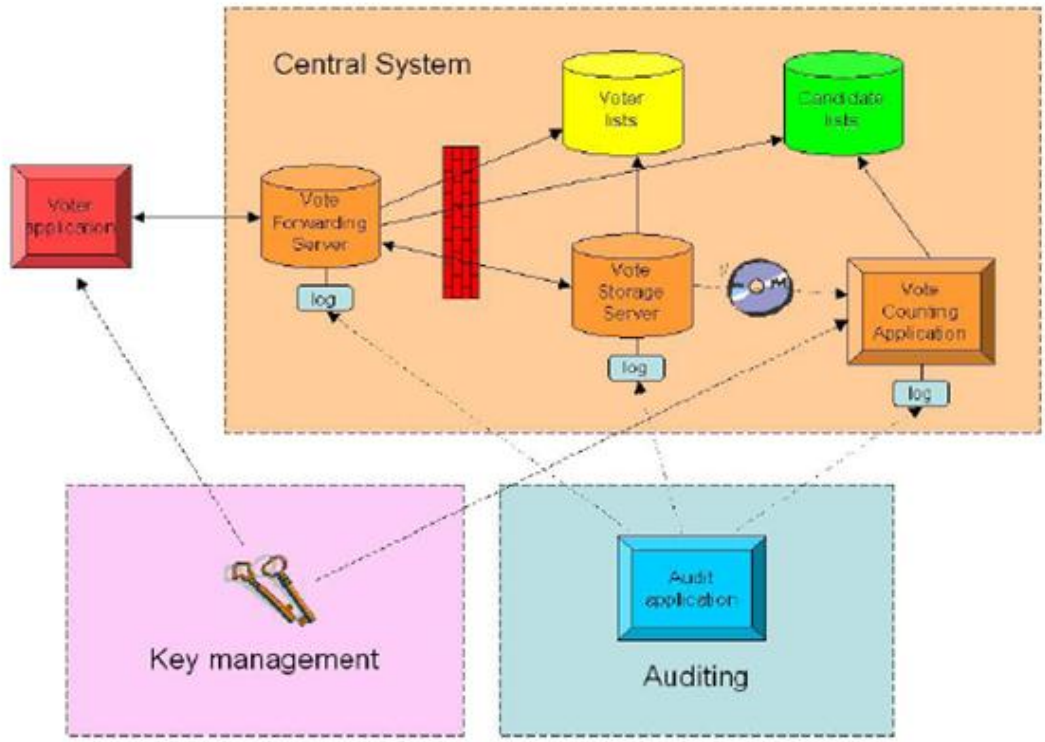
4.1 Systémová architektura

Systémová architektura Estonského elektronického volebního systému se skládá z několika vzájemně provázaných komponent. Základní komponenty se dělí na části přístupné z Internetu a na takové části architektury, které nejsou přístupné z Internetu a jsou bezpečněji umístěné za firewallem. Nejvíc chráněnou komponentou je sčítací aplikace, která je používaná dokonce off-line. Volební lístky se do ní přenášejí na externím off-line úložném médiu. Neodmyslitelnými částmi sytému EstEVS jsou management klíčů a auditing. Stojí topologicky mimo centrální

systém, ale zasahují v podstatě do všech etap procesu voleb. Definice systémové architektury EstEVS je následující (14, s. 10-20):

- volební aplikace (Voter application),
- centrální systém (Central System),
  - volební server (Vote Forwarding server, také známo pod názvem Network Server),
  - úložní server (Vote Storage Server),
  - sčítací aplikace (Vote Counting application, také známo pod názvem Vote Counting Server),
- management klíčů (Key management)
- a auditing.

Na následujícím obrázku 13 jsou znázorněny jednotlivé komponenty EstEVS a jejich vzájemné komunikační vazby. Je zřejmé, které komponenty používají pro svou práci seznam oprávněných voličů (Voter list) a seznam kandidátů voleb (Candidate list).



Obrázek 13 Architektura EstEVS

Následuje bližší popis fungování jednotlivých komponent volebního systému, jejich provázanost a procesní závislost.

4.1.1 Volební aplikace

První komponentou, které funkčnost a význam si přiblížíme, je volební aplikace. Je to jediná komponenta v rámci systémové architektury EstEVS, která je používaná širokou veřejností (jak to bylo i při projektu SERVE). Jedná se o webovou aplikaci, která pracuje s uživatelem interaktivně. Používání volební aplikace jako online webové aplikace může zaprvé představovat jisté riziko provázání voliče s jeho volebním hlasem a zadruhé by to mohlo být zneužito například MITM útokem.

Šifrování se provádí prostřednictvím SSL protokolu, který zabezpečuje veškerou komunikaci mezi volební aplikaci a volebním serverem. EstEVS volební aplikace může běžet na počítačích s operačními systémy Windows, Linux i MacOS. V případě použití OS Windows je nutno použít webový prohlížeč Microsoft Internet Explorer[31].

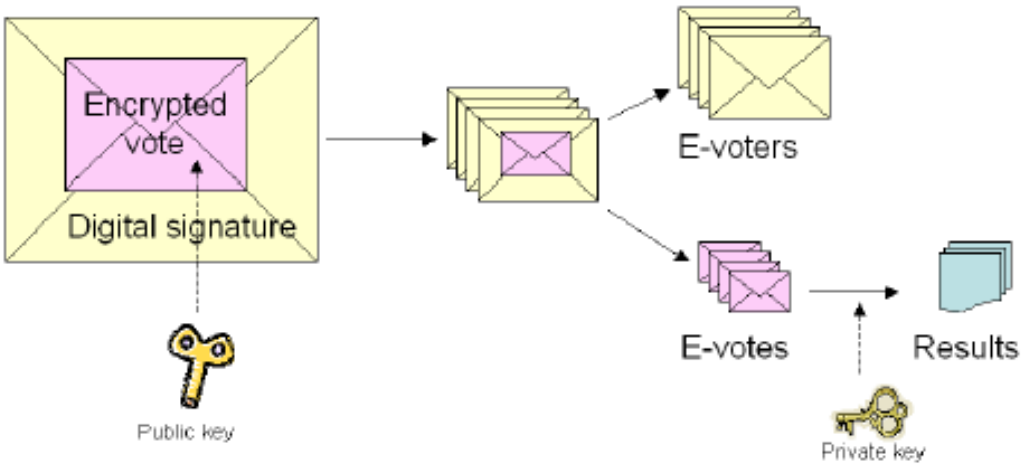
Multiplatformní použití je výhodné pro uživatele (pro voliče není jistě příjemné, že proto, aby mohl volit, musí mít nějaký speciální operační systém na svém osobním zařízení), což by mohlo na druhou stranu vést ke zvýšení různorodosti útoků na různé platformy. Tedy kdyby to bylo zabezpečeno například pro operační systémy Windows (i když o stoprocentním zabezpečení ani nelze uvažovat, protože, jak vidíme v každodenním životě, nové a nové zranitelnosti se objevují v průběhu celého roku, a to ještě nevíme o těch nezveřejněných), neznamenalo by to, že by tím byly pokryty i zranitelnosti řekněme pro Linux.

Předpokládejme, že volič má k dispozici veškeré výše zmíněné hardwarové i softwarové vybavení, potřebné pro provedení elektronické volby. Volič je tedy, po úspěšném přihlášení do volební aplikace, schopen prohlídnout seznam oprávněných voličů a následně možnost provést svou volbu. V případě, že tak volič vykoná,

[31] Zranitelnosti IE již zmíněny v kapitole 3.1.1.

volební aplikace se ho před dalším zpracováním této volby dotáže, jestli ji chce potvrdit. V případě, že volič potvrdí svou volbu, aplikace ji zašifruje pomocí veřejného klíče volebního systému, který je integrován ve volební aplikaci. Spolu s hlasem voliče se zašifruje náhodné číslo – podobně, jak to bylo v systému SERVE v kapitole 3.1.1. Zašifrovaný volební lístek (E-vote, také nazýván Encrypted vote) představuje vnitřní obálku hlasovacího lístku. Tento zašifrovaný volební lístek se následně potvrdí elektronickým podpisem (Digital signature) pomocí privátního klíče voliče. Každopádně by tento elektronický podpis neměl chybět v tomto procesu, protože zaručuje autenticitu volebního lístku. Elektronický podpis tedy představuje vnější obálku hlasovacího lístku. Zašifrovaný a podepsaný hlas pošle volební aplikace volebnímu serveru.

Zmíněný princip (16, s. 41 - 44) použití vnitřní a vnější obálky je znázorněn na následujícím obrázku.



Obrázek 14 Použití dvou obálek

ESTONIAN NATIONAL ELECTORAL COMMITTEE. E-Voting System: General Overview [online]. Tallin, 2010 [cit. 2013-03-02]. Dostupné z: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf

4.1.2 Centrální systém

Centrální systém je v Estonsku pod správou Národní volební komise, je celkem robustní a komplexní, podívejme se ale blíže na fungování jednotlivých komponent, které jej tvoří.

4.1.2.1 Volební server

Volební server je webový server a je to jediný server v rámci centrálního systému, který je přímo přístupný z Internetu. Volební server komunikuje s volební aplikací a s úložním serverem. Pro svou práci používá seznam oprávněných voličů a seznam kandidátů voleb. Má na starosti autentizaci voliče (ověřuje právo volit s pomocí seznamu oprávněných voličů). Když je autentizace neúspěšná, doručí voliči upozornění, v opačném případě posílá na úložní server dotaz, jestli již volič provedl volbu. Odpověď na dotaz je přeposlána voliči a v případě, že volič již volil, je mu umožněno provést volbu znovu. Volební server zobrazuje voliči kandidáty voleb, přijímá zašifrované a elektronicky podepsané hlasovací lístky a ověřuje jich formální správnost. Volební server také ověřuje, jestli identifikace voliče, kterou mu poskytne elektronický podpis z hlasovacího lístku, odpovídá identifikaci vlastníka spojení, které má vytvořené s voličem. V případě pozitivního ověření přepošle elektronický hlasovací lístek na úložní server. Po dokončení hlasování server ukončuje veškerou komunikaci.

4.1.2.2 Úložní server

Úložní server je server, který je umístěn za firewallem ve vnitřní síti centrálního systému. Komunikuje s volebním serverem. Pro svou práci používá seznam oprávněných voličů.

První úlohou úložního serveru, po tom co přijme od volebního serveru hlasovací lístek, je ověření platnosti certifikátu voliče, kterému patří tento hlasovací lístek, a tedy se pokouší provést volbu. Když je certifikát neplatný (nebo když volič nemá právo volit), volič není oprávněn vykonat volbu.

Pro tento účel komunikuje úložní server s dedikovaným serverem, který zjišťuje platnost certifikátů. Je to jediný server, který je potřebný v procesu elektronických voleb a není součástí centrálního systému. Je pod správou AS Sertifitseerimiskeskus (Estonská primární certifikační autorita) a poskytuje tuto základní službu ověření prostřednictvím protokolu OCSP[32] (Online Certificate Status Protocol) (více v [1]).

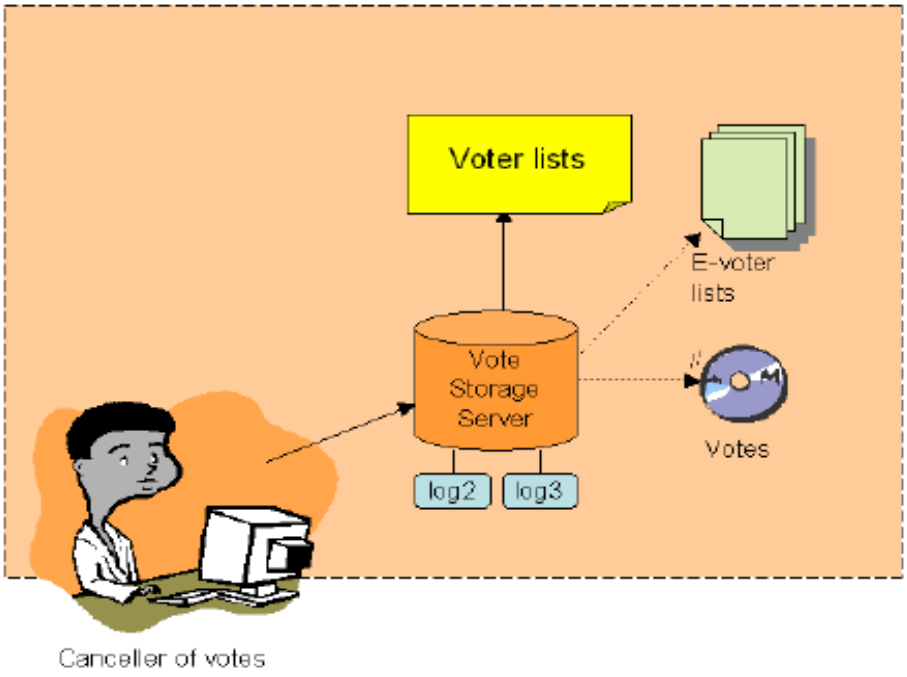
[32] OCSP (Online Certificate Status Protocol) je schéma pro udržení bezpečnosti serveru a ostatních síťových zdrojů. Shromažďuje informace o stavech certifikátů. Z jisté části nahradila fungování revokačních listů certifikátů CRL (viz kapitola 1.3.3).

V případě, že se voličovi podařilo hlasovat úspěšně, pošle úložní server potvrzení *Response* volebnímu serveru, tato zpráva je také doručena voliči. *Response* je textový soubor, který obsahuje informaci o přijetí hlasovacího lístku. Nakonec je přijatý zašifrovaný a podepsaný hlasovací lístek uložen s voličovými identifikačními údaji *PIC* (Personal Identification Code) do logovacího souboru LOG1 (logovací soubory LOG se používají pro logování jednotlivých hlasovacích lístků v různých stádiích jejich putování volebním systémem a jsou podrobněji popsány při definici komponenty management klíčů).

Po ukončení možnosti elektronického hlasování, se hlasovací lístky seřadí podle data přijetí a provede se kontrola na dvojité hlasy, jsou tedy odstraněny duplicitní hlasovací lístky (v případě, že volič volil vícekrát, započte se jenom poslední správně provedená volba a ostatní se zneplatní) a zruší se volební lístky od neoprávněných voličů. Seřazení hlasů zajišťuje ponechání poslední správně provedené volby. V případě zrušení nějakého hlasovacího lístku je zaznamenaná tato akce do logovacího souboru LOG2 spolu s důvodem zrušení daného hlasu.

Nakonec oddělí úložní server vnitřní a vnější obálku hlasovacího lístku (tedy identifikace voliče v podobě elektronického podpisu je oddělena od zašifrovaného hlasu voliče). Elektronické podpisy jsou uloženy odděleně bez obsahu (*E-Voter lists*). Volební hlasy jsou přeneseny do sčítací aplikace off-line na externím médiu *(Votes),* např. DVD. Každý volební okres má přiděleno jedno externí médium. Všechny volební zašifrované lístky, které se pronáší do sčítací aplikace, jsou uloženy do logovacího souboru LOG3.

Seřazení a rušení hlasů je znázorněno na následujícím obrázku.



Obrázek 15 Seřazení a rušení hlasů

ESTONIAN NATIONAL ELECTORAL COMMITTEE. E-Voting System: General Overview [online]. Tallin, 2010 [cit. 2013-03-02]. Dostupné z: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf

4.1.2.3 Sčítací aplikace

Sčítací aplikace je pro dosažení vyšší bezpečnosti off-line komponentou (oddělením od sítě se snižuje riziko potenciálního útoku nejenom z externích, ale i z interních sítí). Data, která jsou zpracovávaná sčítací aplikací, se doručí na off-line fyzickém úložním médiu. Aplikace používá seznam kandidátů voleb, který je uložen v její lokální databázi.

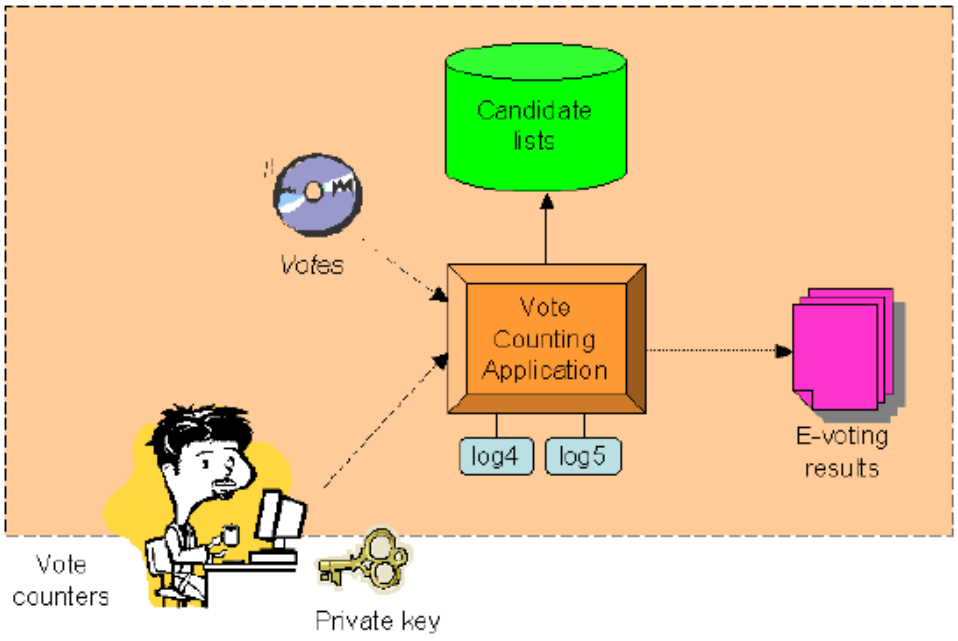
Sčítací aplikaci jsou na začátku její práce předány zašifrované hlasy, které jsou zbaveny elektronického podpisu. Tím se zajišťuje anonymita při sčítání hlasů (komponenta nepozná spojení mezi voličem a jeho volbou). Volební hlasy jsou již seřazeny úložním serverem. Pro dešifrování hlasů se používá privátní klíč volebního systému. Tento privátní klíč (je možné, že privátních klíčů je generováno a použito víc) se aktivuje určenými manažeři pro správu klíčů (také nazývaných Vote counters) podle metodik managementu klíčů (viz kapitola 4.1.3). Sčítací aplikace dále ověří, jestli formát dešifrovaného volebního lístku odpovídá pravidlům voleb. Neakceptovatelné volební lístky jsou uloženy do logovacího souboru LOG4 a nejsou do sčítání zahrnuty. Dešifrované hlasy aplikace porovná vůči seznamu kandidátů (*Candidate list* – viz obrázek 16) a ověří, zda je možné pro daného kandidáta

hlasovat (tedy jestli zvolený kandidát patří do volebního okrsku příslušnému danému voliči). V případě, že bylo hlasováno pro kandidáta, který není na daném seznamu kandidátů, se tento volební lístek také neakceptuje a je uložen do logovacího souboru LOG4.

Výstupem procesu této komponenty je výsledek sečtení správně podaných hlasovacích lístků elektronických voleb *(E-voting results)*, který je předán do běžného papírového hlasování. Všechny volební lístky, které byly započteny, jsou uloženy do logovacího souboru LOG5. Výsledky elektronického hlasování se berou v potaz spolu s výsledky papírového hlasování a jejich spojením se dosáhne celkového výsledků voleb (jestli volič provedl elektronickou volbu i papírovou volbu, započítá se jenom jeho hlas, který odevzdal klasickým papírovým způsobem).

Je žádoucí, aby fáze sčítání hlasů byla opakovatelná. Provádí se opakovaná ověření sčítání hlasů na různých hardwarech, pro zajištění celkové bezchybnosti výsledku sčítání volebních lístků.

Sčítací aplikaci, její procesy a komponenty, které potřebuje k výkonu své činnosti, znázorňuje následující obrázek.



Obrázek 16 Sčítací fáze

ESTONIAN NATIONAL ELECTORAL COMMITTEE. E-Voting System: General Overview [online]. Tallin, 2010 [cit. 2013-03-02]. Dostupné z: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf

4.1.3 Management klíčů

Management klíčů je speciální komponenta, která nepřichází do styku s elektronickými volebními lístky ani s voličskými identifikátory. Má však úplně jiný význam – a to dokonale zabezpečit tyto citlivé údaje. Tato komponenta je zodpovědná za vytváření a správu klíčů systému a voličů. Z bezpečnostního hlediska je to jedna z nejdůležitějších částí volebního systému.

Požadovaná bezpečnost je dosažena principem asymetrické kryptografie. První částí volebního procesu je pro tuto komponentu vygenerování páru klíčů pro volební systém EstEVS. Ty se generují v HSM[33] tak, že privátní klíč nikdy neopustí tento modul. Veřejný klíč se integruje do volební aplikace a používá se na zašifrování každého volebního lístku voliče. Soukromý klíč z páru je uložen pro použití sčítací aplikace a slouží pro dešifrování přijatých hlasovacích lístků. Maximální důležitost v rámci managementu klíčů se klade na použití právě tohoto soukromého klíče, a to, aby byl použitelný jenom sčítací aplikací a jenom v určený čas v den voleb, případně v průběhu potřebného přepočítání hlasů. Když uplyne doba pro podávání stížností, soukromý klíč i všechny jeho zálohy se zničí (zničení soukromého klíče je velmi vhodný způsob, jak znemožnit přístup k zašifrovaným datům a také k případným zálohám těchto citlivých dat a to poměrně rychle).

Generování páru klíčů a použití soukromého klíče volebního sytému, je v zodpovědnosti odpovědných manažerů pro správu klíčů. V procesu volebního systému jich je několik. Je určeno 7 privilegovaných členů z Národní volební komise, ze kterých alespoň 4 musí být přítomných při provádění takových operacích v rámci procesu elektronických voleb, které jsou definované jako kritické z hlediska bezpečnosti. Manažeři pro správu klíčů mají PIN kód pro to, aby se mohli autentizovat v případě potřeby práce s HSM.

Důvod, proč se klade důležitost na zabezpečení privátního klíče je ta, že je vystaven hlavně následujícím dvěma bezpečnostním hrozbám.

První je kompromitace klíče (klíč se stane známý veřejnosti – neoprávněným osobám pro znalost této informace). Naplnění hrozby by mohlo znamenat pro

[33] HSM (Hardware Security Module - hardwarový bezpečnostní modul) je zaměřen na správu klíčů a zrychlení kryptografických procesů z hlediska elektronických podpisů.

neoprávněné subjekty, které by měli přístup k elektronicky podepsaným hlasovacím lístkům, zjištění, kdo za koho volil, což by znamenalo nedodržení jedné z hlavních myšlenek voleb, kterou je tajnost voličovy volby.

Druhou hrozbou je poškození privátního klíče (nemožnost jeho dalšího použití). V tomto případě nastává neschopnost dešifrování elektronicky podepsaných volebních lístků a tedy nemožnost určení výsledků voleb. Z toho plyne potřeba zálohování privátního klíče, aby v případě ztráty nebo technického selhání, byl k dispozici záložní klíč.

Soukromí a utajení voliče a jeho volby může být ohroženo v případě výskytu následujících dvou bezpečnostních hrozeb najednou

- přístup neoprávněné osoby k soukromému klíči volebního systému,
- přístup neoprávněné osoby k elektronicky podepsaným hlasům uloženým v systému.

Ačkoli jsou tyto hlasy a tento klíč uloženy odděleně, představuje tato kombinace bezpečnostních hrozeb určité bezpečnostní riziko. Jedinečný privátní klíč je pravděpodobněji mnohem jednodušší ochránit než množství elektronických volebních lístků, které se přenáší z volební aplikace přes volební server až do sčítací aplikace. Z toho plyne, že zajištění bezpečnosti se zaměřuje prvotně na management klíčů.

4.1.4 Auditing

Tato komponenta má také speciální význam a také nepřichází přímo do styku s citlivými informacemi (myšleno s volebními hlasy a identifikačními údaji o voličích) v rámci centrálního systému. Slouží v podstatě na kontrolu toho, jestli centrální systém EstEVS funguje tak, jak je od něj požadováno.

Zaznamenává (loguje) důležité informace v rámci centrálního systému do několika různých auditních souborů, které vznikají v různých stavech volebního procesu. Je stanovena privilegovaná volební komise, která má právo řešit případné stížnosti nebo spory a nahlížet do souborů, ve kterých se provádí logování. Na rozdíl od projektu SERVE stojí tato komponenta topologicky mimo centrální systém.

4.1.4.1 Auditní aplikace

Existuje pět různých souborů, do kterých auditní aplikace zapisuje informace v různých stádiích putování volebních lístků volebním systémem spolu s časovým razítkem[34] vytvořeného logu. Soubory určené pro logování a pro následný audit jsou následující:

1. Soubor LOG1 slouží pro logování přijatých volebních lístků od volebního serveru, spolu s identifikátorem voliče.
2. Zrušené volební lístky spolu s identifikátorem voliče a důvodem zrušení se ukládají do souboru LOG2.
3. Volební lístky odeslané do sčítací aplikace spolu s identifikátorem voliče se logují do souboru LOG3.
4. Neplatné volební lístky se logují do souboru LOG4.
5. A volební lístky, které byly započteny, se logují do souboru LOG5.

Do každého souboru se ukládají volební lístky a jiná data podle stavu, v jakém se nacházejí. Je potřebné upozornit, že volební lístky se tam neukládají přímo, ale v zahašované podobě. Důvodem je zvýšení bezpečnosti. Haš zašifrovaného volebního lístku (v případě, že je použit dostatečně bezpečný hašovací algoritmus) nám zaručuje, že ani privilegovaná osoba s právem nahlížení do auditních souborů by se neměla dozvědět, jak daný volič hlasoval i kdyby měla privátní klíč systému, protože nelze jednoduše odvodit originální hodnotu z její haše (viz kapitola 1.3.1.4).

Auditní aplikace nám tedy umožňuje zjistit životní proces každého odevzdaného hlasu a dává komplexní nástroj pro řešení většiny sporů ohledně odevzdaných hlasů.

Existují následující možnosti stavu voličova hlasu. Hlas je přijat do úložního serveru a tedy zapsán do souboru LOG1. Pak je hlas úložním serverem buď zrušen (z důvodu duplicity) a zapsán v LOG2 nebo je přenesen do sčítací aplikace a zapsán v LOG3. V sčítací aplikaci je hlas buď zneplatněn a zapsán v souboru LOG4 nebo je platný, zahrnutý do sčítání hlasů a zapsán v souboru LOG5. V rámci auditingu je tedy možné provést kontrolu na integritu logovacích souborů a to například tak, že

[34] Časové razítko je sekvence znaků identifikujících, kdy nastala daná událost.

každý auditní záznam v souboru LOG1 má odpovídající položku právě v jednom ze souborů LOG2 nebo v LOG3 a naopak (protože každý volební hlas který byl přijat, byl buď duplicitní a byl zrušen nebo byl jedinečný a byl přesunut pro sčítání do sčítací aplikace). Každý auditní záznam v souboru LOG3 má odpovídající záznam v právě v jednom ze souborů LOG4 nebo LOG5 a naopak (protože každý hlas je sčítací aplikací označen buď za platný a je započten, nebo za neplatný). Dále, každý záznam v LOG4 a LOG5 má odpovídající elektronický podpis, uložen v úložním serveru, který jej získal oddělením vnitřní a vnější obálky. Také lze zkontrolovat, že počet hlasů, které se spočetli, je roven počtu řádků v souboru LOG5, a že záznamy ze souboru LOG2 spolu se záznamy ze souborů LOG4 a LOG5 jsou právě všechny záznamy v souboru LOG1.

5. Výsledné porovnání

Následuje porovnání třech zmíněných systémů – systému SERVE, volebního systému v Estonsku a ideálního elektronického volebního systému. Poukážeme na základní rozdílné vlastnosti jednotlivých systémů a uvedeme příklady útoků, které by se díky těmto vlastnostem daly nebo nedaly provést.

Shrňme si tedy základní rozdílné vlastnosti systému SERVE a EstEVS.

Vlastnost systému	SERVE	EstEVS	Ideální systém
Délka období, v průběhu kterého lze volby provést	30 dní	7 dní	Požadavek pro voliče 3.5 – nenáročnost volby – souvisí také s časovou nenáročností
Povinná registrace voličů před volbami	Ano	Ne	Požadavek pro voliče 3.5 – nenáročnost volby
Možnost opakované volby s možností změny volby předchozí	Ne	Ano	Ano Požadavek pro voliče 1.1 – právo na provedení opakované volby
Volební lístek voliče se před odesláním do centrálního systému voličem podepisuje	Ne	Ano	Ano Požadavek 3.7 – lístek se před odesláním podepíše
Volební lístky se nachází na úložním serveru po jistou dobu v nezašifrované podobě	Ano	Ne	Ne Požadavek pro voliče 3.1 – utajení voleb a požadavek 3.6 – volební lístky jsou zašifrovány pomocí bezpečného šifrovacího schématu a zůstanou zašifrovány minimálně po dobu sčítání hlasů
Přenos zašifrovaných volebních lístků online kanálem z úložního na sčítací server spolu se seznamem voličů, kterým tyto lístky patří	Ano	Ne	Ne Požadavek pro voliče 3.1 - utajení voleb
Sčítací komponenta je umístěna off-line	Ne	Ano	Není stanoveno, jestli musí být komponenta on-line nebo off-line, důležitost se klade na její bezpečnost
Existence logovacího procesu, který zaručí možnost přesného dohledání stádia putování volebních lístků volebním	Ne	Ano	Ano Požadavky pro voliče 1.2 a pro privilegované osoby 1.3, které říkají o právu kontroly, jestli se jednotlivé hlasovací lístky správně

systémem			započetly; Požadavek 3.9 – o logovaní
Multiplatformnost operačních systému pro použití volební aplikace	Ne Jenom Microsoft Windows	Ano Windows, Linux, MacOS	Požadavek pro voliče 3.5 – nenáročnost volby

Tabulka 2 Porovnání vlastností systémů

5.1 Útoky na volební aplikaci

Ještě před volením pomocí volební aplikace v rámci systému SERVE má subjekt povinnost zaregistrovat se jako volič (při této příležitosti je voličovi přiděleno identifikační číslo a PIN). Zde vidíme rozdíl s Estonským volebním systémem, ve kterém díky PKI není nutná registrační fáze.

Zkusme se podívat na bezpečnost. Proč by například nemohl útočník pomocí MITM útoku komunikovat s voličem tak, **aby si myslel, že se doopravdy zaregistroval** (registrační proces by z pohledu voliče byl nezměněn, volič by dostal nějaký PIN kód a byl by informován, že byl úspěšně zaregistrován)? Při konstrukci systému SERVE by to šlo provést, neboť při registračním procesu by mohl tímto útokem odposlechnout voličovy přihlašovací údaje a odvolit tak za něj.

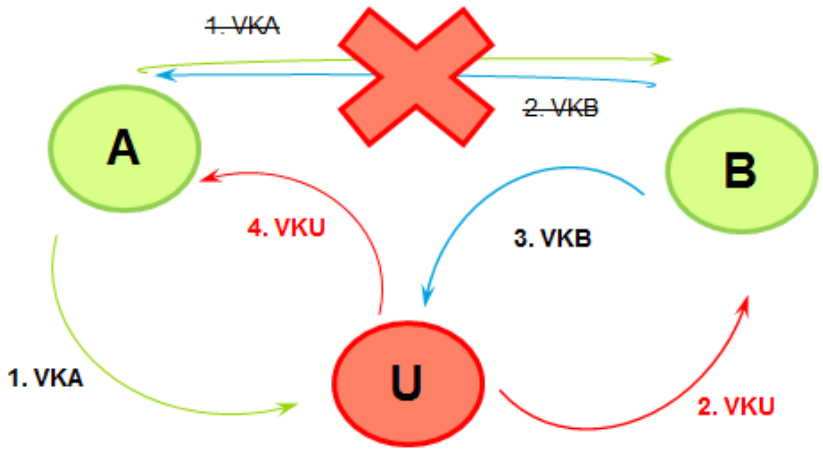
MITM útok by se dal také provést na spojení mezi volební aplikací a volebním serverem s cílem **změnit voličův hlas**. Kdyby útočník vystupoval jako prostředník mezi volební aplikací a volebním serverem, tak by přes něj procházela veškerá komunikace, například přihlašovací údaje voliče, zašifrovaný volební lístek. Útočník by tak mohl tuto komunikaci číst a pozměňovat. V případě systémů SERVE i EstEVS se posílá voličovi *Response*, která mu, když se podaří hlasovat úspěšně, sdělí, že jeho hlas byl přijat volebním systémem. Tuto *Response* by musel útočník doručit voličovi, aby snížil pravděpodobnost odhalení tohoto útoku voličem. Když má volič podezření, že něco není v pořádku, mohl by o tom informovat příslušné úřady, které by mohly proces voleb zastavit.

V kapitole 3.1.1 pro systém SERVE a 4.1.1 pro EstEVS jsme uvedli, že šifrování a autentizace se provádí prostřednictvím SSL protokolu, který zabezpečuje HTTP komunikaci mezi volební aplikaci (klient) a volebním serverem.

V kapitole 1.4.2 bylo zmíněno, že pro obranu před MITM útokem při komunikaci pomocí HTTP protokolu se může použít HTTPS protokol. Nicméně to, že protokoly SSL 3.0 i TLS (které jsou používány při HTTP protokolu) jsou kryptograficky bezpečné, automaticky neznamená, že když je použijeme, tak bude vše zabezpečeno tak, jak si představujeme – existují slabá místa, která se i v tomto případě dají zneužít.

Na které místo by se asi dalo zaútočit při používání tohoto protokolu? Pokud je již spojení mezi klientem (útočník chce přesvědčit klienta, že komunikuje s daným serverem) a serverem navázáno, certifikáty jsou vyměněny a data se šifrují, je pozdě. Vhodný čas pro útok je před uskutečněním tohoto spojení.

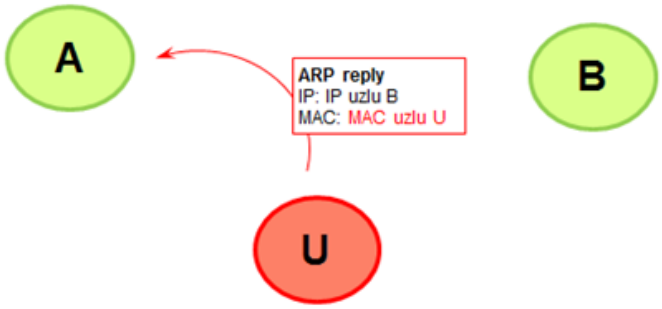
Kdyby se útočníkovi podařilo podvrhnout svůj certifikát klientovi tak, aby si myslel, že to je autentický certifikát daného serveru, měl by pravděpodobně vyhráno, protože útočník by věděl, kterým algoritmem klient šifruje posílaná data (ten je ustanoven při zahajování SSL/TLS spojení – viz kapitola 1.4.2) a měl by privátní klíč, kterým by dešifroval data, jež klient zašifroval útočníkovým veřejným klíčem VKU.



Obrázek 17 MITM Volební aplikace

Toto je další možnost, jak provést MITM útok při použití HTTPS jako komunikačního protokolu. Opišme si trochu detailněji, jak by se mohl útok provést. Využijme kapitolu 1.4.4, která říká o použití ARP cache poisoningu a zkusme provést MITM útok v případě, když se klient (oběť) i útočník nachází ve stejné lokální síti (například když by chtěl volit nějaký zaměstnanec ve firmě, kde by byl počítač, použitý pro provedení volby, připojen do lokální sítě této společnosti – útočník přítomen v dané lokální síti by mohl být například kolega nebo IT

administrátor této společnosti). Použijme označení uzlů A – klient (oběť) a B – server, jako strany, které chtějí spolu komunikovat pomocí HTTPS protokolu. Nechť je strana B lokální gateway nebo lokální DNS server (tyto servery jsou komunikovány v případě potřeby komunikace přes Internet) – pro názornost si vyberme, že strana B bude DNS server. Útočník U se snaží posílat ARP reply pakety straně A, aby si zapsala do své cache, že to správné propojení je – IP adresa uzlu B souvisí s MAC adresou uzlu U (to by šlo například použitím *arpspoof* nástroje).



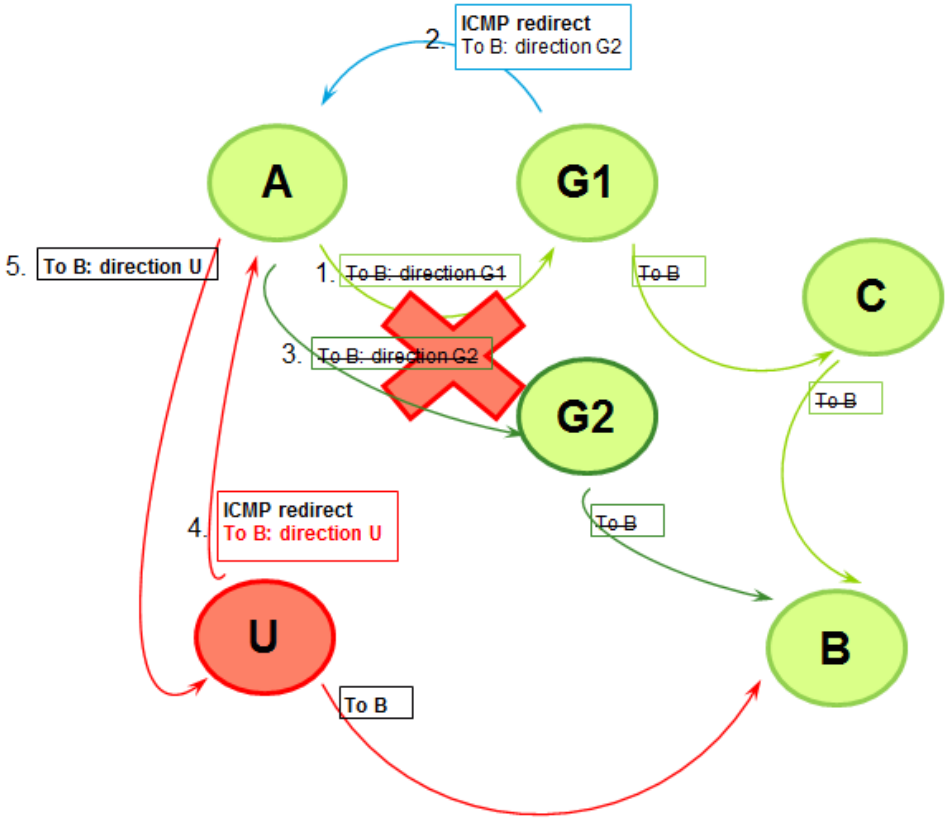
Obrázek 18 ARP cache poisoning Volební aplikace

Získání podobného postavení v lokální síti by útočník mohl také docílit pomocí například techniky Port stealing (viz kapitola 1.4.7). Teď potřebuje útočník samozřejmě odchytit ten správný moment – zahajování HTTPS spojení. Logicky tedy plyne, že bude odposlouchávat dotazy na DNS server (když bude chtít uzel A komunikovat pomocí protokolu HTTP, zadá internetovou stránku do prohlížeče, pošle se dotaz na DNS server, který přeloží tuto adresu na IP adresu – DNS server je při zahajování takového HTTP spojení určitě kontaktován) – to lze provést například pomocí *dnsspoof* nástroje. Dále by útočník narazil na problém s certifikáty. Potřebuje totiž nějaký mít a podstrčit ho uzlu A při zahajování SSL/TLS spojení - tu by mohl pomoci například *webmitm nástroj*. Ten může pomoci při odposlouchávání HTTPS spojení a řízení komunikace s klientem. Ještě by útočník potřeboval komunikaci od uzlu A odchytit a pak ji číst – zachytit a uložit by ji mohl například *tcpdump* nástroj. Teď by mu stačilo jenom použít například *ssldump* pro analyzování, certifikát z *webmitm* použít pro dešifrování zachycené šifrované komunikace a vyextrahovat potřebná data – například přihlašovací uživatelské jméno a heslo.

Když by se útočník a uzel A nacházeli v jiné síti, tak bychom nemohli použít ARP cache poisoning. Existuje několik sofistikovaných technik na to, jak ale docílit analogického důsledku, jako při použití ARP útoku – například kdyby získal útočník

přístup k směrovači[35], mohl by tam přímo změnit konfiguraci a zapnout statické směrování.

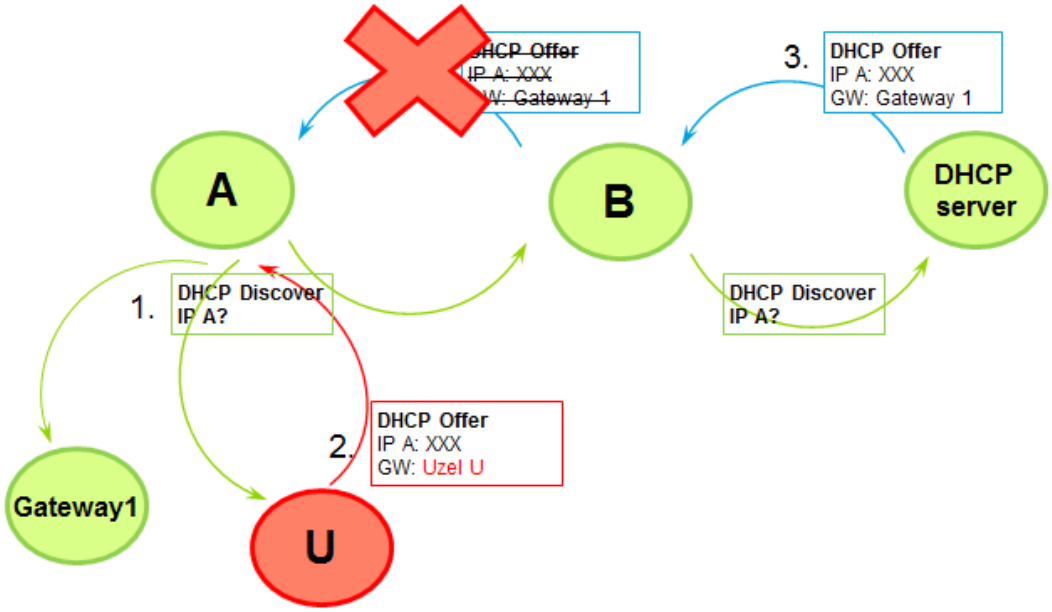
MITM útok by se dal inicializovat například i pomocí ICMP redirecting útoku (viz kapitola 1.4.6). Kdyby totiž pomoci *ICMP Redirect* paketu útočník nastavil oběti, že k serveru (například již zmíněný DNS) vede nejkratší cesta přes něj (útočníka), a serveru by nastavil, že nejkratší cesta od serveru k oběti vede přes útočníka, tak by veškerá komunikace šla přes útočníka.



Obrázek 19 ICMP redirecting Volební aplikace

DHCP spoofing (viz kapitola 1.4.5) je další z MITM technik, pomocí které útočník nastaví oběti jako například DNS server sebe, čímž si zajistí, že veškerá komunikace oběti s Internetem bude probíhat skrz útočníka.

[35] Směrovač (router) je aktivní síťové zařízení, které spojuje sítě a při komunikaci mezi sítěmi se přes něj přenášejí data.



Obrázek 20 DHCP spoofing Volební aplikace

Existuje jedno opatření (viz sekce 3.1.3 Logování a Audit), díky kterému by mohl volič zjistit, zda jeho jméno figuruje na seznamu voličů (kteří volbu provedli) na úložním serveru nebo i na sčítacím serveru. Ale zase, kdyby útočník volební hlas pozměnil, volič by na to nepřišel, protože jeho jméno by figurovalo na seznamech, volič by se mohl dozvědět, že něco není v pořádku, jen kdyby útočník hlas pozdržel a neposlal dále. I kdyby se zjistilo, že takový útok byl proveden, volby by se museli zrušit a systém by se nemohl považovat za adekvátní náhradu papírového volebního systému.

V systému SERVE se zasílané zašifrované volební lístky nepodepisují, takže tento útok by se dal pravděpodobně provést.

V EstEVS se zašifrované volební lístky podepisují, takže útočník by musel najít způsob, jak získat přístup k privátním klíčům voličů (k dostatečnému množství, aby tím mohl ovlivnit výsledek voleb). Když si ale uvědomíme, že volební server v EstEVS si ověřuje na přijatém podepsaném volebním lístku od voliče, že ten, kdo podepsal hlas je ten samý, kdo vytvořil spojení, jinak volební lístek nepřijme, tak tento útok by byl asi těžko proveditelný.

V ideálním systému je dle požadavku 3.7 voličovi zaručeno, že jeho zašifrovaný volební lístek, který chce odeslat do volebního systému k započtení, bude podepsán pomocí volební aplikace, a že podepisovací schéma je bezpečné. A dle požadavku 1.5 neoprávněná osoba nemá možnost přístupu k většímu množství

podepisovacích klíčů voličů (k takovému množství, že by to mohlo ovlivnit výsledek voleb), takže by nebylo pravděpodobné, že by byl tento útok proveditelný.

Na spojení mezi volební aplikací a volebním serverem by se dal provést MITM útok s cílem odepřít voličovi právo volit – a to tak, aby se volič místo na volební server připojil na nějaký podvrhnutý server a přitom si myslel, že je vše v pořádku, a že je připojen na ten správný server.

V případě systémů SERVE i EstEVS se posílá voličovi *Response*, když se mu podaří hlasovat úspěšně, že jeho hlas byl přijat volebním systémem – útočník potřebuje tuto *Response* vygenerovat, tak jak to bylo při útoku na změnu voličova hlasu.

Útočník by tedy mohl nastavit podvržený volební server tak, aby když volič provede svou volbu, aby mu poslal ActiveX kód který by vytvořil falešnou *Response* zprávu, aby si volič myslel, že svou volbu provedl úspěšně.

Pro SERVE i EstEVS je způsob provedení tohoto útoku založen na podobném principu. Zaprvé útočník musí docílit toho, aby se volební aplikace voliče připojila na jeho server místo volebního serveru. Na to by útočník například potřeboval nějaký malware, který by pak potřeboval doručit na volební aplikaci (například, že by si ho volič stáhnul z internetu – kdyby byl malware jako trojský kůň, tak by se například tvářil jako neškodná aplikace, ale na pozadí by mohl provést nežádoucí činnost – například by pomohl k připojení na útočníkův server). Útočník by pro tento účel mohl využít techniku phishing[36], kde by mohl poslat voličům nějaký e-mail (předstíral by, že e-mail byl zaslán například od volební komise nebo by se mohl vydávat za primátora, který navádí voliče volit) s odkazem na stránku obsahující malware.

Dále by potřeboval upravit seznamy voličů na serverech volebního systému tak, aby tam figurovali jména voličů, na což by byl potřebný zase nějaký malware.

[36] Phishing je technika používaná k získávání citlivých údajů, například hesel nebo čísel platebních karet. K nalákání důvěřivé komunikace předstírá, že pochází z populárních sociálních sítí (například facebook), aukčních webů, on-line platebních portálů nebo od IT administrátorů.

5.2 Útoky na volební server

Kdyby útočník mohl zahltit webový volební server, provedením DoS nebo DDoS útoku (dále jen DoS), mohl by ho vyřadit z provozu a znemožnit tak voličům vykonání volby.

Prvním možným způsobem pro provedení útoku takového typu je zahlcení síťového připojení cílového webového serveru různými daty, jež by zablokovaly síť, a oprávnění voliči by nemohli provést svou volbu, protože by se jejich spojení nedostalo přes zahlcenou síť.

V případě systému SERVE je tato možnost útoku pravděpodobná. Zranitelností pro provedení tohoto útoku jsou webové stránky systému, protože kdyby útočník zahltil jejich síťové připojení DoS útokem, oprávnění voliči by nemohli pomocí systému SERVE volit. Odolnost webových stránek vůči zahlcení sítě je určena hlavně jejich propustností. Například webová stránka s propustností 1Gbps by měla odolat 1Gbps DoS útoku. V bezpečnostní analýze (12, s. 19) se uvádí, že byly pozorovány i 150 Gbps DoS útoky, což by mohlo pravděpodobně ohrozit dostupnost systému SERVE.

Druhou možností je, že by útočník zahltil přímo výpočetní zdroje webového serveru nějakými nepotřebnými úlohami a držel by ho zaneprázdněn, že by nedokázal odpovídat na žádosti o připojení oprávněných voličů. Tento útok se dá provést různými způsoby. SERVE například používá webové stránky komunikující SSL protokolem a SSL je snadno podléhající DoS útoku. Útočník by mohl například posílat mnoho žádostí o SSL spojení, což znamená pro webový server, příjemce těchto žádostí, provést pomalou kryptografickou operaci (typicky počítání s RSA privátním klíčem[37]) pro každou žádost o nové spojení. Pro ilustraci si vezměme následující úvahu. Dnešní moderní počítače mohou vygenerovat přibližně 100 nových spojení za sekundu a hardwarově toto číslo lze zvednou na tisíce takových spojení za sekundu. Pro porovnání, webové stránky internetového bankovnictví zvládnou v dnešní době 15000 nových SSL spojení za sekundu. Takže kdyby se útočníkovi podařilo vygenerovat 500000 nových SSL spojení za sekundu (lze

[37] Vytvoření asymetrického klíče je výpočetně velmi náročná operace, přičemž náročnost exponenciálně stoupá s jeho délkou [13].

předpokládat, že by se útočníkovi podařilo vytvořit s přibližně 10000 zombie počítači botnet a každý počítač by mohl vygenerovat nových 50 spojení za sekundu), tak by mohl zahltit webové stránky 10 až 100 krát více žádostmi, než by byly schopny zvládnout. Proti takovým DoS útokům je velmi náročné se bránit, nebo nějak snížit potenciální riziko útoku. Kdyby útočník například vyřadil z provozu síťové služby v jisté demografické oblasti, která je známá svými volebními preferencemi, mohl by tak ovlivnit celkový výsledek voleb. Voliči v rámci systému SERVE mohou volit 30 dní před dnem voleb, takže například kdyby voliči využili tohoto poměrně většího časového rámce pro provedení volby a nenechávali by si volbu na poslední dny, tak by se dal následek DoS útoku trochu zmírnit.

DoS útok by mohl být proveden pomocí ARP cache poisoningu (viz kapitola 1.4.4). Když chce volební server komunikovat s voličem (tedy přes Internet), tak ví, že musí komunikovat přes gateway. Zná sice její IP adresu, ale musí si zjistit její linkovou adresu. Takže útočník by mohl posílat falešné ARP reply pakety, kde by uváděl, že linková adresa gateway je například nějaká neexistující adresa. Pak volební server, v domnění, že posílá pakety na gateway, by je posílal na neexistující linkovou adresu a nikdo by mu tedy neodpověděl.

Dle Estonské volební legislativy je délka průběhu elektronických voleb stanovena na 7 dní moci (rozdíl oproti projektu SERVE – 30 dní – je celkem velký). To může být potenciálně dostatečně dlouhá doba, aby si každý volič mohl najít čas provést elektronickou volbu. Na druhé straně, kdyby v průběhu těchto sedmi dní nastal DoS útok například na volební server, takže by voliči nemohli provést svou volbu, neboť by byl nedostupný, a tento dopad by nešel odstranit po dobu například několik desítek hodin, tak by to docela mohlo omezit časové možnosti voličů, kteří ještě nevykonali svou volbu a voliči, kteří možná chtěli volit, již nebudou chtít nebo moci.

V ideálním systému by se tedy mělo dbát na určení optimální doby pro provedení voleb, na kapacitu a vyvažování zátěže síťových připojení, na zavedení nějakých prevenčních systému, které dokáží některé pokusy o DoS útoky filtrovat.

5.3 Útoky na úložní server

Zabývejme se takovým útokem, kde by se útočníkovi podařilo docílit toho, že by oprávněné osoby k volbě mohly volit vícekrát a jejich hlas by byl pokaždé započten.

V systému SERVE není možné, aby osoba, oprávněna k volbě, mohla provést volbu více než jedenkrát. Úložní server rozhoduje o voličovém právu přístupu a právu k vykonání volby, tedy jestli je volič registrován a jestli ještě neprovedl úspěšnou volbu na základě seznamu identifikačních údajů voličů, kteří již volbu provedli, který si tato komponenta udržuje aktuální v průběhu celého trvání elektronických voleb (viz kapitola 3.1.2.2). Útok by se tedy mohl provést na funkčnost úložního serveru s cílem umožnění opakované volby pro oprávněné voliče pomocí nějakého malware, který by musel mít a který by musel na tento server dostat (protože systém SERVE nepočítá s možností dvojí volby, chybí fáze kontroly na dvojí hlasy, takže všechny přijaté hlasy by se započetli).

V EstEVS se po ukončení možnosti elektronického hlasování hlasovací lístky seřadí podle data přijetí a provede se kontrola na dvojité hlasy, jsou tedy odstraněny duplicitní hlasovací lístky (v případě, že volič volil vícekrát, započte se jenom poslední správně provedená volba a ostatní se zneplatní) a zruší se volební lístky od neoprávněných voličů. Seřazení hlasů zajišťuje ponechání poslední správně provedené volby. V případě zrušení nějakého hlasovacího lístku je tato akce zaznamenaná do logovacího souboru LOG2 spolu s důvodem zrušení daného hlasu (viz kapitola 4.1.2.2). V tomto případě by se dal provést útok takovým způsobem, že útočník by propašoval na úložní server malware, který by narušil proces kontroly na dvojité hlasy. Tedy do sčítací fáze by se zahrnuly všechny platně odevzdané lístky. Navíc by musel tento malware poupravit seznam voličů, kteří provedli volbu, aby se snížila pravděpodobnost odhalení toho, že někteří voliči volili vícekrát. V EstEVS dále není udržována informace (neloguje se to žádným způsobem), jestli volič provedl opakovanou volbu a ani žádná další kontrola, která by ověřila, jestli počet voličů, kteří provedli volbu je roven počtu přijatých hlasů.

V rámci ideálního volebního systému by se tento útok neměl dát provést díky požadavku pro voliče 3.2, který říká o tom, že voličovi je zaručeno, že jeho správně

provedená volba se započte a započte se jenom jeho poslední správně provedená volba.

Teď si přibližme útok, kde by útočníkův cíl bylo to, že by neoprávněné osoby k volbě mohli volit a jejich hlas by byl započten. Musela by se tímto útokem obejít kontrola, jestli má volič právo volit a muselo by se zabránit, aby po vykonání této volby bylo voličovo jméno zaznamenáno na seznamu voličů, kteří provedli volbu. Útočník by tedy potřeboval nějaký malware, který by dokázal toto docílit. Dále by útočník potřeboval mít takový přístup k úložnímu serveru, že by na něj mohl utajeně dostat tento malware. Potřeboval by pravděpodobně pomoc alespoň jedné privilegované osoby, která má potřebný přístup k tomuto serveru (například developer nebo administrátor serveru) – „čím lepší malware, tím je potřebný menší fyzický přístup.“ Buď by mohl někoho podplatit, nebo by mu mohl vytvořit nějakou zranitelnost nebo by mohl být sám tou osobou nebo by mohl využít nezpůsobilost některé osoby (potřeba školení těchto osob).

V ideálním volebním systému by k tomuto útoku pravděpodobně nemohlo dojít, protože privilegovaná osoba dle požadavku 2.2 nesmí zneužít svých pravomocí a dle požadavku 2.3 nesmí pomoct neoprávněným osobám získat přístup do systému. Požadavek 3.9 říká, že voličovi je zaručeno, že logovací systém v rámci volebního systému je bezpečný a loguje vše, co je potřebné pro dohledatelnost jakékoli události, potřebné pro řešení bezpečnostních incidentů nebo pro kontrolu procesu v zpracování hlasu.

Pro systém SERVE by to bylo pravděpodobně proveditelné. Jak jsme se dozvěděli v kapitole 3.1.3, v systému se nevytváří žádné logy. Neexistovaly by tak žádné auditní záznamy, které by se mohly ověřit, že bylo přidáno několik nových hlasovacích lístků. Úložní server i jednotlivé sčítací servery si ukládají seznamy voličů, kteří volbu provedli. Tedy u přidání lístků by také útočník potřeboval mít přístup k seznamu voličů, kteří volili, aby samozřejmě (když útočník chce snížit pravděpodobnost odhalení tohoto útoku) seděl počet volebních lístků a počet voličů, kteří provedli volbu. V systému SERVE je toto jediná možnost kontroly hlasů. Takže pokud se takový útok útočníkovi podařil, nikdo by nemusel zjistit, že k němu došlo.

Pro EstEVS by bylo nepravděpodobné, že by došlo k takovému útoku bez toho, aby se na to přišlo. Tento volební systém, jak jsme se dozvěděli v kapitole

4.1.4, má propracovaný auditní systém, který zvyšuje pravděpodobnost neporušení integrity v rámci procesů volebního systému, díky kterému by se tento útok mohl odhalit.

Pro systém SERVE je možné využít následující zranitelnost v procesech úložního serveru také na útok, který by byl zaměřen na změnu volebních lístků (tímto útokem by se porušila i tajnost voleb). Dle kapitoly 3.1.2.2: „Po dešifrování přijatých dat se tato citlivá data (volební lístek a identifikační údaje voliče) nachází po krátkou dobu na úložním serveru v nezabezpečeném formátu, až dokud server volební lístek znova nezašifruje pomocí privátního klíče příslušného sčítacího serveru.“ Útočník by mohl tedy změnit tyto hlasovací lístky předtím, než se znova zašifrují nebo je smazat. Jak je zřejmé, tento útok by se dal aplikovat na mnoho volebních lístků, takže by mohl mít dopad na celkový výsledek voleb. Tak jako při předchozím způsobu útoku by útočník potřeboval nějaký malware, který by dokázal toho docílit. Také by útočník potřeboval mít takový přístup k úložnímu serveru, že by na něj mohl utajeně dostat tento malware. Úložní server i jednotlivé sčítací servery si ukládají seznamy voličů, kteří volbu provedli, že u mazání lístků by také útočník potřeboval mít přístup k seznamu voličů, kteří volili, aby samozřejmě (když útoční chce snížit pravděpodobnost odhalení tohoto útoku) seděl počet volebních lístků a počet voličů, kteří provedli volbu. V systému SERVE je toto jediná možnost kontroly hlasů.

Pro EstEVS, ani ideální systém, by provést útok takovým způsobem nešlo, neboť lístky se nevyskytují v rámci volebního systému v nezašifrované podobě. V EstEVS se hlasovací lístky dešifrují až ve sčítací komponentě, která je umístěna off-line a tedy může mít úplně jiné zabezpečení, než úložní server. Útočník by se ale mohl zaměřit na to, že by si zjistil provázání mezi zašifrovanými volebními lístky a voličovými identifikátory (elektronickými podpisy), a tak by mohl smazat ty hlasy, které by chtěl smazat buď na základě identifikátorů voličů, nebo na základě zašifrovaných volebních lístků. Kdyby chtěl tyto lístky dešifrovat, musel by mít buď přístup k dešifrovacímu privátnímu klíči systému EstEVS, nebo by musel mít přístup k jednotlivým náhodným číslům, pomoci kterých se provádělo zašifrování jednotlivých volebních lístků – to číslo se náhodně generuje pro každého voliče osobitě. Takže by asi útočník potřeboval nějaký malware, který by dokázal

odposlechnout ve volební aplikaci každého voliče, jaké číslo bylo při šifrování použito.

V rámci EstEVS by se dalo zaútočit na volební a úložní server s cílem smazat nežádoucí volební lístky ještě předtím, než je úložní server od volebního přijme. V momentě přijetí se totiž zaznamená do souboru LOG1 informace o přijetí zašifrovaných volebních lístků spolu s identifikátorem voliče od volebního serveru. Útočník by ale zase potřeboval nějaký vhodný malware a přístup k těmto dvěma serverům.

V ideálním systému by se mohlo také použít Řešní 5.1, které říká o homomorfním šifrování - využití takové kryptografické funkce (aplikované při šifrování volebních lístků voliče), aby se daly veškeré voličské hlasy sečíst bez nutnosti dešifrace jednotlivých hlasů. Tato homomorfní šifra dovoluje pracovat se zašifrovanými daty. Dešifrovalo by se až výsledné sečtení.

Pro systém SERVE je možné využít následující zranitelnost v procesu komunikace úložního a sčítacího serveru na útok, který by byl zaměřen na smazání nežádoucích volebních lístků. Dle kapitoly 3.1.2.3: „Úlohou každého sčítacího serveru je pravidelné připojování se zabezpečeným komunikačním kanálem k úložnímu serveru a následné dotazování se na seznam voličů a nové zašifrované volební lístky. Tato data jsou danému sčítacímu serveru po úspěšné autentizaci zaslána. Po přijetí dat sčítací server ověří jejich totožnost, potvrdí úložnímu serveru jejich příjem a ukončí s ním komunikaci.“ Co kdyby se stalo, že by se sčítací server dotazoval úložního serveru na aktualizaci dat tak často, že by od něj dostal pouze jeden volební lístek a tedy i jméno toho jednoho voliče? Zajisté by nastala kompromitace tajnosti hlasu a nechtěné hlasy by tak mohl například smazat. Zase je ale potřebné, aby útočník smazal i voliče ze seznamu voličů. Jak již bylo výše uvedeno, útočník by pro tento útok potřeboval nějaký malware, který by dokázal toto docílit a také přístup k úložnímu serveru, aby na něj mohl utajeně dostat tento malware.

Kdyby měl útočník přístup k náhodnému číslu voliče, pomocí kterého se zašifroval jeho volební lístek, tak z informací – zašifrovaný volební lístek a jméno voliče, by byl schopen zjistit, jak volič volil, tedy by byla porušena tajnost voleb. Protože když útočník ví, jaké jsou možnosti na volbu a zkusil by si je všechny

zašifrovat pomocí veřejného klíče systému a pomocí daného náhodného čísla, tak by si to uměl (nebo dokázal) porovnat se zašifrovaným volebním lístkem voliče, který se posílá z úložního na sčítací server v rámci systému SERVE.

V EstEVS komunikace mezi úložním a sčítacím serverem nehraje taktovou roli, neboť zašifrované hlasy se přenášejí do sčítací aplikace na off-line úložním médiu.

5.4 Útoky na sčítací server

V systému SERVE se nachází několik sčítacích serverů. Každý sčítací server přímo komunikuje s úložním serverem a přijímá od něj potřebná data (zašifrované volební lístky a seznamy voličů, kterým tyto volební lístky patří). Tedy útoky na tento server nebo toto spojení, jsou probírány v kapitole 5.3 – Útoky na úložní server.

V rámci EstEVS je sčítací aplikace off-line komponentou. Data, která jsou zpracovávána sčítací aplikací, se doručí na off-line fyzickém úložním médiu. V rámci této aplikace neexistuje provázání, které by mohlo narušit tajnost voleb.

Pro přidání volebních lístků útočník nepotřebuje elektronický podpis jednotlivých voličů. Potřebuje ale vytvořit tyto zašifrované volební lístky a pak je nějak dostat na to off-line médium. V logovacím souboru LOG3 jsou uloženy zašifrované a podepsané volební lístky, které se doručují do sčítací aplikace spolu s identifikátorem voliče. Takže by volič musel zaútočit i na tento logovací soubor, který by poupravil tak (přidal zašifrované volební lístky a nějaké identifikátory voličů), aby z něj nešlo poznat, že přidal nějaké další volební lístky. Takže i kdyby útočník získal přístup k off-line úložnímu médiu a podařilo by se mu tam dostat zašifrované volební lístky, potřeboval by přístup i k logovacím souborům. Čím více komponent systému třeba do útoku zahrnout, tím by to mohlo znamenat menší šanci na úspěch.

Ze záruky 3.9 je voličovi zaručeno, že logovací systém v rámci volebního systému je bezpečný a loguje vše, co je potřebné pro dohledatelnost jakékoli události, potřebné pro řešení bezpečnostních incidentů nebo pro kontrolu procesu v zpracování hlasu (souvisí s právem kontroly volebních lístků pro voliče 1.2 a pro privilegované osoby 1.3).

Závěr

Dalo by se říct, že elektronický volební systém je více zranitelný než papírový volební systém, neboť je pravděpodobně ohrožen větším počtem hrozeb, které ohrožují vetší množství hlasovacích lístků „najednou“. I to je jedním z argumentů, proč je zavedení elektronického volebního systému složitý úkol. Při využívání elektronického volebního systému v praxi je totiž potřebné dosažení alespoň takové úrovně bezpečnosti, jaká se očekává od klasických papírových voleb.

Cílem této práce bylo jednak popsat architekturu dvou již navržených volebních systémů, z kterých jeden je uveden do praxe (EstEVS) a druhý byl navržen, ale po různých bezpečnostních analýzách bylo zakázáno jeho používaní (SERVE); dále podat návrh na základní požadavky, které bychom od ideálního volebního systému čekali a nakonec tyto systémy navzájem porovnat a nastínit možnosti útoků, které poskytují svou architekturou, vlastnostmi a požadavky.

Již při popisování fungování těchto dvou systémů navržených pro provádění elektronických voleb je vidět základní zranitelnosti systému SERVE, které se nedají řešit pouhým nastavením nějakých „parametrů“, ale bylo by nutné fungování celého systém změnit. Mnoho ze zranitelností systému SERVE systém EstEVS nemá, což jasně nastínila i poslední kapitola pomocí opisu základních útoků, které by se daly na systém SERVE provést a na systém EstEVS většinou nikoli; ideální systém by podle definovaných požadavků tyto zranitelnosti také neobsahoval. Výsledkem práce je tedy poukázání na nedokonalosti zabezpečení systému SERVE a dokonalosti systému EstEVS. Navrhovaný ideální volební systém by mohl vypadat obdobně jako systém EstEVS.

Seznam použité literatury

[1] OCSP (Online Certificate Status Protocol). ROUSE, Margaret. Http://searchsecurity.techtarget.com [online]. 2007 [cit. 2013-03-02]. Dostupné z: http://searchsecurity.techtarget.com/definition/OCSP

[2] Vícefaktorová autentizace [online]. 2010[cit. 2013-03-02]. Dostupné z: http://www.cleverandsmart.cz/vicefaktorova-autentizace/

[3] MARŤÁK, Pavel. Bezpečnost dat v praxi. IT Systems [online]. 2005 [cit. 2013-03-02]. Dostupné z: http://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm

[4] SMEJKAL, Vladimír. Řízení rizik ve firmách a jiných organizacích: 3., rozšířené a aktualizované vydání. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6.

[5] KROPÁČOVÁ, Andrea. Bezpečnost elektronických dat a elektronické komunikace. Zpravodaj ÚVT MU Bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě. roč. 16, č. 4, s. 15-20. ISSN 1212-0901. Dostupné z: http://www.ics.muni.cz/bulletin/articles/522.html

[6] Hašovací funkce, principy, příklady a kolize. In: KLIMA, Vlastimil. Personal page: Vlastimil Klima [online]. 2005 [cit. 2013-03-02]. Dostupné z: http://cryptography.hyperlink.cz/2005/cryptofest_2005.htm

[7] Hašovací funkce MD5 a další prolomeny!. In: KLIMA, Vlastimil. Root.cz [online]. 2004 [cit. 2013-03-02]. Dostupné z: http://www.root.cz/clanky/hasovaci-funkce-md5-a-dalsi-prolomeny/

[8] Odposloucháváme data na přepínaném Ethernetu: ARP Cache poisoning. In: HALLER, Martin. Lupa.cz: Server o českém Internetu [online]. 2006 [cit. 2013-03-02]. Dostupné z: http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-2/

[9] Odposloucháváme data na přepínaném Ethernetu: DHCP Spoofing. In: HALLER, Martin. Lupa.cz: Server o českém Internetu [online]. 2006 [cit. 2013-03-02]. Dostupné z: http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-4/

[10] Odposloucháváme data na přepínaném Ethernetu. In: HALLER, Martin. Lupa.cz: Server o českém Internetu [online]. 2006 [cit. 2013-03-02].

Dostupné z: http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-3/
[11] GENTRY, Craig. A fully homomorphic encryption scheme [online]. 2009 [cit. 2013-03-02]. Dostupné z: http://crypto.stanford.edu/craig/craig-thesis.pdf. Dissertation. Stanford University. Vedoucí práce Dan Boneh.
[12] JEFFERSON, David, Aviel D. RUBIN, Barbara SIMONS a David WAGNER. Security analysis of SERVE. 2004. Dostupné z: http://www.servesecurityreport.org/paper.pdf
[13] VALÁŠEK, Michal Altair. Přísně tajné šifry: Asymetrické šifry pro tajné zprávy a připojení k bankám. Ihned.cz [online]. 2012, 5. 11. 2012 [cit. 2013-03-02]. Dostupné z: http://tech.ihned.cz/geekosfera/c1-58281550-prisne-tajne-sifry-asymetricke-sifry-pro-tajne-zpravy-a-pripojeni-k-bankam
[14] ESTONIAN NATIONAL ELECTORAL COMMITTEE. E-Voting System: General Overview [online]. Tallin, 2010 [cit. 2013-03-02]. Dostupné z: http://www.vvk.ee/public/dok/General_Description_E-Voting_2010.pdf
[15] BERGER, Josef. Elektronický systém voleb a hlasování (E-voting) [online]. 2012 [cit. 2013-03-02]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/bergejos_2012dipl.pdf. Diplomová práce. České vysoké učení technické v Praze. Vedoucí práce Ing. Leoš Boháč, Ph.D
[16] RÖSSLER, Thomas Gert. Electronic Voting over the Internet - an E-Government Speciality [online]. 2007 [cit. 2013-03-02]. Dostupné z: https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=34776. Dissertation. University of Technology Graz, Austria. Vedoucí práce Univ.-Prof. Dr. Reinhard Posch.
[17] CHOWDHURY, M J Morshed. UNIVERSITY OF TARTU. Comparison of e-voting schemes: Estonian and Norwegian solutions [online]. Dostupné z: http://courses.cs.ut.ee/2010/security-seminar-fall/uploads/Main/chowdhury-final.pdf
[18] Electronic ID Card. [online]. [cit. 2013-03-08]. Dostupné z: http://e-estonia.com/components/electronic-id-card

Seznam tabulek

Seznam použitých zkratek

ARP – Adress Resolution Protocol je protokol, který se stará o překlad IP adresy na MAC adresu.

CA – Certifikační autorita vystupuje při komunikaci dvou subjektů jako třetí nezávislý důvěryhodný objekt, který vydává certifikáty. CA zaručuje, že deklarovaný veřejný klíč přísluší danému subjektu a potvrzuje planost vydaného certifikátu.

CAM – Content Addressable Memory tabulka slouží k ukládání MAC adres s příslušným portem.

CRL – Certificate Revocation List je seznam zneplatněných certifikátů, které zveřejňuje CA.

DHCP – Dynamic Host Configuration Protocol je protokol, který je určený k dynamickému přidělování síťových parametrů (zejména IP adres) koncovým zařízením. DHCP server přiděluje počítačům pomocí DHCP protokolu síťové parametry.

DDoS – Distributed Denial of Service je distribuovaný DoS útok. Jedná se o útok, který je charakteristický tím, že se ho účastní více než jeden počítač.

DoS – Denial of Service (odmítnutí služby) je technika útoku na internetové služby nebo stránky, či sítě, při níž dochází k přehlcení systému požadavky a pádu nebo minimálně nefunkčnosti a nedostupnosti pro ostatní uživatele.

DNS – Domain Name System je hierarchický systém doménových jmen, který je realizován servery DNS a protokolem stejného jména, kterým si vyměňují informace. Jeho hlavním úkolem a příčinou vzniku jsou vzájemné převody doménových jmen a IP adres uzlů sítě.

EstEVS – Estonian E-Voting System je Estonský elektronický volební systém.

HTTP – Hypertext transfer Protocol je protokol aplikační vrstvy pro přenos internetových stránek.

HTTPS – Hypertext transfer Protocol Secure je zabezpečená verze HTTP protokolu (zabezpečením se myslí šifrování přenášených dat pomocí protokolu SSL nebo TLS).

HSM – Hardware Security Module je hardwarový bezpečnostní modul, který je zaměřen na správu klíčů a zrychlení kryptografických procesů z hlediska elektronických podpisů.

ICMP – Internet Control Message Protocol je protokol, který primárně neslouží k přenášení dat, ale k přenášení informací o chybách, upozorněních a jiné.

IP – Internet Protocol je základní protokol síťové vrstvy používaný v rámci počítačových sítí a Internetu. IP je zodpovědný za směrování paketů ze zdrojového do cílového zařízení. IP adresa – je číslo, které se používá na identifikaci síťových zařízení v sítích, které používají IP protokol. Označením IP se v praxi často myslí IP adresa.

IRC – Internet Relay Chat byl jednou z prvních možností komunikace v reálném čase po internetu.

MAC – Media Access Control je podvrstva linkové vrstvy, která řeší přístup ke sdílenému médiu. MAC adresa - identifikátor zařízení v rámci informačních sítí. Označením MAC se v praxi často myslí MAC adresa.

MITM – Man in the middle je označení pro útok, jež patří mezi nejznámější problémy v informatice a kryptografii. Jeho podstatou je snaha útočníka odposlouchávat komunikaci mezi účastníky tak, že se stane aktivním prostředníkem.

OCSP – Online Certificate Status Protocol je schéma pro udržení bezpečnosti serveru a ostatních síťových zdrojů. Shromažďuje informace o stavech certifikátů. Z jisté části nahradila fungování revokačních listů certifikátů CRL

PKI – Public Key Infrastructure je v asymetrické kryptografii označení infrastruktury správy veřejných klíčů. Pomocí veřejného klíče v podpisovém certifikátu lze ověřovat elektronický podpis vlastníka privátního klíče. Pomocí veřejného klíče v šifrovacím certifikátu lze šifrovat zprávu pro vlastníka privátního klíče.

RFC – Request For Comment je souhrn doporučení ohledně protokolů (popisu komunikace) Internetu.

SERVE – Secure Electronic Registration and Voting Experiment.

SoD – Segregation of Duties, tzv. rozdělení pravomocí.

SSL – Secure Socket Layer, tzv. vrstva bezpečných soketů, je protokol, který poskytuje zabezpečení komunikace proti odposlouchávání či nechtěné změně dat

v průběhu komunikace šifrováním dat, která se přenáší a autentizací komunikujících stran.

TCP – Transmission control protocol je protokol transportní vrstvy, který navazuje spojení mezi klientem a serverem. Garantuje spolehlivé doručování a zachovává pořadí paketů (bloků dat).

TLS – Transport Layer Security protokol je nástupcem protokolu SSL. Slouží na zabezpečení komunikace.

X.509 – Je standard pro systémy založené na PKI. Specifikuje mezi jiným formát certifikátů, seznamů zneplatněných certifikátů, parametry certifikátů a metody kontroly platností certifikátů.