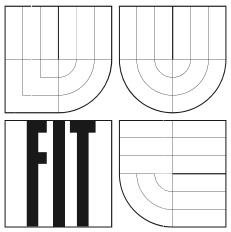
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ



Vliv postranních kanálů na soukromí

Ročníkový projekt

2006 **Milan Tomášek**

Zadání:

1. Prostudujte standard pro hodnocení IS - Common Criteria - zejména část popisující soukromí, dále se seznamte s úlohou skrytých kanálů z hlediska kryptoanalýzy, ale i obecné bezpečnosti.
2. Analyzujte vliv skrytých kanálů na zachování soukromí v systémech, které tuto vlastnost nabízejí, diskutujte možné úpravy standardu tak, aby pokryly tuto oblast.
3. Vyberte s pomocí vedoucího projektu několik typických transakcí v informačních systémech, definujte kontext, ve kterém tyto transakce probíhají (i z pohledu příslušné komunikace) a určete jejich informační hodnotu.
4. Pokuste se vytvořit co nejobsáhlejší klasifikaci různých kontextů a na jejím základě se pokuste stanovit pravidla pro určení jejich informační hodnoty z hlediska analýzy skrytých kanálů.
5. Diskutujte význam vytvořené klasifikace a příp. metrik na systémy zaručující soukromí.

Kategorie: Bezpečnost
Literatura:

- Common Criteria for IT Security Evaluation, http://csrc.nist.gov/cc/.
- Anonymity bibliography, http://www.freehaven.net/anonbib/topic.html.

Vliv postranních kanálů na soukromí

Odevzdáno na Fakultě informačních technologií Vysokého učení technického v Brně
dne 10. května 2006

Prohlášení

Prohlašuji, že jsem tuto ročníkovou práci vypracoval samostatně pod vedením Daniela Cvrčka. Uvedl jsem všechny literární prameny a publikace ze kterých jsem čerpal.

Tímto dávám Fakultě informačních technologií Vysokého učení technického v Brně svolení k použití a úpravám textu i jeho částí pro vědecké a výukové účely při zachování autorských práv. Současně souhlasím s tím, že programový kód, pokud byl vytvořen jako součást této práce, je možné používat v souladu s General Public Licence.

. . . . . .

Milan Tomášek

10. května 2006

Abstrakt

Má ročníková práce se zabývá vlivem postranních kanálů na soukromí a také bezpečnost uživatelů při provádění různých typů IT transakcí.

Základem hodnocení informačních systémů je standard nazývaný Common criteria. Jednou z částí tohoto standardu je třída nazývaná Soukromí, kterou se budu zabývat trochu podrobněji.

V oblasti skrytých kanálů se budu z mnoha jejich možných variant zabývat těmi, které jsou z našeho úhlu pohledu (komunikace na větší vzdálenosti) relevantní. U vybraných transakcí potom budu zkoumat vliv informací ze skrytých kanálů na soukromí a bezpečnost uživatelů.

Z dat získaných pomocí skrytých kanálů je také možné určit jejich informační hodnotu a na základě ní pak rozhodnout o tom, do jaké míry daný systém zaručuje anonymitu svých uživatelů.

Na závěr se pokusím o vytvoření co nejobsáhlejší klasifikace kontextů.

Klíčová slova

Common kritéria, bezpečnost, soukromí, skrytý kanál, kryptoanalýza, anonymita, informační hodnota transakce, kontext transakce, informační systém, analýza bezpečnosti.

Poděkování

Chtěl bych tímto poděkovat vedoucímu mého ročníkového projektu Ing. Danielu Cvrčkovi, Ph.D. za velmi dobrou spolupráci a za podněty k řešení mé práce.

Abstract

My year project is concerned with effects of side channels to privacy and security of users, while different IT transactions are executed.

The base of classification of information system is a standard called Common criteria. One of the main part of this standard is class called Privacy, which I'll be interested in more closely.

I'll be interested only in covert channels which are just relevant in case of our visual angle (communication for long distances). I'll search the influence of informations with privacy and security of users for some chosen transactions.

There is possibility of assigning information value of dates gained from covert channels. On the basis of the information value we can make decision on the level of system users anonymity.

In the end I'll try to create extensive classification of many different contexts.

Keywords

Common Criteria, security, privacy, covert channel, cryptoanalysis, anonymity, information value of transaction, context of transaction, information system, security analysis.

Obsah

Kapitola 1

Úvod

V rámci této práce se budu zabývat bezpečností, při provádění různých druhů transakcí v informačních technologiích a také mírou soukromí, která je zaručena uživatelům při různých typech komunikace. Dále se pokusím formulovat rizika, která při těchto transakcích vznikají a možné způsoby, jak těmto rizikům předcházet.

V první části se budu zabývat všeobecně uznávanými kritérii pro hodnocení bezpečnosti informačních systémů (Common Criteria) a pojmy, které s těmito kritérii úzce souvisí. Speciálně pak rozeberu oblast, zabývající se bezpečností a soukromím uživatelů. V závěru první části ještě budu definovat míry záruky hodnocení, určující požadavky na bezpečnost hodnocených informačních systémů.

V další kapitole budu pojednávat o tzv. skrytých kanálech, které se mohou v softwaru vyskytovat, jejich členění a definování profilu útočníka. Řeč bude hlavně o nebezpečí, které tyto kanály mohou způsobit v moderní kryptografii, o možnosti zneužití odposlechnutých informací neoprávněnými osobami, o negativním ovlivnění soukromí uživatelů a rizicích týkajících se obecné bezpečnosti. Také se pokusím specifikovat jakým směrem by se měly ubírat snahy o potlačení tohoto nebezpečí, jelikož je toto riziko v současné době hodně podceňované a podle mého zatím tato problematika nebyla adekvátně zkoumána.

Čtvrtá kapitola bude jakousi analýzou vybraných typických transakcí, definováním jejich kontextu a formulováním možného zneužití více, či méně citlivých informací ze strany neautorizované třetí osoby. Společně s vedoucím projektu jsme vybral transakce: placení platebními kartami, používání elektronického bankovnictví, telefonování pomocí mobilního telefonu a vybíraní elektronické pošty. V závěru této kapitoly se zaměřím i na informační hodnotu transakcí. Budu zkoumat míru entropie co se týče identity konkrétního uživatele a s tím související počet a povahu informací potřebných k profilování komunikujícího uživatele, případně i k zjištění jeho totožnosti.

Dále budu snažit vytvořit co nejobsáhlejší klasifikaci různých kontextů, čili jakýsi obecný

přehled všech možných typů informací, které jsou přenášeny v průběhu komunikace v informačních systémech. U všech těchto kontextů se budu snažit určit jejich informační hodnotu s ohledem právě na analýzu skrytých kanálů.

V samotném závěru práce se pak pokusím zhodnotit význam vytvořené klasifikace, zdali je na základě tohoto vytvořeného přehledu možné určit míru spolehlivosti systémů z pohledu zaručení soukromí uživatelů. Následovat bude zamyšlení o možném pokračování tohoto projektu.

Kapitola 2

Common Criteria (CC)

Jsou to společná kritéria pro hodnocení bezpečnosti informačních technologií. CC vznikla na základě již dříve používaných kritérií hodnocení, zejména amerických TCSEC a Federal Criteria, evropských ITSEC a kanadských CTCPEC. Na vývoji CC se podílely národní organizace, působící v oblasti bezpečnosti a standardizace, z šesti států světa, jmenovitě Kanady, Francie, Německa, Holandska, Velké Británie a Spojených států amerických a jsou posledním výsledkem úsilí o vytvoření společného standardu v oblasti hodnocení bezpečnosti informačních technologií. Hodnocení podle CC se soustřeďuje na hodnocení produktů IT, tzn. operační systémy, databázové systémy, síťové produkty, specializované bezpečnostní produkty, atd. Hodnocení sady bezpečnostních požadavků a specifikací pro daný produkt nazýváme v CC “bezpečnostní cíl” (Security Target, ST) a hodnocení implementačně nezávislé sady bezpečnostních požadavků nazývané v CC “profil ochrany” (Protection Profile, PP). ST a PP se hodnotí zejména z hlediska úplnosti a technické správnosti. Profily ochrany (PP), které úspěšně prošly hodnocením podle CC jsou zaznamenány do registrů PP a mluví se o nich jako o certifikovaných (registrovaných) profilech. V oblasti výstavby a hodnocení bezpečnosti informačních systémů pro zpracování utajovaných informací se CC mohou uplatnit pro specifikaci funkčních bezpečnostních požadavků a při stanovení požadované úrovně záruk (EAL) pro jednotlivé komponenty informačního systému. [8]

2.1 Důležité pojmy v souvislosti s CC

- EAL (Evaluation Assurance Levels) - míry záruky hodnocení. CC poskytuje 7 předdefinovaných balíků pro záruky, udávajících úroveň hodnocení a definujících požadavky na bezpečnost informačních systémů.
- CEM (Common Evaluation Methodology) - metodologie pro provádění hodnocení podle Common Criterií. CEM zahrnuje hodnocení na úrovních EAL1 až EAL4.

- EPL (Evaluated Products List) - jde o seznam produktů, které již byly certifikovány. Tyto seznamy jsou vydávány každou zemí, která provádí certifikace.
- PP (Protection Profile) - profily ochrany. Je to množina implementačně nezávislých bezpečnostních požadavků (zahrnující i EAL), které úspěšně prošly hodnocením podle CC. Tyto profily jsou organizovány do registrů PP.
- ST (Security Target) - bezpečnostní cíl, množina bezpečnostních požadavků pro daný produkt.
- TOE (Target of Evaluation) - je to výraz pro předmět hodnocení, kterým je konkrétní IT produkt, IT systém.
- TSF (TOE Security Functions) - funkce, zajišťující ochranu předmětu hodnocení.

2.2 Rozdělení CC

CC jsou rozdělena do 3 částí:

- Část 1: Úvod a všeobecný model

  V první části jsou uvedeny definice pojmů, je zde vysvětlena základní filozofie CC a je prezentován obecný model hodnocení. Důležitou součástí je vymezení několika stavebních prvků, které slouží pro jednotné vyjádření bezpečnostních požadavků.

- Část 2: Bezpečnostní funkční požadavky

  Ve druhé části jsou stanoveny funkční komponenty, které jsou používány jako standardní způsob vyjadřování funkčních požadavků. Jde o katalog funkčních komponent, rodin a tříd (celkem je zde 11 tříd). Dvě důležité funkční třídy, které jsou z hlediska tohoto projektu nejvíce důležité jsou třída zabývající se soukromím a třída popisující důvěryhodné cesty/kanály.

  - Třída **Privacy** (Soukromí): požadavky na soukromí poskytnou uživateli ochranu proti odhalení a zneužití jeho identity jiným uživatelem. Rodiny této třídy jsou zodpovědné za anonymitu (Anonymity), pseudonymitu (Pseudonymity), nespojitelnost (unlinkability) a nepozorovatelnost (Unobservability), (viz. CC a soukromí).
  - Třída **Trusted path/channels** (Důvěryhodné cesty/kanály): tato třída se zabývá komunikačními cestami mezi uživateli a TSF (TOE Security Functions) mezi TSF. Důvěryhodné cesty jsou tvořeny důvěryhodnými kanály. Uživatel TSF může inicializovat přenos, u kterého je zaručena ochrana před modifikací ze strany nedůvěryhodných aplikací.

- Část 3: Požadavky na záruky bezpečnosti

  Třetí část zahrnuje komponenty pro popis požadavků na záruky. Je katalogem komponent záruk, jejich rodin a tříd. Rovněž jsou v ní definována kritéria pro hodnocení profilů ochrany (PP) a bezpečnostních cílů (ST). V CC je pro oblast záruk definováno 8 tříd.

[1]

2.3 Míry záruky hodnocení (EAL)

CC poskytuje 7 předdefinovaných balíků pro záruky (assurance package), známých jako Evaluation Assurance Levels (EALs), v českém překladu míry záruky hodnocení. Jde o stupnici udávající úroveň hodnocení. Jsou dobře promyšlené, vyvážené a obecně aplikovatelné. Veškerá hodnocení IT podle CC se dnes provádějí na úrovni některé z EAL (převážně do úrovně EAL4).

Stručně lze jednotlivé úrovně popsat následujícím způsobem:

- EAL1 je vhodná, pokud je vyžadována určitá základní důvěra ve správnost fungování hodnoceného PP, ST nebo TOE, avšak hrozby nejsou považovány za vážné. Důvěry se dosahuje nezávislým testováním shody hodnoceného PP, ST nebo TOE s neformální funkční specifikací a zkoumáním předložených příruček pro uživatele.

- EAL2 již vyžaduje spolupráci vývojáře, který musí v podstatě dodat funkční specifikace, určité informace o návrhu bezpečnostních funkcí na úrovni globálního návrhu, tzv. high-level design a výsledky testování, vývoj si nevyžaduje více úsilí nežli je potřebné pro dodržování dobré komerční praxe, a v podstatě nepřináší zvýšení nákladů. Poskytuje nízkou až střední nezávisle ověřenou bezpečnost v případě, že není dostupná kompletní informace z fáze vývoje. Důvěry se dosahuje analýzou vyžadované dokumentace, ověřením výsledků některých testů, analýzou síly funkcí a analýzou zřejmých zranitelností.

- EAL3 je možno ještě dosáhnout bez podstatných změn základních existujících vývojářských praktik. Je aplikovatelná v případě, že se vyžaduje střední úroveň nezávisle ověřené bezpečnosti a je nutné důkladné zkoumání TOE (ST, PP). Navíc oproti EAL2 je potřeba rozsáhlejší testování, kontroly vývojového prostředí a zajištění správy konfigurace.

- EAL4 stále umožňuje pohybovat se v rámci dobré komerční vývojářské praxe. I pře svoji přísnost nevyžadují zásadní specializované znalosti a dovednosti. EAL4 je nejvyšší úrovní záruk, kterou lze dosáhnout za “rozumné náklady” zpětně pro již existující produkt. Poskytuje střední až vysokou úroveň záruky nezávisle ověřené bezpečnosti. Navíc oproti EAL3 se již vyžaduje také detailní návrh, tzv. low-level design TOE, neformální model bezpečnostní

politiky TOE a dodání určité podmnožiny implementace (např. část zdrojového kódu bezpečnostních funkcí). Analýza zranitelnosti musí demonstrovat odolnost vůči průniku útočníků s nízkým potenciálem pro útok.

- EAL5 vyžaduje aplikaci speciálních technik bezpečnostního inženýrství ve středním rozsahu. Dané TOE je již navrženo a vyvíjeno s cílem dosáhnout úrovně záruk EAL5. Nepředpokládá se však velké zvýšení nákladů oproti EAL4. EAL5 je tak vhodná v případech, kdy se vyžaduje vysoká úroveň záruky nezávisle ověřené bezpečnosti aniž by náklady na specializované techniky byly příliš vysoké. Oproti EAL4 je vyžadováno dodání kompletní implementace TOE, formální model bezpečnostní politiky TOE, poloformální prezentace funkčních specifikací, poloformální globální návrh (high-level design) a poloformální demonstrace korespondence. Analýza zranitelnosti musí demonstrovat odolnost vůči průniku útočníků se středním potenciálem pro útok. Vyžaduje se také analýza **skrytých kanálů** a modularita návrhu.

- EAL6 vyžaduje aplikaci technik bezpečnostního inženýrství do přísného vývojového prostředí a je určena pro vývoj TOE sloužícího pro ochranu vysoce hodnotných aktiv proti význačným rizikům, kdy lze odůvodnit dodatečné náklady. Navíc oproti EAL5 se vyžaduje poloformální detailní návrh, rozsáhlejší testování, návrh TOE musí být vrstvený, prezentace implementace strukturovaná. Analýza zranitelnosti musí demonstrovat odolnost vůči průniku útočníků s vysokým potenciálem pro útok. Analýza skrytých kanálů musí být systematická. Vyšší nároky jsou kladeny na správu konfigurace a kontroly vývojového prostředí.

- EAL7 je použitelná pro vývoj produktů určených do extrémně rizikového prostředí nebo kde vysoká hodnota aktiv ospravedlňuje vyšší náklady. Praktické použití EAL7 je v současnosti omezeno na TOE a úzce vymezenou bezpečnostní funkčností, kde lze provést formální analýzu v požadované míře. Vyžaduje se plná formalizace, formální model bezpečnostní politiky, formální prezentace funkčních specifikací a high-level návrhu, poloformální detailní návrh, formální a poloformální demonstrace korespondence. Testování se vyžaduje na úrovni bílé skříňky (white-box) a musí být dosaženo úplného nezávislého potvrzení výsledků všech předložených testů. Složitost návrhu musí být minimalizována.

2.4 CC a soukromí (Privacy)

Problematikou soukromí se v CC zabývá třída Privacy (Soukromí) náležící do části bezpečnostních funkčních požadavků. Tato třída, jak je již z názvu patrné obsahuje požadavky na soukromí, které uživateli poskytují ochranu proti odhalení a zneužití jeho identity.

Tato třída sestává ze čtyř rodin, které pak dále obsahují jednotlivé komponenty, viz. obr. 2.1.

2.4.1 Anonymita (Anonymity)

Požadavky anonymity poskytují ochranu uživatelovy identity.

Komponenta 1 (Anonymity): Tato komponenta vyžaduje, aby bylo uživateli umožněno použití zdrojů nebo služeb, aniž by byla odhalena jeho identita. TSF (TOE security functions) mají zajistit, aby nebylo možné zjistit skutečné jméno uživatele, v závislosti na operacích, které provádí nebo objektů, které používá, či ostatních osob, s nimiž komunikuje.

Komponenta 2 (Anonymity without soliciting information): Anonymita bez vyžádaných informací umocňuje požadavky komponenty 1. TSF se nemohou dotazovat na identitu uživatele, dále musí zajistit uživatelem požadované služby nad objekty bez vyžádání jakékoliv zmínky o skutečném jméně uživatele.

2.4.2 Pseudonymita (Pseudonymity)

Pseudonymita zajišťuje podobně jako anonymita možnost uživatele používat zdroje nebo služby, bez toho, aniž by byla odhalena jeho identita, ale aby mohl být stále zodpovědný za jejich použití.

Komponenta 1 (Pseudonymity): Pseudonymita požaduje, aby ostatní uživatelé nebo subjekty nebyli schopni určit identitu jiného uživatele v závislosti na operaci, kterou vyvolal nebo objektů, které používá, či ostatních osob, s nimiž komunikuje. Tento uživatel však musí být stále zodpovědný za svoje akce. Systém musí také být schopný poskytnout počet aliasů uživatele ostatním subjektům. Dále musí být zajištěno, aby bylo na základě zadaného aliasu a hesla možné identifikovat uživatele.

Komponenta 2 (Reversible pseudonymity): Oboustranná pseudonymita požaduje, aby bylo možné určit identitu uživatele na základě poskytovaného aliasu (pouze autorizovaným důvěryhodným osobám).

Komponenta 3 (Alias Pseudonymity): Požaduje, aby byla dodržována jisté pravidla pro tvorbu aliasů sloužících jako zástupná jména uživatelovy identity. TSF musí zajistit poskytnutí aliasu ke skutečnému uživatelskému jménu, ale tento alias nesmí být spojován s již dříve vytvořenými aliasy daného uživatele.

2.4.3 Nespojitelnost (Unlinkability)

V této je zajištěno, že uživatel může opakovaně používat zdroje, či služby, bez toho, aniž by ostatní osoby byly schopny spojit toto jejich použití dohromady.

Komponenta 1 (Unlinkability): TSF musí zajistit, aby ostatní uživatelé nemohli zjistit, zda stejný uživatel spustil určitou konkrétní operaci v systému.

2.4.4 Nepozorovatelnost (Unobservability)

Rodina Unobservability chrání uživatele při používání prostředků a služeb. Je totiž zajištěno, že uživatel může použít prostředky a služby aniž by kdokoliv ostatní byl schopen zpozorovat, že jsou právě používány.

Komponenta 1 (Unobservability): Zajišťuje, že uživatelé, ani jiné subjekty nejsou schopny zjistit, zdali je konkrétní operace právě prováděna.

Komponenta 2 (Allocation of information impacting unobservability): Alokace informací ovlivňujících nepozorovatelnost vyžaduje, aby TSF poskytovaly specifické mechanismy k vyhnutí se koncentraci funkcí souvisejících se soukromím v rámci hodnoceného systému. Takové soustředění by mohlo mít negativní dopad na nepozorovatelnost, v případě, že by nastal bezpečnostní kompromis.

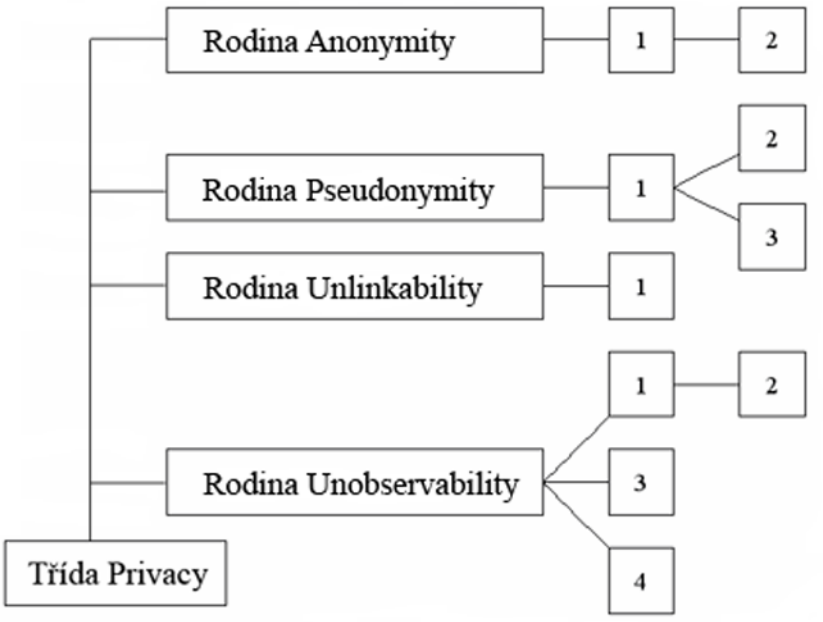
Komponenta 3 (Unobservability without soliciting information): Nepozorovatelnost bez vyžádaných informací požaduje, aby se TSF nepokoušely získat soukromé informace, které by teoreticky mohly být použity k ústupkům co se týče nepozorovatelnosti (musí poskytnou subjektu službu, aniž by došlo k vyžádání soukromé informace).

Komponenta 4 (Authorized user observability): Pozorovatelnost autorizovaného uživatele vyžaduje, aby TSF zajistily jednomu nebo více autorizovaným uživatelům využití prostředků, či služeb.

2.4.5 Dekompoziční diagram

Na obrázku 2.1 můžeme vidět strukturu třídy Soukromí, zobrazující rodiny třídy a jejich jednotlivé komponenty. Tento diagram nám může ukázat hierarchické vazby mezi jednotlivými komponentami (pokud existují). Například u rodiny Anonymity je komponenta 2 hierarchicky závislá na komponentě 1. V případě rodiny Pseudonymity jsou komponenty 2 a 3 závislé na komponentě 1,

ale v rodině Unobservability je komponenta 2 závislá pouze na komponentě 1 (nikoliv na komponentách 3 a 4). [3]



Obrázek 2.1: Dekompoziční diagram třídy Privacy

Kapitola 3

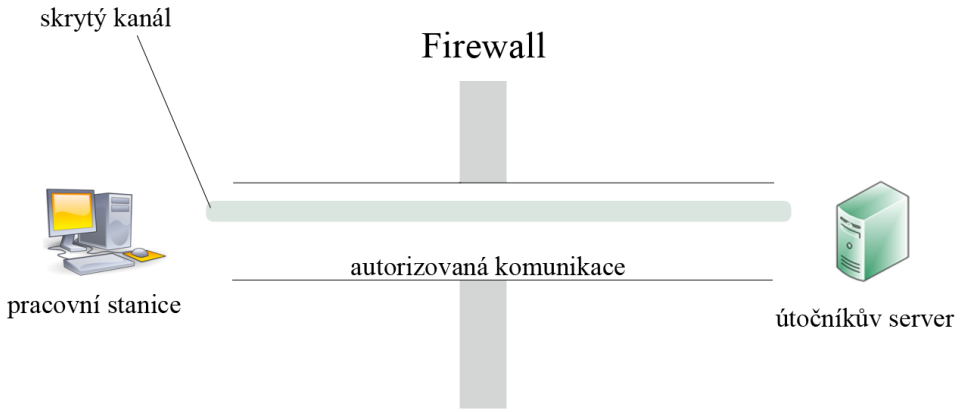
Skryté (postranní) kanály

Skrytým kanálem nazýváme každý nežádoucí způsob výměny informací mezi kryptografickým modulem a jeho okolím. Jde o komunikační kanály cestami, které k tomu nebyly sestaveny, ale jejich použití je možné. V současné době většina tzv. bezpečných zařízení produkuje při provádění kryptografických algoritmů informace ve formách, se kterými návrh těchto zařízení nepočítal. Cesty, kterými unikají tyto nežádoucí informace, se nazývají skryté kanály a množství informací, které z nich lze získat, závisí na formě skrytého kanálu. V mnoha případech je možné tyto informace efektivně analyzovat a využít je pro narušení bezpečnosti (kompromitaci) bezpečného zařízení. Skryté kanály v operačních systémech dovolují procesům nepozorovaně komunikovat i přes bezpečnostní zóny, definované nastavením systému. Používá se zatížení procesoru, názvy dočasných souborů a prakticky jakýkoliv jiný sdílený prostředek.

Útoky využívající postranní kanály by se daly v podstatě rozdělit do dvou skupin.

1. Pasivní útoky - jejich podstata spočívá v měření různých typů veličin (spotřeba proudu, elektromagnetické vyzařování) V tomto případě dochází k u skrytých kanálů k využívání komunikačních cest, vytvořených ostatními procesy.

2. Aktivní útoky - při tomto typu útoku se cizí osoba nespokojí pouze s odposlechem různých hodnot, ale záměrně v systému vyvolává chyby a poruchy. V případě aktivního útoku vytváří skrytý kanál vlastní komunikační trasu. Právě tyto typy útoků nás budou zajímat. Na obr. 3.1 můžeme vidět typické provedení skrytého kanálu. Firewall propouští konkrétní autorizovanou komunikaci (HTTP, HTTPS, FTP, MSN, atd.). Útočník vytvoří skrytý kanál v oblasti povolených protokolů.[10]



Obrázek 3.1: Ukázka typického skrytého kanálu

3.1 Klasifikace skrytých kanálů

1. **Ztrátové a neztrátové kanály** – Pokud je pravděpodobnost doručení všech dat rovna jedné, Lze takový kanál nazvat neztrátovým. Pokud je určitá pravděpodobnost ztráty dat, musí se použít odpovídající technika korekce chyb.

2. **Paměťové a časové kanály** – jsou rozděleny podle média, které používají. Paměťové používají zápis dat do paměti a principem časových kanálů je zjištění doby přístupu procesů ke zdroji a dobou jeho provádění.

3. **Hromadné kanály** – u tohoto typu můžeme použít několik jednotlivých cest k paralelnímu přenosu jedné informace, s použitím synchronizace přenášených dat.

   Hromadné komunikační kanály mohou být použity coby kompenzace ceny za synchronizaci, popřípadě i dekódování informace. Pokud jsou všechna data vysílána a přijímána sériově pak říkáme, že jde o kanál sériově shromážděný, pokud paralelně, jde o paralelně shromážděný kanál. Kombinace sériově i paralelně shromážděného kanálu je taky možná (například data mohou být zasílána sériově a přijímána paralelně a naopak), ale není příliš efektivní.

4. **Podprahové kanály** - nejedná o typického zástupce skrytých kanálů. Narozdíl od předchozích variant, kdy šlo o nevědomě vzniklé postranní kanály, jsou totiž podprahové kanály implementovány do systému zcela záměrně a útočníkem je v tomto případě vývojář takového systém. Je-li tento typ kanálu implementovaný do kryptografického zařízení, bez vědomí

uživatel, pak mluvíme o zvláštním typu postranního kanálu nazývaném jako kleptografický. [6]

3.2 Typy informací získaných pomocí skrytých kanálů

- **Chybová hlášení** - v tomto případě odposlouchává útočník zprávy, které zasílá napadený uživatel serveru. Pokud bude následně opakovaně zasílat fragmenty těchto zpráv serveru sám útočník, tvářící se jako právoplatný uživatel, bude mu serverem zpět odesílán chybový report. Na základě těchto reportů je pak útočník již schopen dešifrovat i původní znění zprávy.

- **Časové prodlevy** - jsou založeny faktu, že časy odezvy a prodlení v přístupu procesu například k procesoru mohou být nosiči informací. Jedna z variant útoku je například měření času potřebného k zašifrování zprávy, která vychází z toho, že určité operace, které závisí na tajném klíči trvají krátkou nebo dlouhou dobu v závislosti na hodnotách jednotlivých bitu klíče (v případě nuly je výpočet rychlejší, v případě jedničky je pomalejší a to cca dvojnásobně).

- **Spotřeba paměti** - velikost využité paměti při vykonávání daného procesu procesorem může být, podobně jako spotřebovaný čas výpočtu, také podstatnou informací.

- **Elektromagnetické vyzařování** - tento typ informace narozdíl od předchozích typů záleží pouze na fyzikálních vlastnostech napadeného modulu. Nedochází k odposlechu informací vzdáleně, ale zaměřuje se na měření elektromagnetických vln vyvolaných hardwarem, na kterém běží procesy. Jelikož intenzita vyzařování klesá s kvadratickou vzdáleností od zdroje záření, je možnost zisku informací z tohoto zdroje velice omezená. Tento způsob odposlouchávání bohužel není brán jako trestná činnost. Do této kategorie informací by se dalo zahrnout i akustické a tepelné vyzařování zařízení.

- **Diferenciální analýza spotřeby proudu, napětí** - principem je, jak již název napovídá, měření spotřeby. Velikou výhodou oproti měření doby trvání výpočtu je informace o chování relativně malé části kódu, čímž se tato analýza stává daleko efektivnější (ovšem s pouze na omezenou vzdálenost). V současnosti se také objevuje kombinace analýzy času a spotřeby proudu.

- **Otisky prstů na klávesnici, atd.**

3.3 Profil útočníka

Je také důležité uvědomit si, jak vypadá model útočníka a které typy skrytých kanálů jsou pro nás relevantní. Z našeho pohledu bude útočník osoba, která příslušnou komunikace sleduje vzdáleně, pomocí zařízení připojeného kdekoliv na trase mezi dvěma komunikujícími subjekty. Tím pádem vůbec nemusíme brát v potaz variantu kdy je podmínkou ke získání informací, aby se útočník nacházel v bezprostřední blízkosti napadeného zařízení (různé typy vyzařování, otisky prstů, atd.).

3.4 Postranní kanály a kryptoanalýza

Když mluvíme o postranních kanálech v souvislosti s kryptoanalýzou, můžeme říct, že je to každá informace o fungování šifrovacího systému, kterou dá program útočníkovi k dispozici.

Kryptoanalýza je věda zabývající se luštěním matematických mechanismů ochrany dat, je velice úzce spojena s kryptografií, která tyto mechanismy vytváří a vylepšuje (jejich spojením vzniká věda nazvaná kryptologie).

Problematika postranních kanálů je v oblasti kryptoanalýzy relativně nová záležitost a přináší revoluční útočné metody, které v historii kryptografie nemají obdoby. V tomto případě se totiž nepokouší útočník rozlomit šifru hrubou silou a nesoustředí se na její matematickou podstatu, ale zaměřuje se na její nejslabší místo, kterým je způsob její implementace.

Ukazuje se, že riziko prolomení špatně navrženého systému je i při použití dokonalého šifrovacího algoritmu neúnosně velké. a proto by se měly snahy kryptoanalytiků především zaměřit na snížení tohoto typu nebezpečí.[9]

3.5 Zachování soukromí a obecná bezpečnost

Když vezmeme v potaz, že s využitím skrytých kanálů by mohl případný útočník obejít šifrovací algoritmus bez jeho skutečného prolomení, je sebedokonalejší šifrovací metoda zbytečná. Ohrožena je tím pádem nejen ztráta soukromí uživatelů, ale také obecná bezpečnost obyvatel, jelikož by molo dojít k úniku takových informací, jako jsou například seznamy chráněných svědků, vojenské materiály, lékařské záznamy, apod.

Možnosti jak získat tyto citlivé údaje jsou v zásadě dvě. V prvním případě jde o neoprávněnou osobu která napadne počítač zvenku (nedostatky v systému, které mohou vést k úniku informací), v tom druhém jde o samotného výrobce vámi používaného šifrovacího softwaru, který ve vlastním produktu úmyslně vytvoří skryté cesty pro pozdější tajnou komunikaci (tzv. podprahové kanály).[5]

3.6 Úpravy standardu

Postranní kanály jsou v dnešní době považovány za jednu z největších hrozeb moderní kryptografie. Bohužel tyto typy útoku doposud nebyly dostatečně zkoumány a proto proti nim zatím nemohly být vytvořeny adekvátní opatření. Problémem je, že ani norma FIPS PUB 140-2, zabývající se bezpečností kryptografických modulů, ochranu proti těmto kanálům neřeší. Je to jednak vůli již zmiňované mladosti této problematika a za druhé také kvůli potenciálně velkému množství skrytých kanálů.

Na druhou stranu, veškeré výhrady ohledně bezpečnosti šifer v souvislosti s postranními kanály se týkaly pouze způsobu jejich implementace, nikoliv jejich podstaty.

S ohledem na zachování vyšší míry soukromí a bezpečí by měl být větší dohled nad výrobci programového vybavení a to zvláště v těch případech, kdy příslušný software manipuluje s tajnými daty. Také by bylo vhodné efektivně a systematicky stíhat osoby které infiltrací do cizích systémů v podstatě provádějí trestnou činnost srovnatelnou například s vykradením banky.

Kapitola 4

Analýza bezpečnosti transakcí v IS

V této kapitole se budeme zabývat různými typy transakcí, stanovíme jejich informační hodnotu a budeme klasifikovat kontext ve kterém jsou transakce prováděny. Podrobná analýza je potřebná, potřebná pro pozdější určení požadavků na bezpečnost systému a pro uvědomění si všech možných rizik, které by mohly v souvislosti s transakcemi vzniknout.

4.1 Vybrané typické transakce v IS

Z nepřeberného výčtu transakcí, které se ve světě informačních technologií uskutečňují jsme vybrali následující:

- Platby pomocí platebních karet
- Elektronické bankovnictví
- Mobilní telefonování
- Vybírání elektronické pošty

4.1.1 Platby pomocí platebních karet

Platební karty jsou v dnešní době čím dál víc se rozšiřující nástroj pro placení na internetu, v obchodech, či restauracích. Hlavní výhodou je jejich univerzálnost. Uživatel nemusí mít mnoho bankovních účtů pro placení přes transakční systém a specifické banky. Pomocí platební karty může zaplatit téměř jakýkoliv klient bez ohledu na to, jaká banka mu jeho kartu vydala.

Rozdělení platebních karet

Elektronické karty jsou nejrozšířenějším typem karet. Jsou použitelné pouze pro transakce, které jsou online ověřeny v kartovém centru, tedy pro výběry z bankomatů a platby u obchodníků disponujících elektronickým platebním terminálem.

Princip systému je následující. Po potvrzení objednávky za zboží či službu je klient přesměrován na důvěryhodnou (pro asociaci VISA/MasterCard) a verifikovanou třetí stranu, kde vloží informace o své platební kartě a potvrdí provedení transakce. Poté je zjištěna autenticita držitele karty na straně vydavatele karty, tedy ověření platnosti karty. Pokud je výsledek kladný, dochází teprve k autorizaci platby a jejímu následnému zaúčtování. Důvěryhodné třetí strany poskytující autorizační rozhraní platby jsou v ČR například Global Payments Europe a jejich systém PayMUZO, dále samostatná implementace České spořitelny. Výhody této metody jsou, poměrně vysoká bezpečnost prováděných transakcí a také univerzálnost použití.

Co se bezpečnosti transakcí pomocí platební karty týče, není problémem ani tak bezpečnost systému jako takového, ale špatná disciplína na straně uživatelů. Jde o nedostatečnou ochranou přístupových hesel a PIN kódů.

Výhodou elektronických karet z hlediska bezpečnosti informací je větší utajení osobních údajů o majiteli karty, kdy obchodník nezná téměř žádné údaje o zákazníkovi a nemůže tudíž dojít ke snížení soukromí majitele karty. Výhodou je také nulová možnost zneužití zablokované karty.

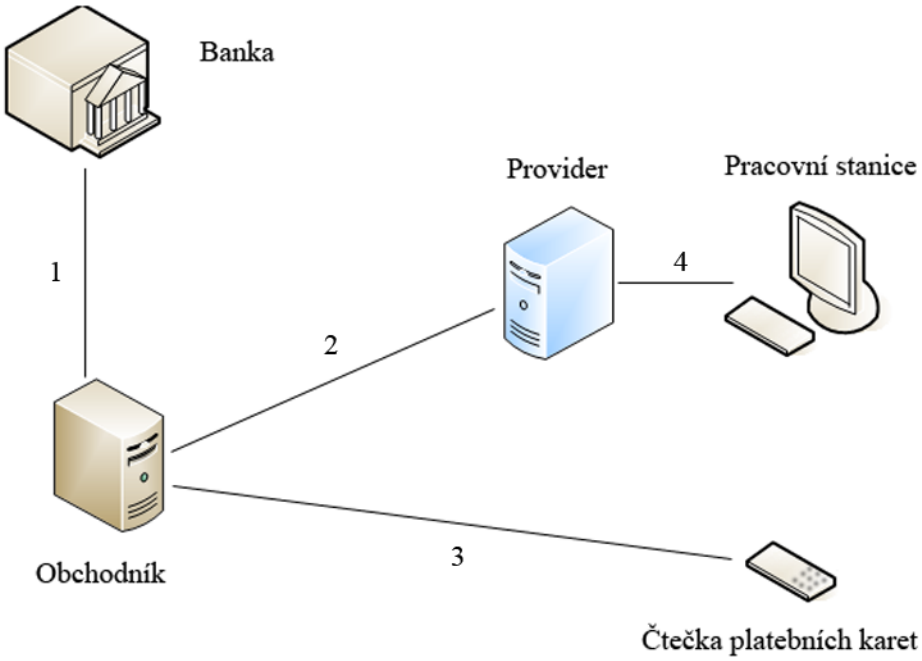
Embosované karty se oproti elektronickým kartám liší v tom, že mají plasticky vytištěny veškeré informace o majiteli karty, její platnosti atd. Platba se provádí tak, že obchodník otiskne údaje z karty na účet, který zákazník podepíše.

Výhodou Embosovaných karet je, možnost použití na více místech než karty elektronické. Naopak, velkou nevýhodou je daleko větší možnost zneužití karty i po nahlášení její ztráty. Obrovské riziko při placení tímto typem karet tkví v možnosti obchodníka shromažďovat osobní údaje o zákaznících, o produktech které kupují, kolik peněz za ně platí atd.

V případě vytvoření organizovaného seskupení takovýchto obchodníků by pak bylo teoreticky možné vytvořit databázi zákazníků a určit kdy provádějí svoje platby, kde se platby uskutečňují, jaké produkty si konkrétní osoba kupuje, množství peněz, které daný zákazník utratí za určité období. Takovéto informace by se mohly stát velice dobrým obchodním artiklem.

4.1.2 Elektronické bankovnictví

Převod finančních prostředků z jednoho účtu druhý pomocí elektronického bankovnictví je další typická IT transakce, která je díky masovému nástupu internetu do domácností rozšířená mezi



Obrázek 4.1: Schéma placení platební kartou

širokou veřejností. Většina bank v dnešní době nabízí možnost připojit se na zabezpečené internetové rozhraní, pomocí kterého je možné zasílat finanční prostředky z účtu vlastníka.

S bankou je možné komunikovat v zásadě dvěma způsoby:

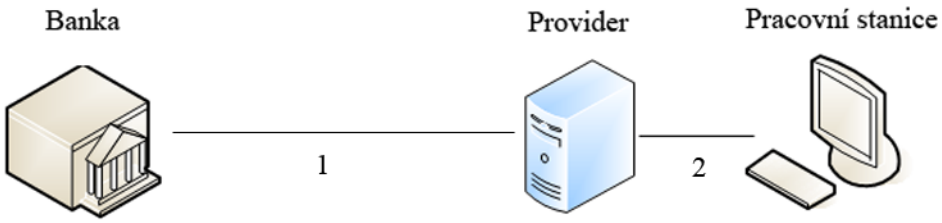
- Přes **tenkého klienta**, kdy se klient spojuje s bankou pomocí internetového prohlížeče.
- Přes **bankou dodanou aplikaci**, kdy si klient na svém počítači nainstaluje příslušný software vytvořený přímo pro komunikaci se svojí bankou.

Co se týče bezpečnostních technik, je celé spojení mezi bankou a klientem šifrováno pomocí SSL (Secure Sockets Layer). Pro ověření, zda opravdu probíhá komunikace s bankovní aplikací se banka musí prokázat certifikátem třetí strany CA (Certification Authority). Klient banky se prokáže svým identifikačním jménem a příslušným heslem.

V cestě by transakci neměla stát žádná nedůvěryhodná třetí strana, transakce by měla být vždy pouze na úrovni klient a jeho banka. Velice důležitá je disciplinovanost účastníků platební transakce (ochrana přihlašovacích jmen a hesel, ochrana osobního počítače pomocí kterého transakce probíhá před škodlivým softwarem).

Určitě největší riziko při používání elektronického bankovnictví spočívá v nedostatečné ochraně počítačů ze strany uživatelů. Do počítače může být například nainstalován tzv. RAT (Remote Access Tool) program, což je v podstatě speciální typ trojského koně, který umožňuje vzdálenou správu uživatelova počítače. V takovém případě si pak může třetí osoba například zjistit seznam stisknutých kláves apod. Také se nedá doporučit používání počítačů u kterých člověk nemá plnou kontrolu nad bezpečnostními nastaveními. Typickým příkladem jsou například internetové kavárny.

Ze strany banky pak může teoreticky dojít k úniku citlivých informací o klientech, jako je stav jejich účtu, uskutečněné transakce, kompletní osobní údaje (jméno, bydliště, rodné číslo).



Obrázek 4.2: Schéma komunikace u elektronického bankovnictví

4.1.3 Mobilní telefonování

Každý uživatel mobilní sítě má přiděleno svoje telefonní číslo MSISDN. Síť GSM ve skutečnosti používá k identifikaci jednotlivých uživatelů tzv. IMSI číslo (International Mobile Subscriber Identity). Aby však nešlo vystopovat konkrétní telefon a tak i jeho majitele, přiděluje vždy ústředna po zapnutí telefonu jeho dočasnou identitu, jde o náhodně generované číslo TMSI.

Ověřeni “pravosti” uživatele má na starosti Autentifikační centrum (AuC). Účelem je zabránit přihlášení do sítě jakéhokoli zařízení, které se snaží vypadat jako běžný uživatel a volat na jeho účet. K ověření pravosti se používá algoritmus A3 a A8 (označovaný také A38), který se nachází na SIM kartě

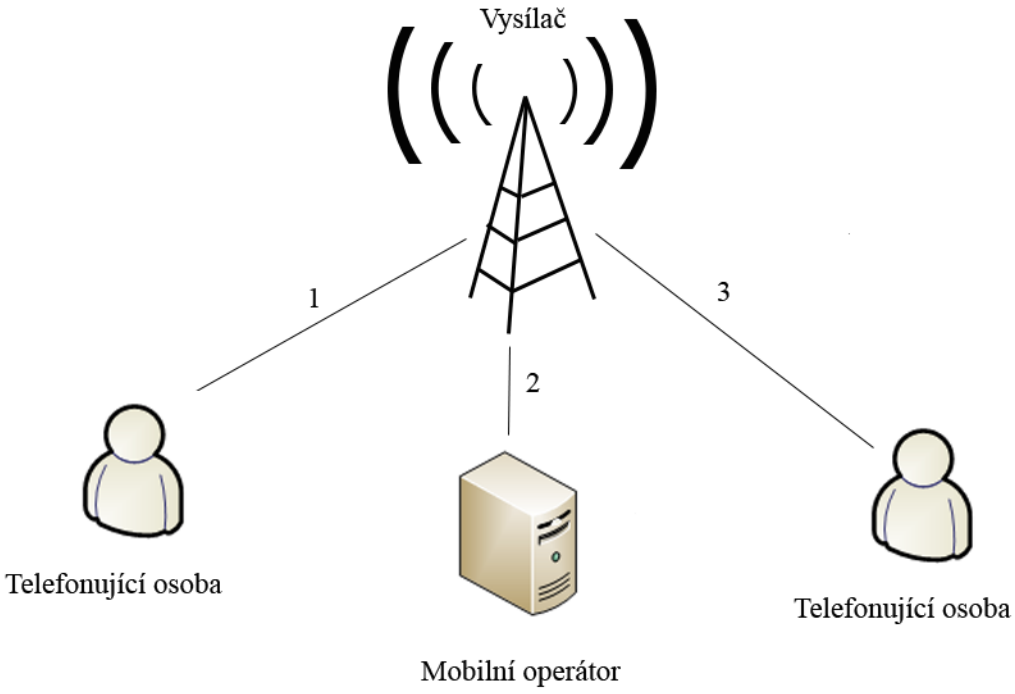
Po zapnutí zašle telefon svoje IMSI. Odezvou sítě je náhodné číslo o velikosti 128 bitů. Algoritmus A3 na základě přijatého čísla a tajného klíče vygeneruje 32 bitové číslo, které se musí shodovat s číslem vygenerovaným ústřednou. Poté algoritmus A8 vygeneruje 64 bitový šifrovací klíč, který je použit při šifrování přenášených dat.

Podoba algoritmu A38 sice není pevně daná, ale většina operátorů používá stejný algoritmus COMP128. Tento algoritmus se však již podařilo ze SIM karty vyčíst. Z toho vyplývá teoretická možnost neoprávněného uživatele připojit se do sítě jako její právoplatný uživatel.

Další fází po navázání spojení s ústřednou je šifrování dat. Veškerá data jsou chráněna proti odposlouchávání pomocí šifrování algoritmem A5. Tento algoritmus, stejně jako vlastní šifrování, je implementován kvůli rychlosti těle telefonu. Výstupem A5 je vždy dvojice hesel dlouhá 114 bitů, jedno pro odchozí data ve směru z mobilního telefonu do centrální stanice, druhé heslo je pro příchozí data v opačném směru.

Pro odposlech hovoru je nutné znát šifrovací klíč (čili je potřeba znát tajný klíč na SIM kartě). Riziko úspěšného napadení systému se ještě zvyšuje skutečností, že 64 bitový šifrovací klíč má ve skutečnosti pouze 54 bitů a na 64 bitů je doplněn nulami. Z těchto důvodů není síť GSM vhodná pro přenos důvěrných dat, popřípadě je nutné pro jistotu použít vlastní zabezpečovací algoritmy.

Dalším slabým místem, ze kterého je možné provádět odposlech cizích hovorů je samotná centrální stanice, kde jsou samozřejmě dostupné všechny potřebné údaje (algoritmus A38, A5, tajný klíč). V dnešní době je odposlouchávání hovorů z mobilních telefonů častým prostředkem pro odhalování trestné činnosti, avšak hranice mezi využitím a zneužitím těchto technik je velice tenká.



Obrázek 4.3: Schéma komunikace u mobilního telefonování

4.1.4 Vybírání elektronické pošty

Používání elektronické pošty je určitě jedním z nejběžnějších a nejpoužívanějších komunikačních prostředků dnešní doby. Jako takový však v sobě také skrývá velká rizika při jeho používání, hlavně pak v kombinaci s nedisciplinovanými a počítačově méně erudovanými uživateli. Pro výměnu dat mezi jednotlivými servery, popřípadě mezi serverem a uživatelem existují následující komunikační protokoly.

Protokoly používané pro elektronickou poštu

SMTP (Simple Mail Transfer Protokol) definuje způsob, jakým si jednotliví MTA (Mail Transfer Agent) vyměňují zprávy, nikoliv však způsob a místo jejich uchovávání. Zajišťuje spolehlivý a efektivní přenos (komunikace probíhá přes port 25). Pro komunikaci se mezi dvěma účastníky (sender, receiver) vytvoří komunikační kanál, skrz který jsou zasílány příkazy druhé straně.

POP3 (Post Office Protocol, Version 3) je protokol používaný pro přístup klientů k poštovnímu serveru (standardně probíhá komunikace přes port 110). Komunikace probíhá vždy mezi klientem a serverem pomocí zasílání zpráv. Připojení klienta k serveru můžeme rozdělit do tří fází - Spojení se serverem, autorizace klienta, aktualizace serveru (provedení úkonů požadovaných klientem).

IMAP4 (Internet Mail Access Protocol, Version 4) je podobně, jako POP3 používán ke komunikaci klienta se serverem. Výhodou protokolu IMAP4 oproti POP3 je však ten, že nepřenáší celý mailbox ze serveru na počítač, ten je stále na serveru a klient s ním může pracovat, jako by byl mailbox na jeho osobním počítači. Protokol IMAP4 může pracovat stejně jako protokol POP3. Jistou nevýhodou tohoto protokolu je však jeho výrazně menší rozšíření oproti POP3.[2]

Hlavní rizika při používání elektronické pošty

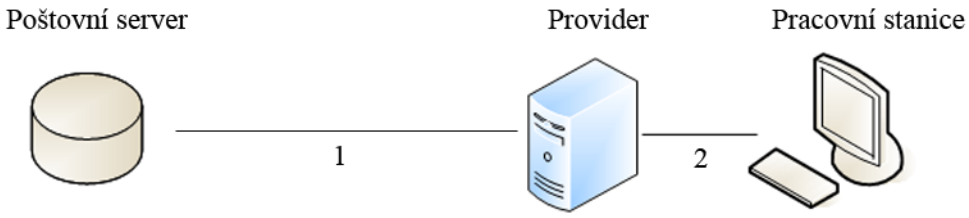
SPAM jde o pojem označující nevyžádanou poštu především reklamního charakteru, která sice sama o sobě nijak neškodí, ale do značné míry uživatele obtěžuje a omezuje (zabírá místo ve schránce, musí se mazat neustále přicházející zprávy, snižuje se přehlednost). Alarmující je fakt, že v dnešní době SPAM představuje 60% z veškeré doručené pošty. Existují sice algoritmy filtrující tento typ nevyžádaných zpráv, nicméně problém se tím neřeší, ale pouze zmírňuje. Daleko efektivnější varianta proti těmto útočníkům by pravděpodobně byly soudně vymahatelné sankce, které by znatelně převyšovaly možné zisky plynoucí z rozesílání SPAMu. [7]

Viry jsou velice významnou hrozbou na poli elektronické komunikace. Narozdíl od SPAMu, kdy je “útočník” dobře znám a přijímané zprávy jsou fakticky neškodné, je situace v případě

počítačových virů poněkud odlišná. Viry se šíří v přílohách emailů a při jejich otevření mohou způsobovat často katastrofální následky. Z důvodu nemožnosti identifikovat původce útoku je jediným spolehlivým řešením jak se vyhnout nepříjemnostem použití aktualizovaného antivirového programu a neotevírání podezřelých příloh v příchozí poště.

Ztráta soukromí je další nebezpečí, o kterém se dá v souvislosti s elektronickou poštou mluvit. Uživatel je při registraci poštovního účtu často nucen zadávat soukromé informace, které jsou provozovateli příslušného serveru plně k dispozici a i když se zaváže k diskrétnímu nakládání s těmito daty, možnost zneužití citlivých údajů uživatelů je zjevná. Také obsah poštovních schránek není zcela v bezpečí před nepovolanými osobami. Případnému útočníkovi stačí znát pouze přihlašovací jméno a heslo. Může jít jednak o interního zaměstnance, který má přístup ke všem datům, nebo osobu "zvenčí", která získala tyto údaje například odposlechem uživatele.

Proto je dobré chránit svoje přihlašovací jméno a heslo a pokud možno vůbec nepoužívat poštovní schránku jako úložiště důležitých dokumentů a dat.



Obrázek 4.4: Schéma komunikace s poštovním serverem

4.2 Informační hodnota vybraných transakcí

Informační hodnotu jednotlivých transakcí budeme brát jako míru entropie, čili pravděpodobnost, s jakou jsme schopni určit konkrétního uživatele, při uvažování různého typu informací, které jsou v průběhu transakcí přenášeny. Nejprve je nutné si stanovit, jaké informace o uživateli je schopný útočník zachytit při komunikaci uživatele cílem a seřadit tyto informace na základě jejich vypovídací hodnoty. Budeme zkoumat, do jaké míry třetí osoba schopná určit profil uživatele, či dokonce v kterém okamžiku (jestli takový okamžik nastane) je útočník schopen odhalit jeho přesnou identitu.

Kvalifikovat, jaké informace je a není možné získat je velice obtížné. Vždy totiž musíme prát v potaz také lidský faktor, takže k úniku informací může dojít také v rámci všech subjektů majících přístup k informacím přímo na komunikační cestě. Jde například o správce serveru kde jsou uloženy schránky elektronické pošty, obsluhu telefonní ústředny nebo obchodníka u kterého nakupujeme zboží. Všechny tyto osoby mají pochopitelně přístup k tajným informacím. Také vývojáři systémů mohou záměrně implementovat komunikační kanály, které potom zneužijí pro vlastní potřebu.

Dalším úzkým místem bezpečnosti systému je také samotný jeho uživatel, který ať už z nedbalosti, či nevědomosti nedostatečně ochraňuje svůj počítač před infiltrací cizích osob.

V těchto všech případech by jsme mohli říct, že ke kompromitaci komunikujícího uživatele a ke zjištění jeho skutečné identity může dojít velice jednoduše a prakticky při jakémkoliv typu transakce.

Proto se budeme v následujících přehledech zabývat opravdu pouze variantou, kdy útočník nemá žádnou spojitost s institucemi figurujícími při provádění transakcí a kdy se jedná pouze o neúmyslně odeslané informace, které je možné zachytit.

Následuje rozbor jednotlivých transakcí, které byly popsány výše.

- **Platby pomocí platebních karet**

Typ informace	**Zúžení okruhu relevantních uživatelů**	**Získání informace (obr. 4.1)**
Typ transakce	V případě platby pomocí osobního počítače víme, že uživatel musí mít jednak přístup k PC a také přístup k internetu	4
Banka uživatele	Snížení skupiny obyvatel pouze na klienty konkrétní banky, přes kterou transakce probíhá	1
Čas transakce	Můžeme určit, kdy se uživatel pokouší provést platbu	2, 3, 4
Cena transakce	Jestliže budeme znát cenu transakce, dá se přemýšlet o koupěschopnosti uživatele	1, 3
Typ objednávaného zboží	Pokud známe typ objednávaného zboží, můžeme dále omezit skupinu zákazníků daného obchodu.	1, 3
Místo transakce	V případě, že dochází k použití karty v obchodě, či restauraci jsme schopni určit konkrétní město	3
Provider uživatele	Pokud zjistíme poskytovatele internetu, mohli bychom teoreticky určit například místo odkud jsou transakce prováděny	2, 4

Příklad: Představme si člověka, který si kupuje přes internet pravidelně místenku v autobuse. Na základě informací, které je útočník z této transakce schopen vypozorovat, může s velkou pravděpodobností určit následující:

1. Jde o občana České republiky, čili snížíme okruh možných lidí na necelých 10 miliónů.
2. Jde o osobu, která umí pracovat s počítačem a má přístup k internetu.
3. Banku, které je uživatel klientem.
4. Město, ze kterého osoba odjíždí a cílové město, například Brno - Praha, takže skupina obyvatel se nám dále snižuje na přibližně 1,6 milionu obyvatel.
5. Informaci o době odjezdu dejme tomu v pátek odpoledne, takže půjde pravděpodobně o člověka, který dojíždí do školy, či do zaměstnání.
6. Cenu jízdenky. Díky této informaci můžeme například vyloučit zjistit, že jde o studenta, pokud uplatňuje studentskou slevu. Tím se nám zúží okruh osob na studenty,

kteří pravděpodobně bydlí v Praze a studují v Brně, čili nají buď koleje nebo jsou ubytovaní na privátě.

7. Společnost, se kterou zákazník cestuje a způsob, jakým cestuje.

Díky tomu, že známe jméno společnosti, způsob jakým zákazník cestuje, víme kdy, odkud a kam jede se nám skupina obyvatel omezí na 46 lidí cestujících v určitý den, hodinu a v konkrétním autobuse, z kterých je dejme tomu 15 studentů a do Prahy jich z pojede řekněme deset. Z těchto deseti lidí také rozhodně nebudou všichni klienti konkrétní banky.

Takže jsme ze zdánlivě zbytečných informací dokázali zúžit okruh lidí na velmi malou skupinu.

- **Elektronické bankovnictví**

Typ informace	**Zúžení okruhu relevantních uživatelů**	**Získání informace (obr. 4.2)**
Provedení transakce	Pokud chce uživatel provádět operace pomocí internetového bankovnictví musí mít přístup k PC společně i přístupem k internetu	1, 2
Banka uživatele	Snížení skupiny obyvatel pouze na klienty konkrétní banky, přes kterou transakce probíhá	1
Rychlost přenosu	Podle rychlosti přenášených dat určí útočník teoretickou rychlost připojení k internetu	2
Čas transakce	Můžeme určit, kdy se uživatel pokouší provést platbu	2
Četnost přístupů	Tato informace nám může říct, kdy se obvykle uživatel spojuje se svojí bankou	1, 2
Způsob komunikace	Podle toho, jak jsme odchytili data můžeme určit, zda se jedná o komunikaci pomocí kabelů nebo zda jde o komunikaci pomocí GPRS.	2
Provider uživatele	Pokud zjistíme poskytovatele internetového připojení, mohli bychom teoreticky určit například místo odkud jsou transakce prováděny	1, 2

Příklad: Jako typický příklad můžeme zvolit osobu, která z domácího počítače přistupuje ke svému účtu a provádí nepravidelně platby a sleduje zůstatek na účtu.

Útočník může s velkou pravděpodobností určit následující:

1. Jde o občana České republiky, čímž snížíme okruh lidí na přibližně 10 miliónů občanů.
2. Jde o osobu, která má přístup k počítači a internetu.
3. Na základě rychlosti odesílaných a přijímaných dat určíme jaký typ připojení zákazník může přibližně používat, dejme tomu, že v našem případě nepůjde o zákazníka s vytáčeným připojením.
4. Banku, které je uživatel klientem, takže snížíme počet lidí dejme tomu na 707 tisíc (ČSOB).
5. Providera, pomocí kterého se uživatel připojuje k bankovnímu systému, čímž se omezí okruh obyvatel pouze na zákazníky konkrétního poskytovatele (pomocí adresy IP).

Operace v bankovním sektoru jsou pravděpodobně nejcitlivější a na jejich bezpečnost je kladen největší důraz. Díky tomu jsou také tyto transakce nejlépe chráněné proti případným útočníkům, kteří nemají na velkou vzdálenost šanci vysledovat konkrétního uživatele. Maximálně lze omezit skupinu uživatelů na kenkrétní obec popřípadě sídliště.

- **Mobilní telefonování**

Typ informace	**Zúžení okruhu relevantních uživatelů**	**Získání informace (obr. 4.3)**
Stát	Pokud probíhá komunikace na našem území (popřípadě do zahraničí), můžeme říct že jde o osobu pohybující se na území české republiky	1, 3
Mobilní telefon	Vzhledem k faktu, že jde o mobilní telefonování, pak bude uživatel patrně vlastníkem mobilního telefonu	1, 3
Typ operátora	Na základě jednoho z operátorů snížíme počet lidí pouze na jeho zákazníky	2
Četnost hovorů	Informace, která by mohla sloužit například k odhadu povolání uživatele (podnikatel, student)	1, 3
Čas uskutečnění hovoru	Může nám zúžit skupinu lidí například na ty co jsou vzhůru v noci	1, 2, 3
Místo volání	Zjistíme, zdali se volající osoba pohybuje na území ČR, popřípadě přes který vysílač (v které oblasti) probíhá hovor	1, 3

Příklad: Jako příklad můžeme vybrat podnikatele, který ze svého mobilního telefonu komunikuje se zaměstnanci i se zákazníky.

Útočník může určit následující informace:

1. Opět je pravděpodobné, že jde o občana České republiky.
2. Jde o osobu, vlastnící mobilní telefon. Mobilní telefon již v dnešní době vlastní podstatná část obyvatel, takže pravděpodobnost určení konkrétní osoby se nám zvýší jen málo.
3. Uživatel používá jednoho ze tří u nás registrovaných mobilních operátorů (EuroTel, T-Mobile, Vodafone), takže se okruh obyvatel zužuje na zákazníka konkrétního operátora.
4. Na základě četnosti hovorů můžeme určit jakou může mít teoreticky uživatel profesi. Pokud volá velmi často je pravděpodobné, že půjde o podnikatele, či osobu osobu obchodně činnou.
5. Bude-li útočník znát čas, kdy se uskutečňují hovory, může si udělat obrázek o aktivitě příslušného uživatele.
6. Při zjištění vysílače pomocí kterého komunikace probíhá je také možno určit, zda je osoba v pohybu (po republice) nebo se vyskytuje na jednom místě.

Mobilní telefonování je z pohledu skrytých kanálů také relativně bezpečný způsob komunikace. Útočník je schopný snížit skupinu obyvatel na relativně velký okruh. Mobilní telefon je však zařízení s velkou elektromagnetickou aktivitou a proto by zde připadaly v úvahy spíše metody zabývající se elektromagnetickým vyzařováním.

- **Vybírání elektronické pošty**

Typ informace	**Zúžení okruhu relevantních uživatelů**	**Získání informace (obr. 4.4)**
Doména	Na základě domény prvního řádu můžeme odhadnout příslušnost uživatele ke konkrétnímu státu.	1
Provedení transakce	Pokud chce uživatel provádět operace pomocí internetového bankovnictví musí mít přístup k PC společně i přístupem k internetu	2
Server	Omezení uživatelů pouze na ty, kteří mají účet na konkrétním serveru	1
Rychlost přenosu	Podle rychlosti přenášených dat je možné zjistit teoretickou rychlost připojení k internetu	2
Čas transakce	Na základě přihlášení do systému se dá určit, kdy uživatel navštěvuje svoji schránku	2
Četnost přístupů	Tato informace nám může říct, kdy většinou se uživatel spojuje s poštovním serverem	2
Provider uživatele	Pokud zjistíme poskytovatele internetového připojení, mohli bychom teoreticky určit například místo odkud jsou transakce prováděny	1
Chybové reporty	Na základě chybový zpráv je teoreticky útočník schopen rozluštit samotný obsah zašifrovaných zpráv. Což může vést nejen na odhalení identity uživatele, ale také na zneužití dešifrovaných zpráv.	1

Příklad: Jedním z možných příkladů uživatele elektronické pošty je například dálkově studující člověk na ČVUT Fakulta elektrotechnická, komunikující se svojí fakultou mimo jiné také prostřednictvím elektronických zpráv.

Útočník může určit následující informace:

1. Podle domény prvního řádu můžeme určit příslušnost ke konkrétnímu státu.
2. Jde o osobu, která má přístup k počítači a také k internetu.
3. Na základě serveru, se kterým probíhá komunikace zjistíme, s jakou institucí příslušný uživatel komunikuje. V našem případě jde o vysokou školu ČVUT Fakulta elektrotechnická. Tím jsme snížili okruh všech uživatelů pouze na studenty této fakulty.

4. Podle četnosti přístupů můžeme zjistit, jak často a kdy se daný student přihlašuje ke svému účtu, což může sloužit jako vodítko o jaký typ studenta jde.
5. Pokud budeme znát providera, pomocí kterého se uživatel připojuje k serveru, omezíme okruh obyvatel pouze na zákazníky konkrétního poskytovatele.
6. Pomocí chybových reportů je útočník schopen rozluštit samotné znění přenášených zpráv. Tyto informace mohou vest až k odhalení konkrétní identity studenta. Navíc jsou útočníkovi zcela k dispozici veškeré informace obsažené ve zprávách.

Vybírání elektronické pošty se jeví jako nejnebezpečnější varianta komunikace (ze čtyř, které jsem zkoumal). O bezpečnostní rizika se v tomto případě pravděpodobně nejedná, ale vliv na soukromí uživatelů zde určitě není zanedbatelný. Proto je nutné si uvědomit, že schránka elektronické pošty není nedobytný trezor a komunikace pomocí zasílání elektronických zpráv není z nejnebezpečnějších.

Kapitola 5

Klasifikace kontextů v IT transakcích

Na základě předchozích rozborů v rámci jednotlivých transakcí se nyní pokusíme o vytvoření obecné klasifikace různých kontextů a míru, s jakou je možné zúžit okruh uživatelů při použití dané informace útočníkem. Do přehledu jsou zařazeny i informace, získané pomocí elektromagnetické, tepelné a akustické emitace. Také je brána v potaz metoda měření spotřebovaného napětí a proudu. Ačkoliv nejsou tyto techniky použitelné na větší vzdálenosti (a tím pádem nejsou podstatné pro námi definovaného útočníka), znamenají rovněž potencionální ohrožení bezpečnosti informačních systémů a proto jsou do celkové klasifikace také zařazeny.

V tabulce vidíme jednotlivé druhy informací, které je možno v průběhu komunikace odposlechnout. Jsou přibližně seřazeny podle informační hodnoty od nejnižší, po nejvyšší.

Typ informace	**Vypovídací hodnota informace**
Typ transakce	Umožňuje určit o jaký typ transakce vůbec jde.
Čas provedení	Určení denní doby provádění transakcí (ráno, odpoledne, večer).
Četnost provádění	Jak často uživatelé provádějí konkrétní typ transakce.
Doba přenosu	Informace o tom, jak dlouho trvá komunikace mezi uživatelem a cílem.
Spotřeba času	Doba, po kterou procesor počítače vykonává požadovanou operaci.
Přenášená data	Informace o množství velikosti přenášených dat.
Rychlost přenosu	Udává, jak rychle je schopný uživatel komunikovat a jaké by tím pádem mohl používat připojení.
Typ OS	Informace o verzi operačního systému uživatele.
Typ prohlížeče	Informace o typu internetového prohlížeče.

Typ informace	Vypovídací hodnota informace
IP adresa	Informace o konkrétní IP adrese uživatele.
Typ komunikace	můžeme zjistit, jakým způsobem příslušná komunikace probíhá (pomocí kabelů, vzduchem).
Komunikační port	cesty přes které komunikace probíhá.
Jazyk komunikace	pomocí informace, v jakém jazyce komunikace probíhá můžeme určit příslušnost uživatele ke konkrétnímu státu nebo nérodnosti.
Cílová organizace	pokud známe cílovou organizaci, se kterou uživatel navázal komunikaci, můžeme množinu možných lidí omezit pouze na její uživatele, zákazníky, atd.
Poloha příjemce	místo které je voláno uživatelem při požadavku na provedení transakce.
Poloha odesílatele	místo, ze kterého uživatel komunikuje při průběhu transakce, můžeme omezit uživatele například na konkrétní město, sídliště, atd.
Poskytovatel komunikace	tato informace vypovídá o poskytovateli většinou internetového připojení, jako prostředek prostředek pro komunikaci s jednotlivými institucemi.
Cena transakce	pokud je cílem transakce převod finančních prostředků, je to pro útočníka zajímavá informace pro zjištění finanční situace uživatele.
Typ zboží	informace o typu nakupovaného zboží umožňuje další profilování zákazníků podle toho, co nakupují.
Věk uživatele	informace o věkové skupině (student, produktivní věk, důchodce).
Pohlaví uživatele	informace o tom, zda jde o muže, či ženu.
Vzdělání uživatele	informace o typu vzdělání uživatele na základě titulu.
Jméno uživatele	jde již o velice konkrétní údaj, značně omezující množinu potenciálních jednotlivců.
Adresa uživatele	velice konkrétní údaj, díky kterému se skupina možných lidí sníží v nejlepším případě na několik desítek rodin.
Rodné číslo	údaj prakticky jednoznačně identifikující konkrétní osobu.

Typ informace	Vypovídací hodnota informace
Chybové reporty	zprávy, které mohou vést až na úplné rozluštění zašifrovaných dat.
Elektromagnetické vyzařování [1]	Záření, které je vysíláno zařízením a může být na krátké vzdálenosti měřeno.
Tepelné vyzařování [1]	Jde o podobný princip, jako u elektromagnetického vyzařování, ale na tepelné bázi.
Akustické vyzařování [1]	Měření zvukových emisí, vydávaných zařízením.
Spotřeba proudu a napětí [1]	Jde o diferenciální měření spotřeby proudu a napětí. Při provádění různých procesů může být spotřeba odlišná.

[1] Tyto informace mohou být zjištěny pouze na krátkou vzdálenost a proto úplně nezapadají do našeho modelu. Z hlediska analýzy skrytých kanálů by však neměly být opomenuty.

Kapitola 6

Závěr

V rámci tohoto projektu jsem se zabýval standardem (Common Criteria) pro hodnocení informačních systémů a vlivem skrytých kanálů na soukromí a bezpečnost uživatelů.

Zjistil jsem, že skryté kanály tvoří v dnešní době jednu z největších hrozeb moderní kryptoanalýzy, jelikož se útočník nemusí zabývat samotným prolomením příslušné šifrovací metody, ale zaměřuje se na způsob implementace algoritmů.

Problémem je v zásadě dvojí. První riziko tkví v ohrožení obecné bezpečnosti obyvatel, kdy by mohlo mít odhalení tajných informací katastrofální následky. Common Criteria však s těmito případy počítají. Proto systémy pracující s tajnými informacemi vyžadující nejvyšší míru soukromí a splňující příslušné požadavky hodnocení podle CC, jsou proti zneužití dat dobře chráněné. Analýza skrytých kanálů je v těchto případech nedílnou součástí návrhu a realizace systému.

Druhou skupinou (a v době kapitalismu neméně důležitou) jsou systémy, které sice neoperují s informacemi přímo ovlivňující bezpečí, ale jejichž neoprávněné užití by mohlo způsobit uživatelům nemalé škody. Tyto systémy jsou o to nebezpečnější, že v nich úloha skrytých kanálů velmi podceňována a tím pádem při jejich vývoji nedochází k systematické analýze, která by mohla tato rizika snížit.

V mém projektu jsem ze zaměřil právě na tu druhou skupinu, kde je riziko vzhledem k (ne)použitým ochranným prostředkům podstatně vyšší a fakt, že uživatel při jakékoliv běžné komunikaci nechtěně poskytuje svoje soukromé údaje cizím osobám je jistě nemilou zprávou pro většinu lidí. Za nejvíce typické transakce jsem zvolil vybírání elektronické pošty, elektronické bankovnictví, mobilní telefonování, platby platebními kartami. Na základě definování

Na základě vytvořené klasifikace je teoreticky možné vypozorovat, které typy útoků jsou pomocí skrytých kanálů proveditelné a kterým informačním cestám věnovat nejvyšší pozornost při návrhu informačního produktu. Klasifikace je seřazena tak, že se hodnota informace směrem dolů zvyšuje. To znamená, že čím později se informace v tabulce vyskytuje, tím větší pozornost by jí

měla být věnována při tvorbě systému a analýze z pohledu skrytých kanálů.

Jako možné pokračování mojí práce z pohledu semestrálního a diplomového projektu vidím například reálné sledování některých výše zmiňovaných komunikačních kanálů a na základě získaných informací vytvoření databáze dat a ověření si předpokladů v praxi.

Literatura

[1] Produced by Syntegra. Common criteria for information technology security evaluation. http://www.commoncriteriaportal.org/public/files/ccusersguide.pdf, October 1999. Users Guide.

[2] P. Gašparovič. Elektronická pošta v TCP/IP. http://www.linuxzone.cz, červenec 2005.

[3] Common Criteria group. Common criteria for information technology security evaluation. http://www.commoncriteriaportal.org/public/files/ccpart2v2.3.pdf, August 2005. Part 2: Security functional requirements.

[4] P. Hanáček and J. Staudek. *Bezpečnost informačních systémů*. Úřad pro státní informační systém, 2000. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií.

[5] V. Klíma and T. Rosa. Na kanálu se pracuje. In *Sborník konference OpenWeekend 2003*, pages 41–50, Katedra pocítacu FEL CVUT, Karlovo námestí 13, 121 35, Praha 2, únor 2003.

[6] V. Klíma and T. Rosa. Vybrané aspekty moderní kryptoanalýzy. http://www.stech.cz/articles.asp?ida=100&idk=149, březen 2003.

[7] J. Kulveit. Kdopak to píše. http://www.krypta.cz/articles.php?ID=244, únor 2003.

[8] NBÚ. Informace o hodnocení bezpečnosti informačních technologií. http://www.nbu.cz, 2003.

[9] T. Rosa. Kryptoanalýza s využitím postranních kanálů. http://www.decros.cz/bezpecnost, 2001.

[10] M. Smeets and M. Koot. Covert channels. [research report], University of Amsterdam, February 2006.