VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

DEPARTMENT OF TELECOMMUNICATIONS

ZABEZPEČENÍ ULOŽENÝCH DAT NA PEVNÉM DISKU POČÍTAČE

SECURITY OF DATA STORED ON THE HARD DISK

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

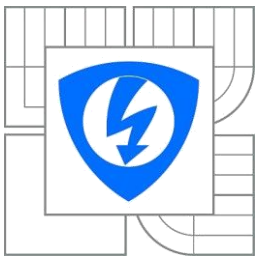
AUTOR PRÁCE — MARKÉTA POLÁŠKOVÁ

AUTHOR

VEDOUCÍ PRÁCE — Ing. ZDENĚK MARTINÁSEK, Ph.D.

SUPERVISOR

BRNO 2014



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Ústav telekomunikací

Bakalářská práce

bakalářský studijní obor
Teleinformatika

Studentka: Markéta Polášková ***ID:*** 146085
Ročník: 3 ***Akademický rok:*** 2013/2014

NÁZEV TÉMATU:

Zabezpečení uložených dat na pevném disku počítače

POKYNY PRO VYPRACOVÁNÍ:

V rámci bakalářské práce prostudujte základy kryptologie a zaměřte se na zabezpečení uložených dat na pevném disku počítače. Vytvořte přehledný rozbor současného stavu problematiky a dnes používaných metod. Seznamte se s útoky postranními kanály a to zejména s časovou a proudovou analýzou postranním kanálem. Prostudujte zařízení ICZ Protect Boot (http://www.protectboot.cz/cs/) a vyzkoušejte jeho funkčnost. Teoreticky vypracujte možné hrozby a rizika použití tohoto zařízení. V praktické části semestrálního projektu vyzkoušejte odolnost zařízení na časovou a proudovou analýzu (ověření implementovaného algoritmu ověření hesla) a vytvořte rozhraní mezi počítačem a zařízením umožňující snímání odebíraného proudu (deska plošných spojů). Z naměřených proudových průběhů určete závislost na vkládaném hesle a šifrovacím klíči. Výsledky přehledně zpracujte.

DOPORUČENÁ LITERATURA:

[1] Mangard, S.; Oswald, E.; Popp, T.: Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security). Secaucus, NJ, USA:Springer-Verlag New York, Inc., 2007, ISBN 0387308571.
[2] Dhem, J.-F.; Koeune, F.; Leroux, P.-A.;: A Practical Implementation of the Timing Attack. 1998
[3] Kocher, P. C.; Jaffe, J.; Jun, B.: Differential Power Analysis. In CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference onAdvances in Cryptology, London, UK: Springer-Verlag, 1999, ISBN 3-540-66347-9, s. 388–397.

Termín zadání: 10.2.2014 ***Termín odevzdání:*** 4.6.2014

Vedoucí práce: Ing. Zdeněk Martinásek, Ph.D.
Konzultanti bakalářské práce:

doc. Ing. Jiří Mišurec, CSc.
Předseda oborové rady

UPOZORNĚNÍ:

Autor bakalářské práce nesmí při vytváření bakalářské práce porušit autorská práva třetích osob, zejména nesmí zasahovat nedovoleným způsobem do cizích autorských práv osobnostních a musí si být plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č.40/2009 Sb.

Abstrakt

Tato práce se věnuje zabezpečení uložených dat na pevném disku počítače a to pomocí šifrování. První část práce vysvětluje základními pojmy kryptografie a popisuje zmínky o ní v historií. V dalších kapitolách se tato práce věnuje postranním kanálům a popisu útoků na tyto kanály. Jakými způsoby má útočník možnost získat informace z kryptografického modulu. Dále jsou popsány typy šifrování, jejich použití v dnešní době a jaké mají slabiny. Bakalářská práce pokračuje příklady jednotlivých šifrovacích programů.a zařízením ICZ Protect Boot. Poslední část této práce se zabývá testováním odolnosti zařízení ICZ Protect Boot. Testováním odolnost vůči proudové analýze pomocí postranního kanálu. Nakonec se bakalářská práce zabývá rozborem komunikace mezi počítačem a zařízením ICZ Protect Boot.

Klíčová slova

Kryptologie, kryptografie, kryptoanalýza, pevný disk, postranní kanály

Abstract

This work is dedicated to the security of data stored on the hard drive of your computer and using encryption. The first part explains the basic concepts of cryptography and describes her in history. In other chapters, this work is dedicated to a description of the side channels and attacks on these channels. How can the attacker obtain information from a cryptographic module. The following section describes the types of encryption they use nowadays and what are their weaknesses. Bachelor thesis continues with examples of individual encryption programs and device ICZ Protect Boot. The last part deals with resistance testing on equipment ICZ Protect Boot. Testing of resistance to flow analysis using a side channel. Finally, bachelor thesis deals with the analysis of communication between the computer and ICZ Protect Boot.

Key Words

Cryptology, cryptography, cryptanalysis, hard disk, side channels

POLÁŠKOVÁ, Markéta *Zabezpečení uložených dat na pevném disku počítače*: bakalářská práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2014. 29 s. Vedoucí práce byl Ing. ZDENĚK MARTINÁSEK, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Zabezpečení uložených dat na pevném disku počítače“ jsem vypracoval(-a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil(-a) autorská práva třetích osob, zejména jsem nezasáhl(-a) nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom(-a) následku porušení ustanovení § 11 a následujících autorského zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonu (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno . . . .

podpis autora

PODĚKOVÁNÍ

Ráda bych poděkovala Ing. Zdeňku Martináskovi, Ph.D., vedoucímu mé bakalářské práce, za jeho čas, trpělivost se mnou a rady při tvorbě této práce. Také bych ráda poděkovala zejména přátelům a rodině za podporu.

Brno . . . .

podpis autora

OBSAH

SEZNAM OBRÁZKŮ

ÚVOD

Před více jak 10 lety málokdo věděl, jakým způsobem obejít heslo do systému Windows. Od té doby se svět změnil a útočníci mají k dispozici dokonalejší prostředky na prolomení i zdánlivě bezpečné formy zabezpečení

Většina uživatelů si myslí, že není potřeba zabezpečit svůj počítač. Buď si nejsou vědomi nebezpečí, nebo jsou přesvědčeni, že právě jim žádný útok na důležitá data nehrozí. Data, ať už se jedná o dokumenty, fotky nebo videa z dovolené, je nutné chránit. V počítači hlavně mohou být i důvěrné soubory s hesly např. do školy a do práce. Ty by mohl útočník získat a pomocí nich se dostat do systému vašeho zaměstnavatele a způsobit škodu v tomto systému. Aby se dalo takovým škodám předejít, je třeba svůj počítač a data obsažené v něm chránit.

Existuje mnoho způsobu ochrany dat. Jedním z těchto způsobů je zálohování dat. V tomto případě se jedná o ochranu proti poškození dat. Další možností je šifrování citlivých dat na počítačích, které sdílí více uživatelů. Šifrování dat představuj převod dat do nečitelné podoby a po zadání hesla pak opětovný převod do původního stavu. Možností, jak šifrovat data v počítači a na externím disku je několik. Některé možnosti jsou přímo součástí operačního systému. Další možností jsou šifrovací programy, které umožňují šifrování dat. Existují také zařízení, které chrání počítač šifrováním dat, např. zařízení ICZ Protect Boot. Toto zařízení využívá vlastností softwaru TrueCrypt.

Tato práce se zabývá problematikou zabezpečení dat na pevném disku.V první části práce se nachází vysvětlení základních pojmů v kryptologii a vědám obsaženým v ní, kryptografii a kryptoanalýze. Další části jsou zaměřeny na druhy šifrování, šifrovací programy a zařízení ICZ Protect Boot. Poslední část, praktická, se zabývá testováním odolnosti tohoto zařízení na útok pomocí postranních kanálů.

1 KRYPTOLOGIE

Kryptologie je věda zabývající šifrováním zpráv, citlivých dat a jejich zabezpečením vůči útočníkovi. Obsahuje dvě důležité části. Jednou z nich je kryptografie, věda zajišťující bezpečnost informačních systémů. Druhá část je kryptoanalýza, což je opakem kryptografie a jejím úkolem je překonávat kryptografické zabezpečení.

Pro lepší pochopení je třeba definovat určité pojmy. Prvním z těchto pojmů je autentičnost. Autentičnost neboli pravost, hodnověrnost znamená, že je jasné s jakým partnerem je vedena komunikace, jeho identita. Dalším pojmem je integrita. V kryptografii znamená integrita platnost dat. Porušení integrity může být náhodnou změnou nebo záměrnou. Náhodná změna je chyba při přenosu dat nebo poškozením pevného disku. Za záměrnou změnu je zodpovědný útočník, např. pokud útočník změní číslo účtu v transakci. Posledním z těchto pojmů je bezpečnost. Bezpečností by se dal označit stav, při kterém ztráty dat (aktiv) nepřekračují stanovenou míru.

1.1 Historie kryptologie

Pro začátek menší náhled do historie kryptologie. Ačkoli se to nezdá, tak kryptologie má v celku dlouhou historii. Pro představu je vhodné uvést pár nejdůležitějších mezníků v kryptologii:

- 500 let př.n.l. - Hebrejské národy: jednoduchá substituční šifra (ATBASH).
- 400 let př.n.l. - Řecko: jednoduché transpoziční šifry a steganografie.
- 50 let př.n.l. - Řím: Caesarova šifra.
- 4. století - šifrování mezi 64 uměními v Kámasútře.
- 10. století - Arabové: základy kryptoanalýzy včetně frekvenční analýzy.
- 13. a 14. století - Evropa: používá se substituční šifra, případně lehké nástavby.
- 15. a 16. století - první návrhy šifrování podle hesla.
- 16. století - Evropa: kryptologie hraje důležitou roli v politice.
- 1586 - Anglie: poprava skotské královny na základě rozluštění šifry.
- 1843 - USA: E. A. Poe píše o šifrách a zveřejní šifrovací výzvy.
- 1861 - Prusko: metoda pro řešení polyalfabetické šifry (Kasiski).
- 1885 - USA: Bealův poklad, jednalo se o skříňku obsahující 3 stránky zašifrovaného textu o pokladu.

- 19. století - rozvoj telegrafu, rozvoj kryptografie pro komerční účely, polní šifry (Playfair), první mechanické přístroje pro šifrování.
- světová válka - důležitá role ve válce i v politice (Zimmermannův telegram), použití komplikovanějších šifer na klasických principech.
- 1926 - Německo: armáda začíná používat šifrovací přístroj Enigma, viz Obr. 1.
- světová válka - klíčová role kryptologie ve válce, použití mechanických šifrovacích strojů.
- 1949 - publikovány práce C. Shannona o teorii informace.
- 50. léta 20. století - rozvoj počítačů, první využití počítačů pro šifrování/luštění.
- 1967 - USA: kniha D. Khana „The Codebreakers".
- 1973 - Anglie: objeven princip šifrování s veřejným klíčem, kvůli utajení však nebyl zveřejněn.
- 1976 - USA: publikován článek „New Direction in Cryptography", začátek rozvoje akademické kryptologie.
- 1978 - USA: zveřejněno RSA (Rivest, Shamir, Adleman), algoritmus realizující kryptografii s veřejným klíčem.
- 1991 - USA: zveřejněno PGP (Pretty Good Privacy), implementace kryptografie s veřejným klíčem.
- 90. léta 20. století - rozvoj kvantové kryptografie [1].

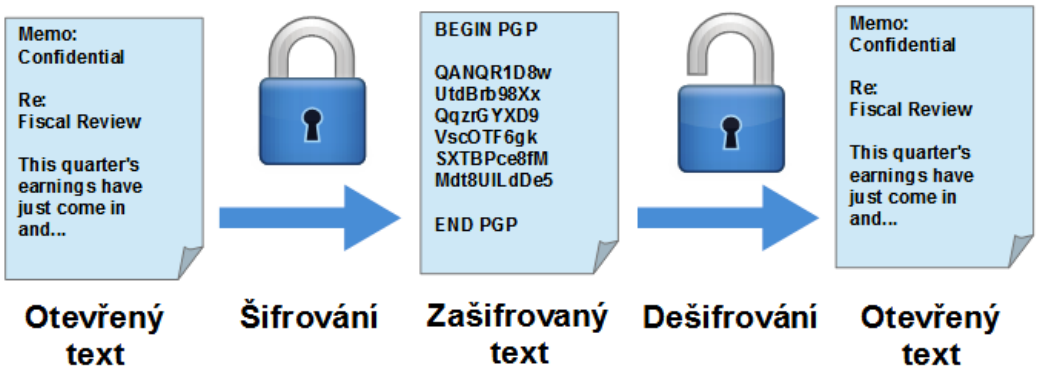
Obr. 1 Enigma - jedna z největších legend v historii kryptoanalýzy [6]

1.2 Kryptografie

Samostatné slovo kryptografie pochází z řečtiny, je složeno ze dvou slov. První slovo je „kryptós“, to znamená skrytý. Druhé slovo, z kterého se to skládá je „gráphein“, což znamená psát. Z toho vyplývá, že se jedná o šifrování. Tato věda se po staletí vyvíjela k větší složitosti spolu s lidskou civilizací a mnohokrát ovlivnila běh dějin. Jedná se teď zejména o utajení strategických vojenských informací, prozrazení politických intrik, příprav atentátů a jiných podobných situací, kdy bylo důležité danou informaci bezpečně přenést. Pro shrnutí může být řečeno, že kryptografie je věda, která se zabývá konstrukcí kryptografických zabezpečení. Šifrování probíhá pomocí šifry, kryptografického algoritmu, ten převádí čitelnou zprávu do šifrované podoby, nečitelného textu. Na rozšifrování textu je třeba mít klíč, tajnou informaci, bez které nelze šifrovaný text přečíst. Na obrázku Obr. 2 je zobrazen proces šifrování.

Na základě vlastností závislosti šifrovacího klíče na dešifrovacím se kryptografické systémy dělí do dvou základních tříd:

- Symetrické kryptografické systémy
- Asymetrické kryptografické systémy [3]

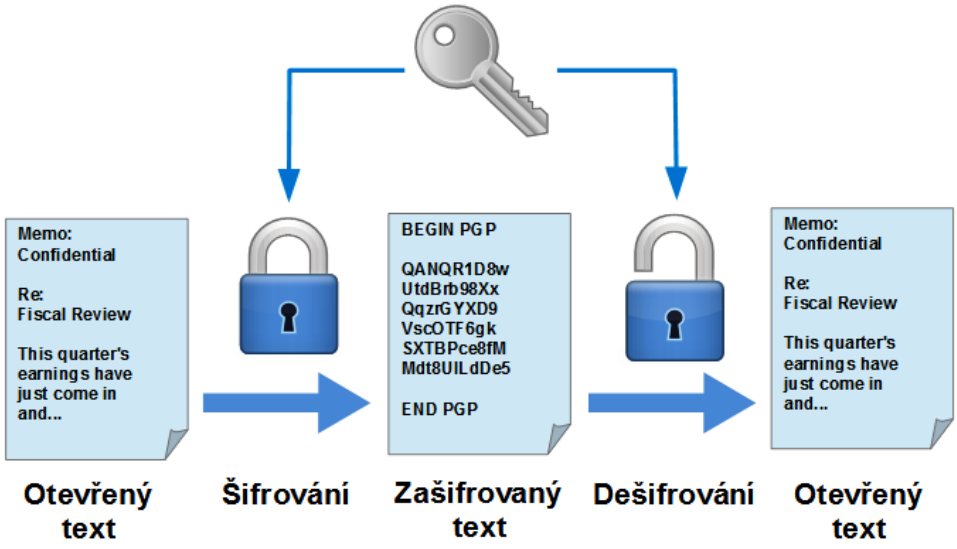


Obr. 2 Proces šifrování

1.2.1 Symetrický kryptografický systém

Jedná se o systém s tajným klíčem, kdy komunikující strany musí držet šifrovací a dešifrovací klíč v tajnosti. Důvod tohoto utajení je jednoduchý, dešifrovací klíč je buď stejný jako šifrovací nebo je z šifrovacího klíče relativně snadno odvoditelný.

Systémy s tajným klíčem jsou velmi rychlé, jsou schopné zašifrovat velký objem dat a slouží k důvěrnosti a autentičnosti zpráv. Velkým problémem u těchto systémů je však bezpečná distribuce klíčů k odesílateli a příjemci. Tento systém má tedy nejlepší využití na zašifrování disku nebo konkrétního souboru [3]. Na obrázku Obr. 3 je blokové schéma symetrického šifrování.



Obr. 3 Symetrické šifrování

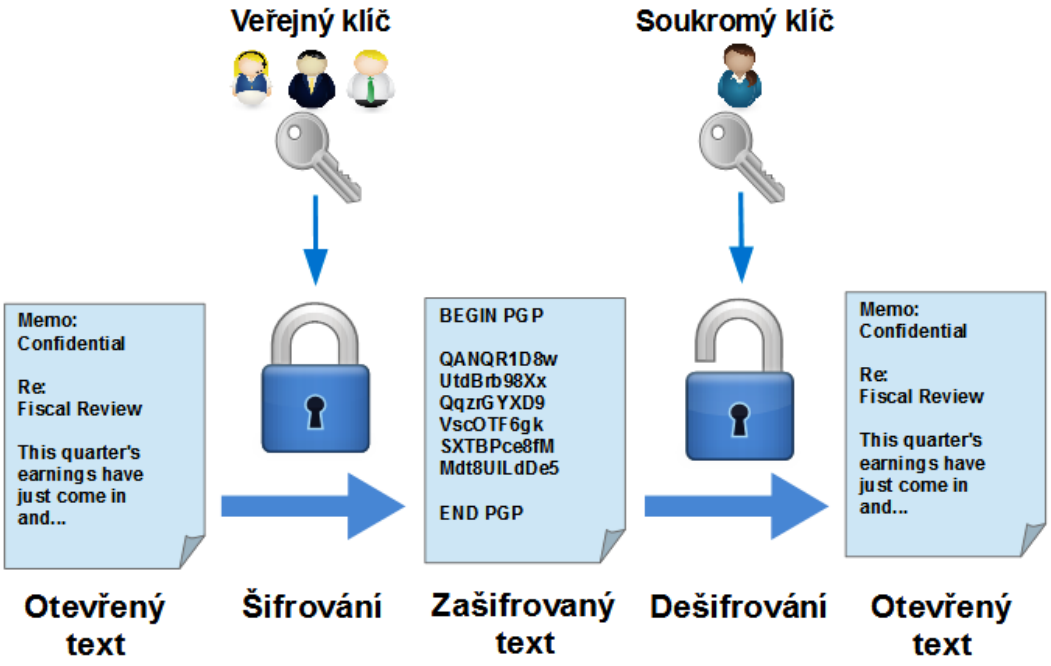
Symetrické kryptografické systémy můžeme dále dělit na:

- proudové šifry - jsou rychlejší než blokové šifry, příkladem této šifry je např. šifrovací algoritmus RC4.
- blokové šifry - oproti proudovým šifrám jsou bezpečnější, příkladem této šifry je AES [3].

1.2.2 Asymetrický kryptografický systém

Oproti symetrickému systému má asymetrický systém klíče dva. U tohoto systému platí, že oba klíče jsou různé, není je možné od sebe odvodit, jeden klíč je soukromý a druhý veřejně známý. Tento systém může zajišťovat důvěrnost a integritu, pokud je šifrovací klíč tajný a dešifrovací klíč veřejný. Z toho vyplývá, že zprávu může zašifrovat pouze majitel soukromého klíče a dešifrovat ji může veřejným klíčem kdokoli. Dále pak může díky veřejnému šifrovacímu klíči a tajnému dešifrovacímu zajistit autentičnost, to ve zkratce znamená, že zprávu může zašifrovat kdokoli, ale

dešifruje ji pouze majitel tajného klíče. Nejznámějším algoritmem v oblasti asymetrických šifer je algoritmus RSA (iniciály autorů Rivest, Shamir, Adleman).[3] Obrázek Obr. 4 zobrazuje blokové schéma asymetrického kryptografického systému.



Obr. 4 Šifrování veřejným klíčem

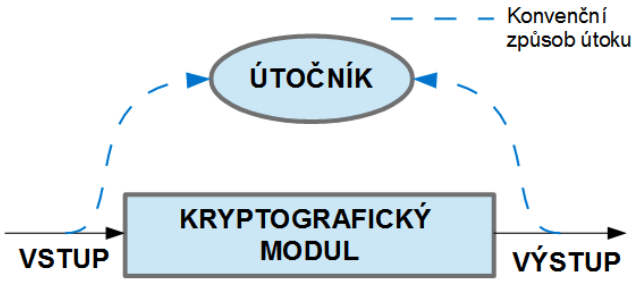
2 KRYPTOANALÝZA

Slovo kryptoanalýza je řeckého původu stejně jako jeho opak kryptografie, skládá se ze dvou slov. Prvním slovem je „kryptós“, to znamená skrytý. Druhým slovem je „analýein“, jehož překlad znamená uvolnit. Kryptoanalýza je věda zabývající se metodami získávání obsahu šifrovaných informací bez znalosti tajného šifrovacího klíče. Dále jsou rozebrány druhy útoků na kryptografické zařízení.

2.1 Konvenční kryptoanalýza

K úvodu, kryptografický modul je realizován buď hardwarově nebo softwarově. Jedná se o zařízení obsahující kryptografické algoritmy sloužící k šifrování dat a dešifrování dat.

Konvenční kryptoanalýza využívá útoku na vstupní a výstupní komunikační kanál kryptografického modulu, kdy útočník na těchto kanálech zachytí zašifrovaná data a vstupní data. Z těchto dat se snaží matematickou analýzou získat hodnotu tajného klíče. Tento typ analýzy je v dnešní době neefektivní a časově náročný, jelikož většina dnes užívaných kryptografických algoritmů je prakticky neprolomitelná v případě, kdy má analytik k dispozici pouze šifrovaný text [4][5]. Schéma konvenční kryptoanalýzy je zobrazeno na obrázku Obr. 5.

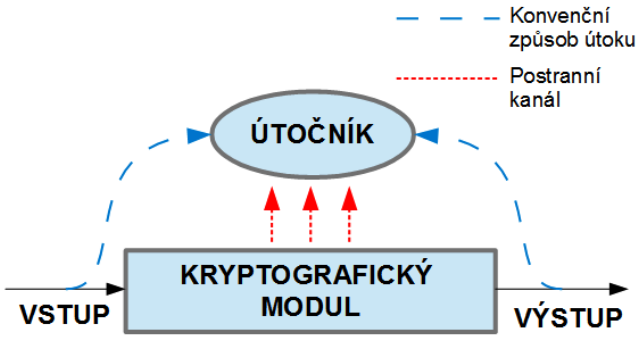


Obr. 5 Konvenční kryptoanalýza

2.2 Kryptoanalýza postranních kanálů

Kryptografický modul při své činnosti produkuje tepelné a jiné záření, spotřebovává výkon ze zdroje atd. Tyto jevy mohou být provázány s průběhem operací uvnitř kryptografického modulu. Takto dochází k nežádoucímu vynesení informací mimo modul, komunikaci s okolím. Vznikají postranní kanály.

Útok postranním kanálem je veden na chyby v implementaci šifrovacího algoritmu. Citlivé informace jsou získávány ze zdánlivě bezvýznamných odezev systému, jako jsou chybová hlášení, doby trvání výpočtů, proudové nebo napěťové poměry v systému, elektromagnetické vyzařování a případně i další odezvy, které mohou být i uměle vyvolané [4]. Na obrázku Obr. 6 je vidět kryptoanalýza využívající postranních kanálů.



Obr. 6 Kryptoanalýza zahrnující využití postranních kanálů

Postranní kanály nám úplně mění celkový pohled na bezpečnost systému. Již nestačí zvolit kvalitní šifru, ale je nutné věnovat pozornost i její implementaci. V současné době není téměř žádná možnost obrany proti kryptoanalýze postranním kanálem.[4]

Přehled známých typů postranních kanálů:

- výkonový (proudový),
- elektromagnetický,
- časový,
- chybový,
- optický,
- akustický,
- kleptografický [4].

Každý z těchto postranních kanálů má přesnou definici způsobu, jakým dochází k nežádoucí výměně citlivých informací kryptografického modulu s jeho okolím. Následně je v rámci útoku nutné získané informace zpracovat a vyhodnotit.

V kryptografii se tento proces souhrnně nazývá analýzou kanálu. Existují dva základní druhy analýz:

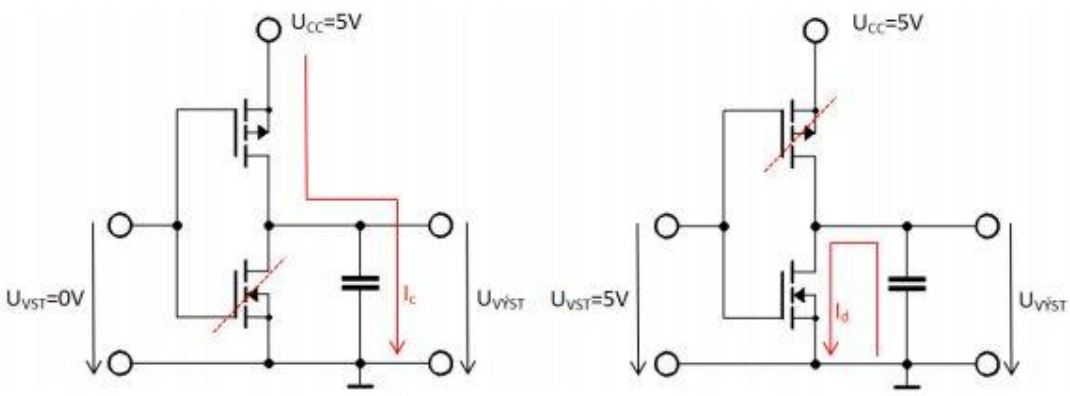
- jednoduchá analýza (Simple Analysis) - představuje základní způsob zpracování výsledků. Informace získané z postranního kanálu jsou útočníkem pozorovány a vyhodnoceny.
- diferenční analýza (Differential Analysis) - je komplikovanější, protože vyžaduje použití matematického aparátu. Umožňuje však nalézt citlivé informace i z postranních kanálů, kde jejich přítomnost není zřejmá. Další výhodou je možnost automatizace procesu, to může výrazně snížit čas nutný k analýze informace získané pomocí postranního kanálu [4] [5].

2.2.1 Výkonový (proudový) postranní kanál

Jedná se o druh postranního kanálu, u kterého se sleduje spotřeba proudu kryptografického modulu, na který je v tu chvíli prováděný útok [4].

Princip funkce výkonového (proudového) postranního kanálu

Většina dnes používaných integrovaných obvodů je založena na využití tranzistorových součástek technologie CMOS. Elementárním stavebním prvkem obvodů typu CMOS je invertor, jehož vnitřní zapojení se skládá ze dvou tranzistorů typu MOS-FET. Tyto tranzistory jsou zapojené jako spínače řízené napětím, viz Obr.7 [4].



Obr. 7 Model invertoru logiky založené na CMOS [4]

Pokud je U_{VST} rovno napětí logické úrovně „0“, je horní tranzistor otevřen a dolní uzavřen. V momentě, kdy se na U_{VST} připojí napětí logické úrovně „1“, je dolní tranzistor otevřen a horní uzavřen. [4]

V případě obou stavů popsaných výše je proudová spotřeba nízká, avšak pro každý stav je různá. V obvodu při přechodu mezi těmito stavy nastává výkonová špička, kdy jsou na krátký okamžik otevřeny oba tranzistory současně, a napájení je zkratováno proti zemi. Tento jev se nazývá dynamickou spotřebou a při měření odebíraného proudu se projeví špičkami v průběhu proudu v závislosti na čase. Její velikost závisí na tom, kolik tranzistorů právě přepíná. Proudovou špičku lze změřit tak, že se do série s V_{DD} nebo V_{SS} zapojí rezistor, na kterém se následně změří úbytek napětí, který odpovídá okamžitému odběru proudu. Tranzistory odebírají malý proud i v klidovém stavu, který se pak mění teplo nebo záření. Dominantním zdrojem výkonových změn je nabíjení (I_C) a vybíjení (I_D) interní kapacitní zátěže, která je připojena na výstupy. Mezi zdroje výkonových změn patří:

- Tepelné vyzařování tranzistorů v klidovém stavu a proudový odběr pro stav logické „0“ a pro stav logické „1“. Elektrická energie se mění na teplo.
- Proudové špičky při přechodu mezi stavy logické „0“ a logické „1“.
- Změny proudu při vybíjení a nabíjení parazitní kapacitní zátěže připojené sběrnice při změnách pracovních stavů. [4]

Z toho plyne, že výkonová spotřeba elektronických obvodů přímo závisí na operacích, které v nich probíhají, tedy na množství překlápěných tranzistorů. Analýzou výkonové spotřeby lze tedy zjistit citlivé informace uvnitř kryptografického modulu. [4]

Jednoduchá výkonová analýza

Jednoduchá výkonová analýza SPA (Simple Power Analysis) je technika útoku výkonovým postranním kanálem založená na přímém pozorování průběhu výkonové spotřeby kryptografického modulu. Tato technika nevyužívá statistických metod nebo jiných matematických postupů.[5]

Útok jednoduchou výkonovou analýzou je vhodný proti kryptografickým protokolům, ve kterých je průběh prováděného programu silně závislý na zpracovávaných datech (obsahuje podmíněnou operaci závislou na datech). Provedení či neprovedení řady instrukcí vykonávaného programu je tak přímo závislé na zpracovávaných datech. Každá instrukce má charakteristický průběh výkonové spotřeby. Pozorováním výkonové spotřeby je určen sled provedených instrukcí

závislých na zpracovávaných datech. Typické příklady takovýchto algoritmů s popisem jejich problematických částí obsahuje následující text.

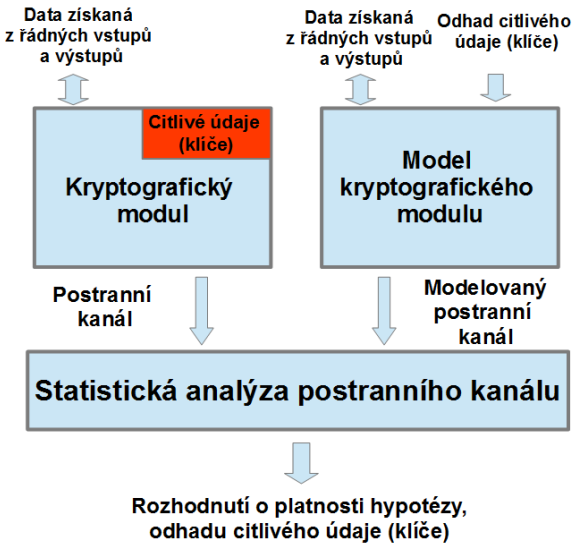
- Permutace - Šifrovací algoritmus DES, ale i řada jiných algoritmů, je založena na řadě permutací. Programový kód permutací přeložený do instrukčních sad cílových mikroprocesorů vnáší do průběhů výkonové spotřeby značné charakteristiky v závislosti na datech do permutací vstupujících.
- Porovnávání - Řada algoritmů obsahuje programový kód pro porovnávání řetězců nebo částí operační paměti. Tyto porovnání jsou opět založena na podmíněných větveních programu, která způsobují významné změny nejen ve výkonovém postranním kanálu, ale také v časovém a dalších kanálech.
- Násobení - Různé typy modulárního násobení jsou jedním z nejvýznamnějších zdrojů informací unikajících řadou postranních kanálů. Informace v kanálu jsou silně korelovány s hodnotami zpracovávaných dat a způsob úniku těchto dat je závislý na konkrétní realizaci procesu násobení.
- Umocňování - Principiálně jednoduché funkce modulárního umocňování jsou založeny na postupném procházení exponentu v iteračních krocích. V závislosti na hodnotě bitu exponentu příslušného dané iteraci jsou nebo nejsou provedeny požadované operace a následné násobení. Na základě hodnoty exponentu je tak program větven v každé iteraci do zcela jiné cesty, je zpracován jiný kód s charakteristickou dobou výpočtu a podpisem v průběhu výkonové spotřeby. Množství prosakující informace roste s počtem exponentů.[5]

Zvláštní případ jednoduché výkonové analýzy je založen na nalezení silné závislosti mezi průběhem výkonové spotřeby a Hammingovou váhou zpracovávaných dat (Hammingova váha reprezentuje počet nenulových bitů ve slově). Z informace o Hammingově váze pracovávaných dat, která uniká výkonovým postranním kanálem, je možné tato data rekonstruovat. Tento způsob jednoduché výkonové analýzy je efektivní proti systémům zpracovávajícím data v menších jednotkách, například bajtech.[4] [5]

Diferenční výkonová analýza

Útok za pomoci diferenční výkonové analýzy DPA (Differential Power Analysis) je jedním z nejnebezpečnějších druhů útoku výkonovým postranním kanálem. Tento typ analýzy je založen na sledování korelace mezi výkonovým průběhem a

programem zpracovávanými daty. Tato vazba je většinou slabá a je nutné použít statistických metod k jejímu nalezení. Základem je model reálného kryptografického modulu. Předpokladem jsou stejná data zpracovávaná jak na reálném modulu, tak na jeho modelu. Následně jsou analyzovány výstupy získané postranním kanálem jak reálného modulu, tak i hypotetického modelu. Pouze pro správný odhad citlivého údaje dochází ke korelaci mezi oběma postranními kanály. V případě, že jsou získána a analyzována data z jednorozměrného postranního kanálu (jeden typ kanálu, získána jedna hodnota pro každý časový okamžik), je diferenční analýza nazývána diferenční analýza prvního řádu. V případě vícerozměrného postranního kanálu (více typů postranních kanálů, je získána řada hodnot pro každý z časových okamžiků) se jedná o diferenční analýzu vyšších řádů.Na obrázku Obr. 8 je schéma modelu diferenční analýzy.



Obr. 8 Model diferenční analýzy

2.2.2 Elektromagnetický postranní kanál

Při analýze elektromagnetického postranního kanálu se využívá principu, kdy změny proudů v obvodech kryptografických modulů, při jejich činnosti, generují střídavé magnetické pole. V případě, že je generované magnetické pole dostatečně silné, může být detekováno. Útočník umístí do blízkosti zařízení cívku a naměřené elektromagnetické pole posléze analyzuje. Tato problematika bude v blízké budoucnosti velmi exponovanou oblastí.[4]

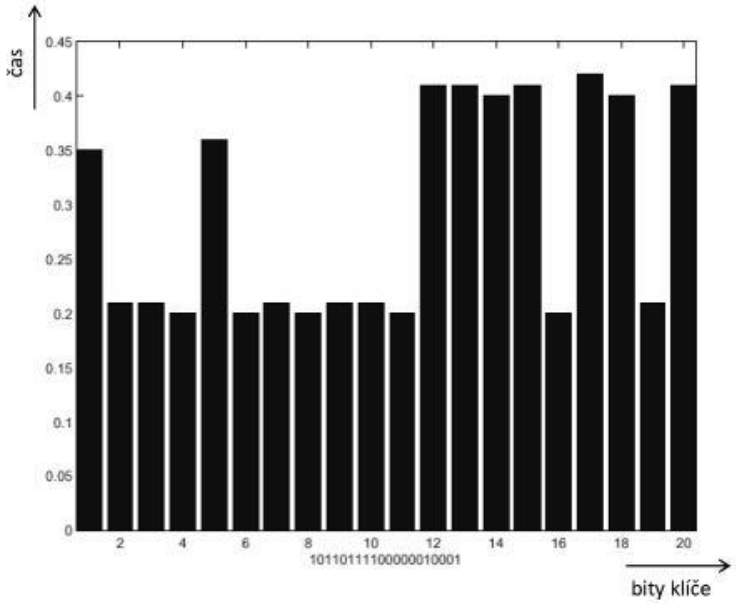
2.2.3 Časový postranní kanál

V případě analýzy časového postranního kanálu se využívá jednoduchý princip, kdy určité operace závislé na tajném klíči trvají různou dobu. Závisí to na konkrétních hodnotách jednotlivých bitů klíče. Na obrázcích Obr.9 a Obr.10 lze vidět příklad časového útoku na privátní klíč RSA v operaci odšifrování nebo podpisu $y = (m^d)\ mod\ n$. Na obrázku Obr. 8 je uveden zdrojový kód pro výpočet modulární mocniny pomocí známého algoritmu „square and multiply“, kdy se jednotlivé bity privátního klíče (exponentu *d*) postupně zpracovávají. Doby průchodu jednotlivých bitů klíče tímto algoritmem jsou tedy různé, jak je vidět na obrázku Obr.9.[4]

Výpočet $y = (m^d \bmod n)$ *square and multiply:*
$d = d_0 d_1 \ldots d_{b-1}$ *(nejvyšší bit* $d_0 = 1$*)*
$R = m$
for $i = 1$ *to* $b-1$
{
    $R = R^2 \bmod n$
    if$(d_i == 1)$ *then* $R = R * m \bmod n$ (*)
}
return R

pozn.: časová náročnost oprerace (*) vyzařuje informaci o bitu klíče d_i

Obr. 9 Algoritmus „square and multiply“[4]



Obr. 10 Čas průchodu algoritmem pro jednotlivé bity klíče d [4]

2.2.4 Chybový postranní kanál

Využití chybového postranního kanálu se ukázalo být velice efektivním způsobem útoku na kryptografické zařízení. Chybový postranní kanál je založený na chybových hlášeních a systémových selháních, kdy kryptografický modul musí komunikovat s okolím. V běžném provozu jsou tato hlášení nutná pro správnou funkci systému. V dalším případě může útočník tento stav vyvolat uměle, kdy postupným opakováním chybných požadavků dojde ke zjištění některých citlivých informací.[4]

2.2.5 Optický postranní kanál

Hlavní myšlenka analýzy optického postranního kanálu je velice jednoduchá. Vychází z faktu,že jednou z nejpoužívanějších součástí integrovaných obvodů jsou tranzistory, jejichž fyzické stavy jsou reprezentovány jedním ze dvou logických stavů „0“ nebo „1“. Kdykoliv tranzistor změní svůj stav, část energie využité tranzistorem se uvolní prostřednictvím fotonů, které tranzistor emituje do svého okolí. Avšak využití kryptoanalýzy postranního kanálu tohoto typu je velice finančně nákladné, časově náročné a rovněž také velice obtížně proveditelné. Zařízení umožňující tuto analýzu se nazývá PICA a nachází se v několika málo laboratořích na světě. [4]

2.2.6 Akustický postranní kanál

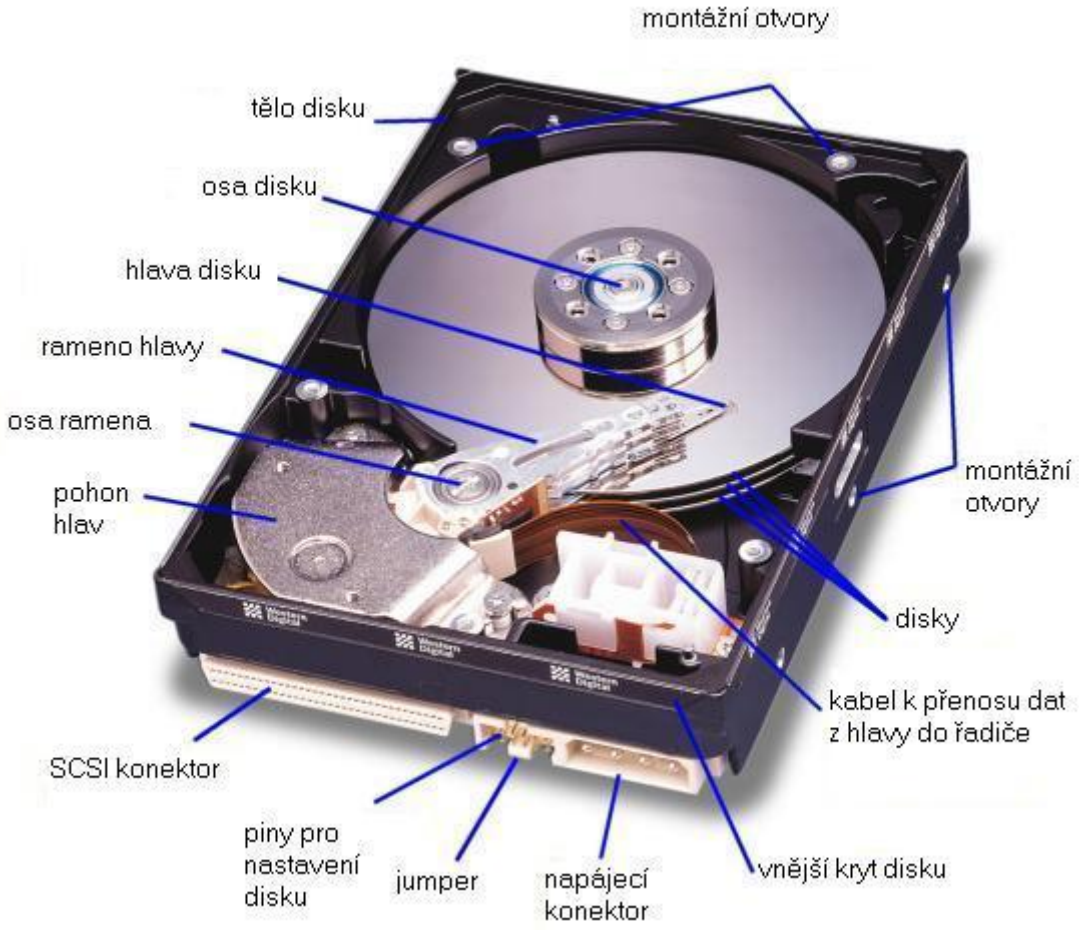
Vyskytuje se u většiny aplikací kryptografických systémů, kde se používá klávesnice pro zadání citlivých údajů (bankomaty, klávesnice PC, klávesnice mobilního telefonu). Dále lze také využít analýzu akustického postranního kanálu například u tiskáren (tiskárny PIN kódů a hesel).[4]

2.2.7 Kleptografický postranní kanál

V tomto případě se jedná o zvláštní příklad postranního kanálu. Může být zařazen mezi tzv. podprahové kanály. Podprahový kanál je kanál, který je v kryptografickém modulu záměrně vytvořen útočníkem bez vědomí uživatele za účelem vynášení citlivých informací. Jedná se o informace, které jsou pod úrovní rozlišovací schopnosti daného modulu, protokolu, typu spojení atp. Problematika těchto kanálů je zatím poměrně nová, která se do budoucnosti stane velice diskutovanou podobně jako oblast elektromagnetických postranních kanálů.[4]

3 PEVNÝ DISK

Je to zařízení, které se používá k dočasnému nebo trvalému uchování dat pomocí magnetické indukce. Data se ukládají na disk pomocí hlavy, zmagnetizováním míst na magneticky měkkém materiálu. Čtení probíhá také pomocí hlavy, která nad zmagnetizovanými místy indukuje elektrický proud. Data, která jsou na disk zaznamenána, jsou zachována v magnetické vrstvě i při odpojení disku od zdroje elektrického proudu. Pevný disk s popisem jednotlivých součástí je na obrázku Obr. 11.



Obr. 11 Části pevného disku[8]

Data na pevném disku můžeme zabezpečit několika způsoby, například hardwarovým šifrováním, softwarovým šifrováním, heslem pro přístup k pevnému disku, BIOS heslem a Windows heslem. V následující části jsou blíže rozebrané hardwarové a softwarové šifrování.

3.1 Hardwarové šifrování

Při hardwarovém šifrování využívají externí disky v dnešní době technologie 256-bitového hardwarového AES (Advanced Encryption Standard) šifrování. Tyto disky slouží pro bezpečný přenos a ukládání citlivých dat jakékoli povahy. Po úspěšné identifikaci se chovají jako běžné výměnné zařízení. Výhodou tohoto šifrování je vysoká rychlost šifrování dat, dále pak skutečnost, že šifrovací klíč neopouští zařízení, tzn. nemůže být získán ani zkopírován.[9]

Použití šifrovaných disků je velmi pohodlné a bezproblémové. Prvním důvodem proč tomu tak je, že na hostitelském počítači není nutné mít nainstalovaný žádný software ani speciální ovladače. Nezanechává žádnou stopu na zařízeních, kde bylo použito. [9]

U pevných disku v počítači, které obsahují hardwarové šifrování, jsou označovány zkratkou FDE (Full Disc Encryption), je třeba si pořídit i externí software. K šifrování na tomto disku sice dochází i bez něj, zajišťuje ho elektronika disku, ale funkce pro přístup k datům nejsou z výroby aktivovány.[10]

Šifrovaná zařízení mohou dále využívat i jiné způsoby ochrany dat, jako například:

- přístupové heslo ,
- biometrická autentizace (otisk prstu),
- nastavení platnosti hesla,
- možnost nastavit si pouze režim čtení dat [9].

3.2 Softwarové šifrování

Jedná se o šifrování pomocí programu, který generuje šifrovací klíč, pomocí kterého se data šifrují.Velkou výhodou tohoto šifrování je snadno dostupná podpora, cenová dostupnost, jeho velké rozšíření. Vývojem těchto programů se zabývá řada firem, nejznámější z nich jsou McAfee, PGP, Check Point a mnoho dalších.

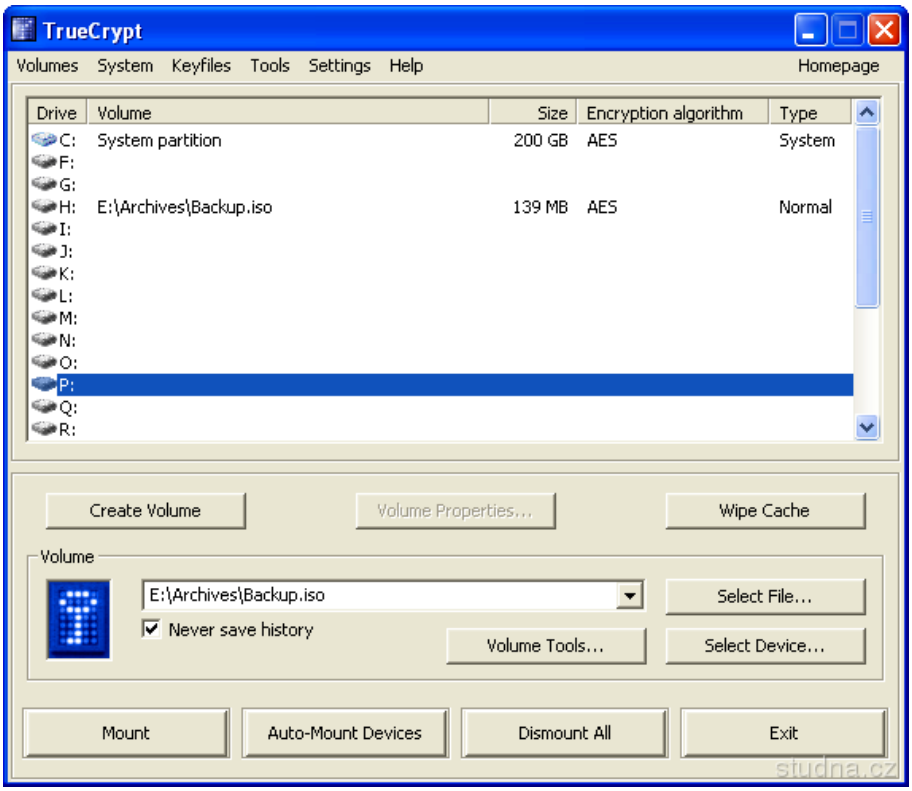
Vliv softwarového šifrování na výkon počítače se uvádí řádově okolo pěti až deseti procent výkonu, což u běžných uživatelů není překážkou, z pohledu omezení provozu. Nevýhodou softwarového šifrování je nutnost jeho otestovaní před nasazením. Důvodem je, umístění šifrovacího softwaru ve vrstvě nad operačním systémem, ten má na jeho funkčnost velký vliv. Vyplývá nám z toho, že pokud budeme vybírat nějaký

šifrovací software musíme ho vybírat podle druhu operačního systému, který máme v zařízení nainstalovaný. Jako zástupce šifrovacích programů si můžeme uvést Kryptel, BestCrypt, TrueCrypt, Cloudfogger a mnoho dalších. Některé z těchto programů jsou rozebrány níže.[11]

3.3 Šifrovací programy

3.3.1 TrueCrypt

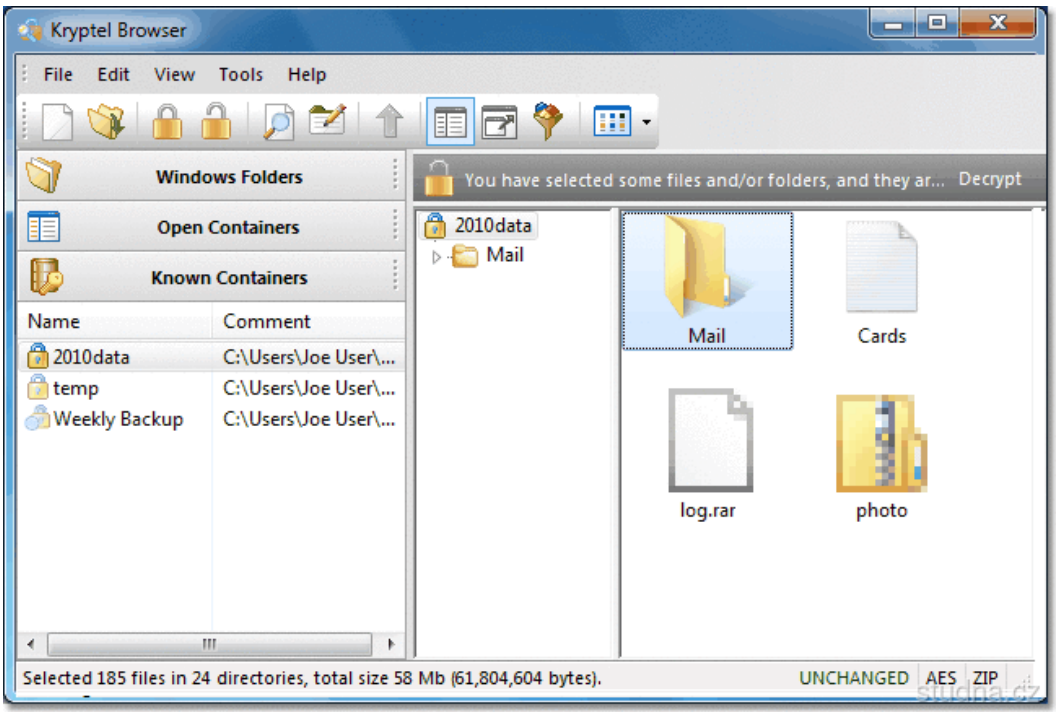
Program umožňuje vytvořit virtuální šifrovaný disk (uvnitř souboru), který lze používat jako skutečnou diskovou jednotku, zašifrovat celý diskový oddíl nebo přenosné datové úložiště (např. USB disk). Každý soubor, který je na disk ukládán je automaticky, během ukládání, šifrován. Možné je i vytvoření skrytých šifrovaných diskových jednotek. Soubory uložené na šifrovaném disku jsou čitelné jen po jeho připojení za použití správného hesla nebo klíče. Umožňuje šifrování systémových oddílů (všechny podporované OS) i nesystémových oddílů bez ztráty dat. Nabízí použití šifrovacích algoritmů AES-256, Serpent a Twofish. Podporována je hardwarová akcelerace na moderních procesorech.[12] Vzhled tohoto programu je na obrázku Obr.12.



Obr. 12 Vzhled programu TrueCrypt [12]

3.3.2 Kryptel

Kryptel je šifrovací software k ochraně dat. Používá silné kryptovací algoritmy (AES, Triple-DES, Blowfish, Twofish, Serpent, IDEA), obsahuje skartovač souborů (specifikace 5220.22-M), umožňuje efektivní kompresi dat (ZIP, BZIP), integruje s Windows Explorerem, podporuje příkazový řádek (možnost použití v dávkách nebo jako NT služba), tvorba šifrovaných záloh [13]. Vzhled tohoto programu je na obrázku Obr.13.



Obr. 13 Vzhled programu Kryptel [13]

3.4 Šifrovací zařízení ICZ Protect Boot

Ochrana je založena na principu zabezpečeného bootování a šifrování disku počítače s využitím silného hesla (64B), které je uloženo na předmětu ICZ Protect Boot, s možností centrální správy vnitřním ICT. Nechrání notebook s daty uživatelů proti pracovníkům vnitřního ICT.

Zavaděč operačního systému je vždy načítán z ICZ Protect Boot (zajištění integrity zavaděče operačního systému).

Silné heslo uživatel nezná, není vkládáno z klávesnice (ochrana před softwarovými i hardwarovými keyloggery). Na obrázku Obr.14 je zobrazeno zařízení ICZ Protect Boot.

Obr. 14 Zařízení ICZ ProtectBoot

Disk notebooku zašifrovaný s využitím ICZ Protect Boot neovlivňuje na disku instalovaný operační systém. Aplikace instalované v operačním systému pracují transparentně. Další bezpečnostní aplikace typu antivir, nebo jiné bezpečnostní produkty pro zabezpečení nastavení operačního systému nebo šifrování dat jsou vhodnými doplňky, které se s ICZ Protect Boot neovlivňují a základní ochranu ICZ Protect Boot vhodně doplňují.

Bezpečnostní produkty třetích stran pak mohou chránit pracovní informace a data uživatele před neoprávněným užitím pracovníky vnitřního ICT.

3.4.1 Vlastnosti a výhody

- BIOS (EFI/UEFI) počítače musí umožňovat boot z USB.
- Trusted Platform Module v počítači není potřeba.
- USB 1.1, 2.0, 3.0 kompatibilní bezpečnostní hardware s vlastním procesorem a firmwarem v odolném obalu obsahuje vlastní zavaděč operačního systému a silné 64 Byte heslo s vysokou entropií.

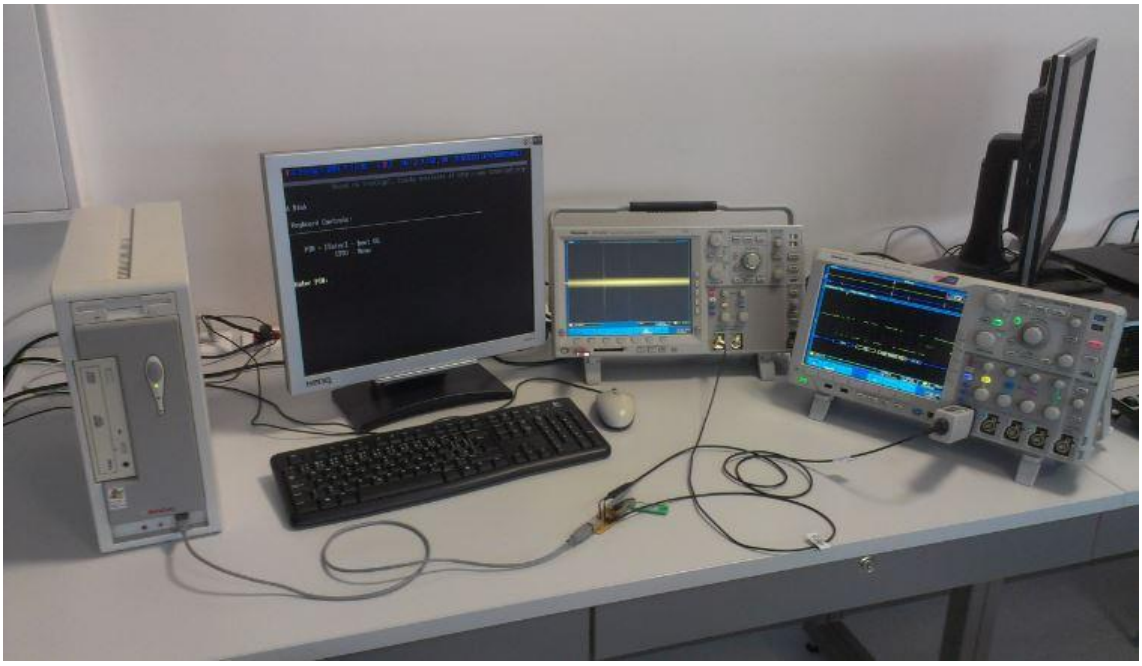
- Uživatel zná jen alfanumerický PIN, kterým je zajištěn přístup k heslu uloženému v ICZ Protect Boot. Toto heslo uživatel negeneruje, nemůže jej změnit a tím tak degradovat úroveň zabezpečení.
- Běžný HDD/SSD je zašifrován AES 256-bit na úrovni sektorů.
- Využívá vlastností standardní edice SW TrueCrypt.
- Prostředí instalovaných Windows a aplikací, běžné pracovní činnosti, zálohování ani případná obnova dat nejsou ovlivněny.
- Zabezpečení heterogenní podnikové flotily počítačů s operačními systémy Windows 7 (SP1) a Windows 8 (32/64b).
- Uživatelsky přívětivý, nevyžaduje školení ani zvláštní znalosti.
- Určen pro společnosti všech velikostí.
- Vhodné pro projektové nasazení.
- Zabezpečená centrální správa.
- Možnost rozšíření Důvěryhodné výpočetní základny®.

3.4.2 Hrozby a rizika

- celá bezpečnost šifrovacího klíče je založená na znalosti PIN kódu. Z tohoto důvodu vznikl úkol otestovat toto zařízení na možnosti útoku, jaké má útočník k tomu, aby uhodl PIN zařízení ICZ Protect Boot.

4 PRAKTICKÁ ČÁST

V rámci praktické části bylo mým úkolem otestovat odolnost zabezpečovacího zařízení ICZ Protect Boot. Experimentální pracoviště je zobrazeno na obrázku Obr. 15.



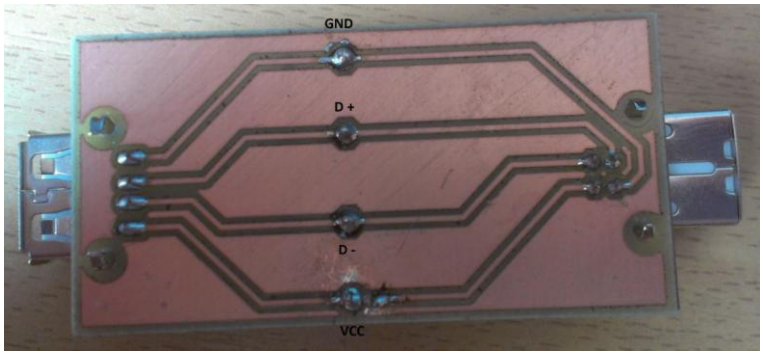
Obr. 15 Experimentální pracoviště

4.1 Úkoly praktické části

- Rozhraní mezi počítačem a zařízením umožňující snímání odebíraného proudu
- Odolnost na proudovou analýzu
- Komunikace zařízení s počítačem

4.1.1 Rozhraní mezi počítačem a zařízením umožňující snímání proudu

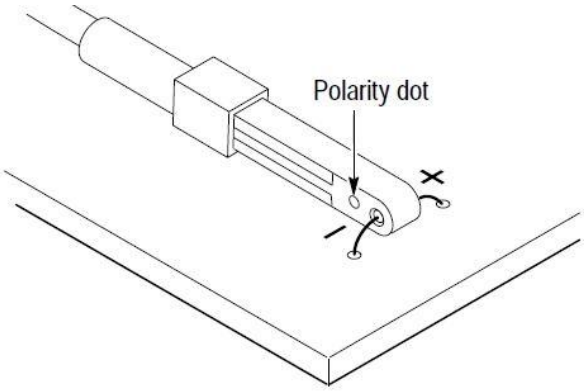
Jako rozhraní mezi počítačem a zařízením, které umožňuje snímat proud, jsem si vytvořila desku plošných spojů. Návrh této desky byl vytvořený v programu EAGLE 6.4.0. a pomocí knihovny obsažené v něm. Nejprve jsem vytvořila schéma, z kterého se mi vygenerovali součástky, které jsem měla správně umístit a navzájem propojit, do prostoru vymezeného pro desku plošných spojů. Podle tohoto návrhu jsem si nechala vyrobit samotnou desku plošných spojů a následně do ní zapájela součástky viz Obr. 16. Tato deska obsahuje 2 konektory, USB-A a USB-B, a vývody pro jednotlivé piny (GND, D+, D-, Vcc). Tato deska sloužila nejen ke snímání odebíraného proudu, ale také ke sledování komunikace zařízení s počítačem, pomocí datových pinů.



Obr. 16 Vyrobená DPS

4.1.2 Odolnost na proudovou analýzu

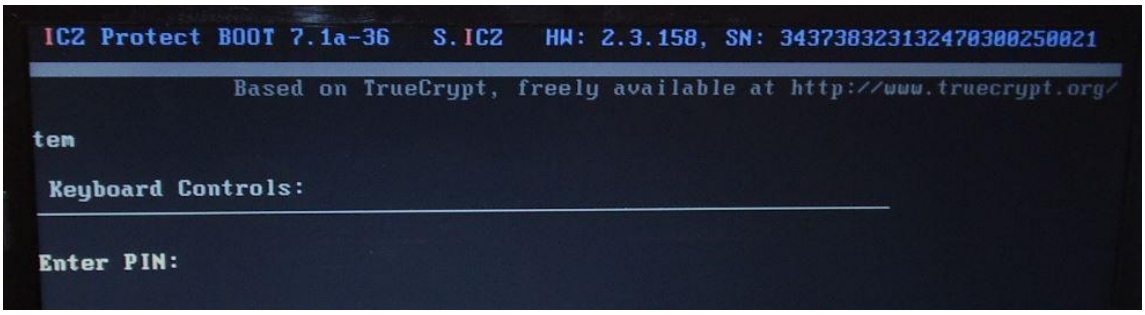
Pomocí vyrobené desky plošných spojů a proudové sondy CT-6 od společnosti Tektronix, jsem se pokusila snímat odebíraný proud zařízením za různých situací na osciloskopu. Na desce plošných spojů budeme využívat 2 vývodů pro napájení (Vcc) spojených pomocí mechanické spojky vodičů (jumper). U proudové sondy je důležité ji správně umístit podle polarizační tečky. Polarizační tečka musí být na záporné straně, viz Obr. 17. Poté správně nastavit osciloskop, aby bylo možné sledovat probíhající změny proudu, tzn. tak, aby byl vidět celý průběh na výšku a nepřesahoval přes obrazovku osciloskopu.



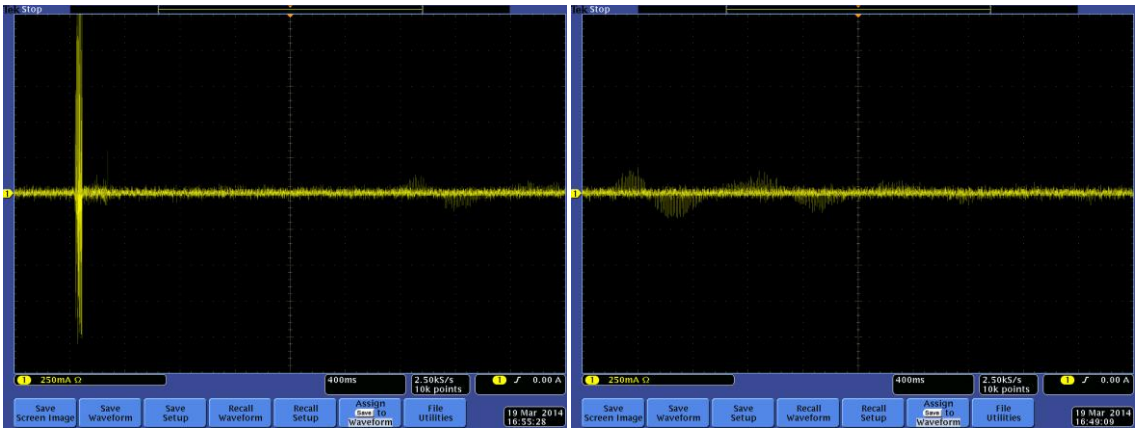
Obr. 17 Správná poloha proudové sondy [14]

Jednou ze situací, při kterých bylo potřeba snímat odběr proudu, je v klidovém stavu, tzn. po startu počítače a načtení úvodní obrazovky s žádostí o PIN, viz Obr.18. Změny v proudovém odběru jsem sledovala od spuštění počítače po samotné načtení úvodní obrazovky. Při sledování proudového odběru se hned po načtení obrazovky

objevil jeden velký „impuls“, viz Orb.19. Tento „impuls“ se objevoval vždy při startu počítače. V žádné další situaci nenastal. V klidovém stavu jsem si mohla všimnou také stále se opakujícího průběhu, který se objevoval i ve všech ostatní situacích ve stejných časových odstupech.



Obr. 18 Výřez z úvodní obrazovky s žádostí o pin



Obr. 19 „Impuls“ při načtení obrazovky (vlevo) a stále se opakující průběh (vpravo)

Další situace, při kterých bylo potřeba sledovat proudový odběr, byly situace při zadávání správného PIN kódu, zadávání špatného PIN kódu a při změně PIN kódu.

Při opakovaném zadávání správného PIN kódu, se mi nejdříve nepodařilo naměřit správné výsledky. Buď se průběh vůbec nezměnil, nebo se tam objevil pouze jeden impuls nahoru od průběhu nebo dolů od něj. Při dalším měření a lepším nastavení osciloskopu se výsledky shodovali, viz příloha A.1. Bližší pohled na naměřené průběhů je zobrazen na příloze A.2.

Při zadávání špatného PIN kódu jsou výsledky téměř stejné. Pokud se zadává PIN s jedním špatným znakem nehledě na jeho umístění,tzn. jestli je to 1.znak v PIN

kódu nebo poslední, výsledek průběhu je stále stejný. Změna nastává jestliže zadáme o znak navíc a znaky jsou různé, viz příloha A.3 a A.4. Tuto změnu je možné vidět nejlépe v příloze A.4, jedná se o světle modrý průběh.

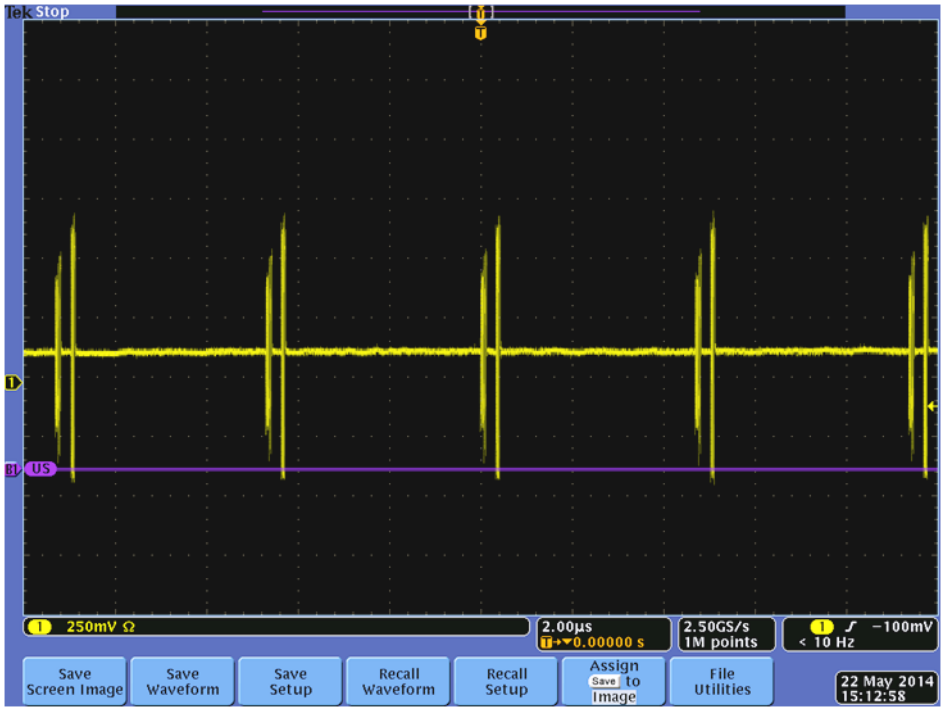
Při změně PIN kódu jsou průběhy podobné, viz příloha A.5 a A.6. Modrý průběh zobrazuje změnu PIN kódu z „start“ na „12345“. Červený průběh zobrazuje změnu PIN kódu z „12345“ na „start“.

Srovnání proudových odběrů při zadání správného a špatného PIN kódu je zobrazeno v příloze A.6. a A.7 Červený průběh zobrazuje správně zadaný PIN a modrý průběh špatně zadaný PIN. Z těchto výsledků můžeme vidět, že se mění délka celého průběhu.

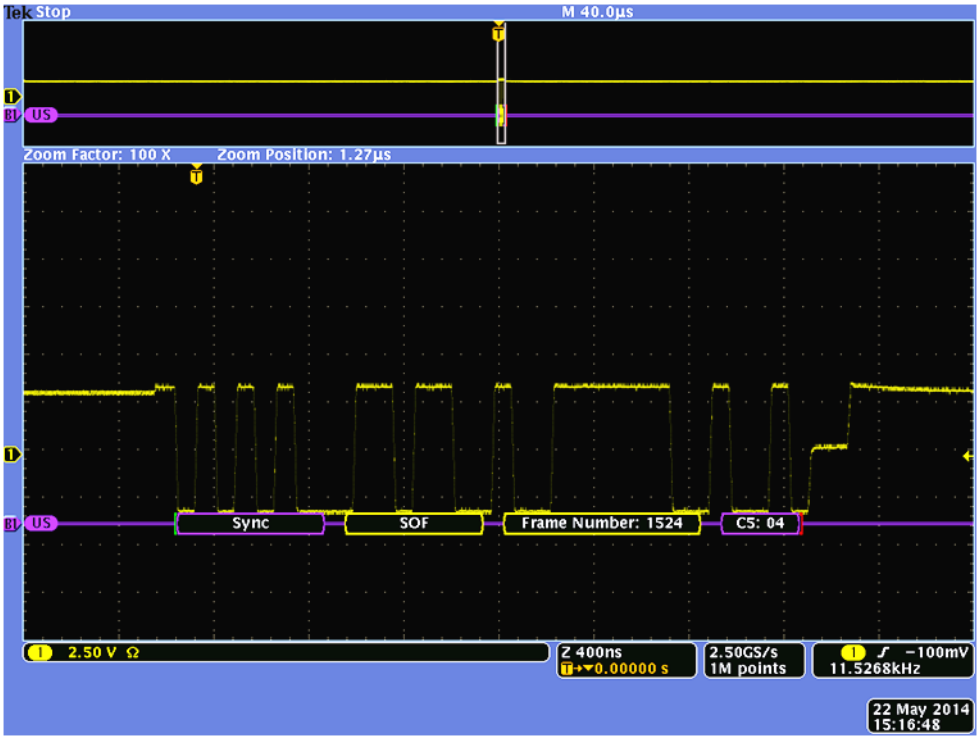
Podle naměřených průběhů a dále jejích analýzy si myslím , že by bylo možné získat PIN kód.

4.1.3 Komunikace zařízení s počítačem

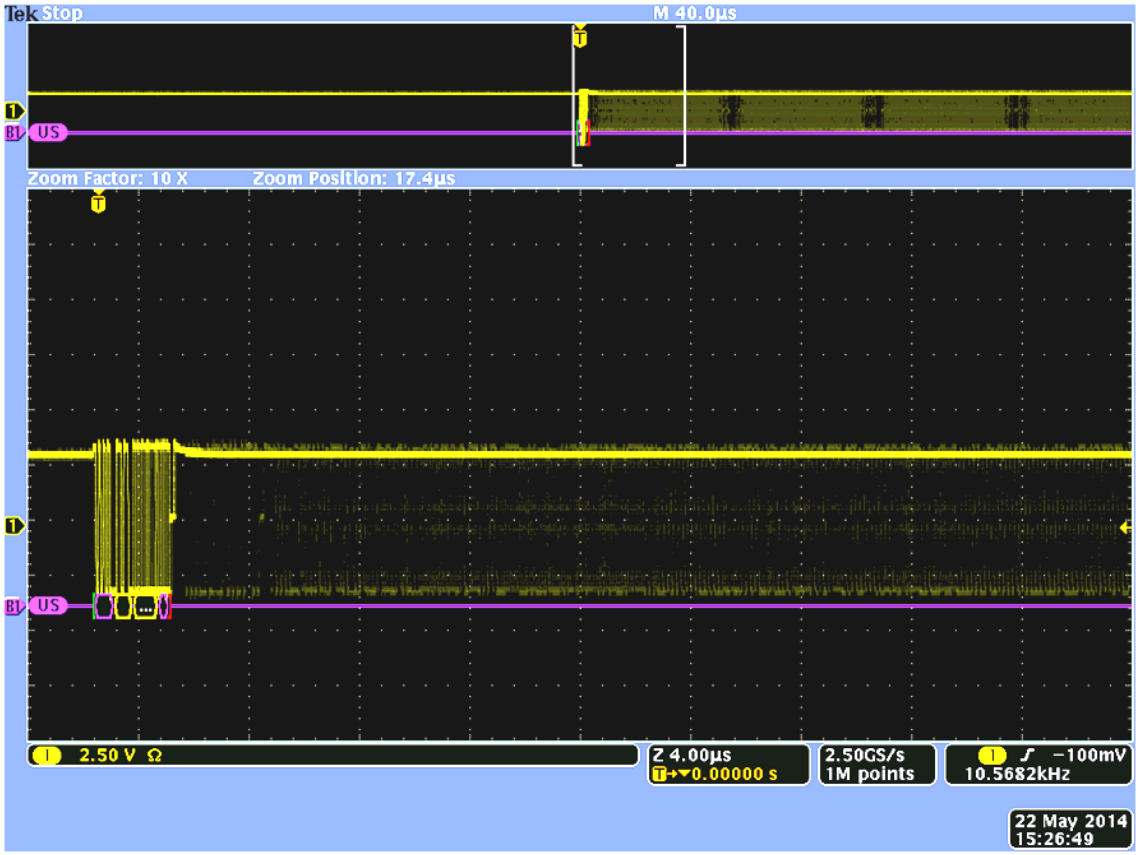
I v tomto případě využijeme vyrobenou desku plošných spojů, tentokrát ale její TDP0500 a nakonec osciloskop. Sondu připojíme k datovým vývodům a nastavíme na ní rozsah 4,25V, aby bylo měření přesnější. Další důležitou částí měření je správné nastavení osciloskopu. Délka nahrávání (záznamu) nastavena na 1M pro lepší rozlišení. Po správném nastavení osciloskopu jsem zapnula počítač a nechala najet operační systém. Pro otestování správného nastavení jsem zapojila nejdříve flash disk a přenášela data z něj na plochu, na osciloskopu byl vidět paketový přenos dat, viz Obr. 20. Díky úspěšnému otestování jsem zapojila v systému i zařízení ICZ ProtectBoot a zapnula dekódování. Výsledkem je obrázek Obr. 21 a také důkazem, že zařízení s počítačem komunikuje i při načteném systému. Můžeme zde vidět jednotlivé bloky: synchronizace (SYNC), začátku rámce (SOF), rámec i se svým označením (Frame Number: 1524). Stejným výsledkem je i dekódování komunikace při načtení úvodní obrazovky a žádosti o pin. Pomocí funkce „single“ se mi nepodařilo zachytit datovou komunikaci při zadávání pinu. Povedlo se mi pouze zachytit jak mizí z obrazovky osciloskopu a to pomoci funkce „start/stop“, viz Obr. 22.



Obr. 20 Paketový přenos



Obr. 21 Dekódovaná komunikace zařízení s počítačem při načteném systému



Obr. 22 Zachycený průběh při zadávání pinu

V horní části obrázku Obr.22 si můžeme všimnout, že při zadávání pinu dojde k datovému přenosu složeného z více bloků. Kvůli rychlému datovému přenosu nebylo v mým silách tento průběh zachytit lépe.

ZÁVĚR

V rámci praktické časti bakalářské práce, bylo mým úkolem seznámit se a vyzkoušet funkčnost zařízení umožňující zabezpečené bootování a šifrování disku počítače. Jedná se o výše zmíněné zařízení ICZ Protect Boot. Zařízení bylo testováno na jednom z počítačů v laboratoři. Zařízení bylo zasunuto do konektoru a po spuštění počítače se objevila úvodní obrazovka s žádostí o zadání pinu. Po zadání pinu byla možnost dále pracovat v tomto prostředí, jako např. změnit pin, odebrat (smazat) počítač ze seznamu používaných přístrojů tímto zařízením.

Dalším úkolem bylo vyzkoušet odolnost na proudovou analýzu. Z tohoto důvodu bylo nutné vytvořit rozhraní mezi počítačem a zařízením, které by snímalo odebíraný proud. Vytvořila jsem desku plošných spojů, pomocí které jsem měla možnost snímat odebíraný prou zařízením. Z naměřených výsledků vyplývá jistá souvislost proudové spotřeby na zadávání. Při správném zadání PIN kódu se průběh nemění, je stejný. Při zadávání špatného PIN kódu jsou průběhy téměř stejné, jen v některých případech se liší, např. při zadání znaku navíc a zadání jiných znaků než jsou obsaženy v PIN kódu. V příloze A.7 jsou dva proudové průběhy, průběh při správném zadání a průběh při špatném zadání. Tyto průběhy jsou různé délky, ale do určité části podobné. Poslední úkolem měření proudové spotřeby bylo změřit průběh při změně PIN kódu. Výsledky tohoto měření je možné vidět v příloze A.5 a A.6. Průběhy jsou podobné.

Zjistit a dekódovat komunikaci mezi počítačem a zařízením, byl poslední úkol praktické části. Díky diferenční sondě a osciloskopu podporující USB dekódování jsem se mohla přesvědčit, že mezi sebou komunikují. Nebylo však v mých silách zachytit průběh při zadávání pinu či jeho změně.

Podle naměřených průběhů zadávání PIN kódu a dále jejich analýzy by bylo možné získat PIN kód.

Z dostupného zdroje [15] je možné se dočíst, že TrueCrypt nejspíš končí. Tento program spolupracuje se zařízením ICZ Protect Boot. Podle informací článku obsahuje program TrueCrypt bezpečnostní chyby a není bezpečné jej nadále používat. Uvádí také možnou alternativu tohoto programu.

LITERATURA

[1] Kryptologie. In: *Amphora Research Group* [online]. 2013 [cit. 2013-12-31]. Dostupné z: http://arg.vsb.cz/Data/Vyuka/PVB12.pdf

[2] Bezpečná komunikace uživatelů. In: *Elektrorevue* [online]. 2002 [cit. 2013-12-31]. Dostupné z: http://www.elektrorevue.cz/clanky/02021/index.html

[3] BURDA, K. *Bezpečnost informačních systémů.* 1. Brno: FEKT VUT Brno, 2005. s. 1 (s.)

[4] *Moderní kryptoanalýza* [online]. Brno, 2011 [cit. 2013-12-31]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/4136/Modern%C3%AD%20kryptoanal%C3%BDza.pdf?sequence=1. Diplomová práce. VUT v Brně.

[5] *Útoky na kryptografické moduly* [online]. Brno, 2008 [cit. 2013-12-31]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/5793/danecek-syllabus.pdf?sequence=1. Diplomová práce. VUT v Brně.

[6] Praktické základy Kryptologie a Steganografie. In: *Security-Portal.cz* [online]. 2004 [cit. 2014-01-02]. Dostupné z: http://www.security-portal.cz/clanky/praktick%C3%A9-z%C3%A1klady-kryptologie-steganografie

[7] *Kryptoanalýza postranními kanály*. Brno, 2013. Dizertační práce. VUT v BRně.

[8] Pevný disk (HDD). *Hardware-Kolář* [online]. 2010 [cit. 2014-01-02]. Dostupné z: http://hardwarekolar.blogspot.cz/2010/09/pevny-disk-hdd.html

[9] Šifrovaný externí disk Stealth HD BIO Gen II 320GB. *ODPOSLECHY.COM* [online]. 2012 [cit. 2014-01-02]. Dostupné z: http://www.odposlechy.com/sifrovany-externi-disk-stealth-hd-bio-gen-ii-320gb

[10] Moderní metody zabezpečení uživatelských počítačů (1.díl). *SystemOnLine* [online]. 2011 [cit. 2014-01-02]. Dostupné z: http://www.systemonline.cz/it-security/moderni-metody-zabezpeceni-uzivatelskych-pocitacu-1-dil.htm

[11] Moderní metody zabezpečení uživatelských počítačů (2.díl). *SystemOnLine* [online]. 2011 [cit. 2014-01-02]. Dostupné z:

http://www.systemonline.cz/it-security/moderni-metody-zabezpeceni-uzivatelskych-pocitacu-2.-dil.htm

[12] TrueCrypt 7.1a. *Dobré programy* [online]. 2012 [cit. 2014-01-02]. Dostupné z: http://www.dobreprogramy.cz/truecrypt

[13] Kryptel 6.4. *Dobré programy* [online]. 2013 [cit. 2014-01-02]. Dostupné z: http://www.dobreprogramy.cz/kryptel

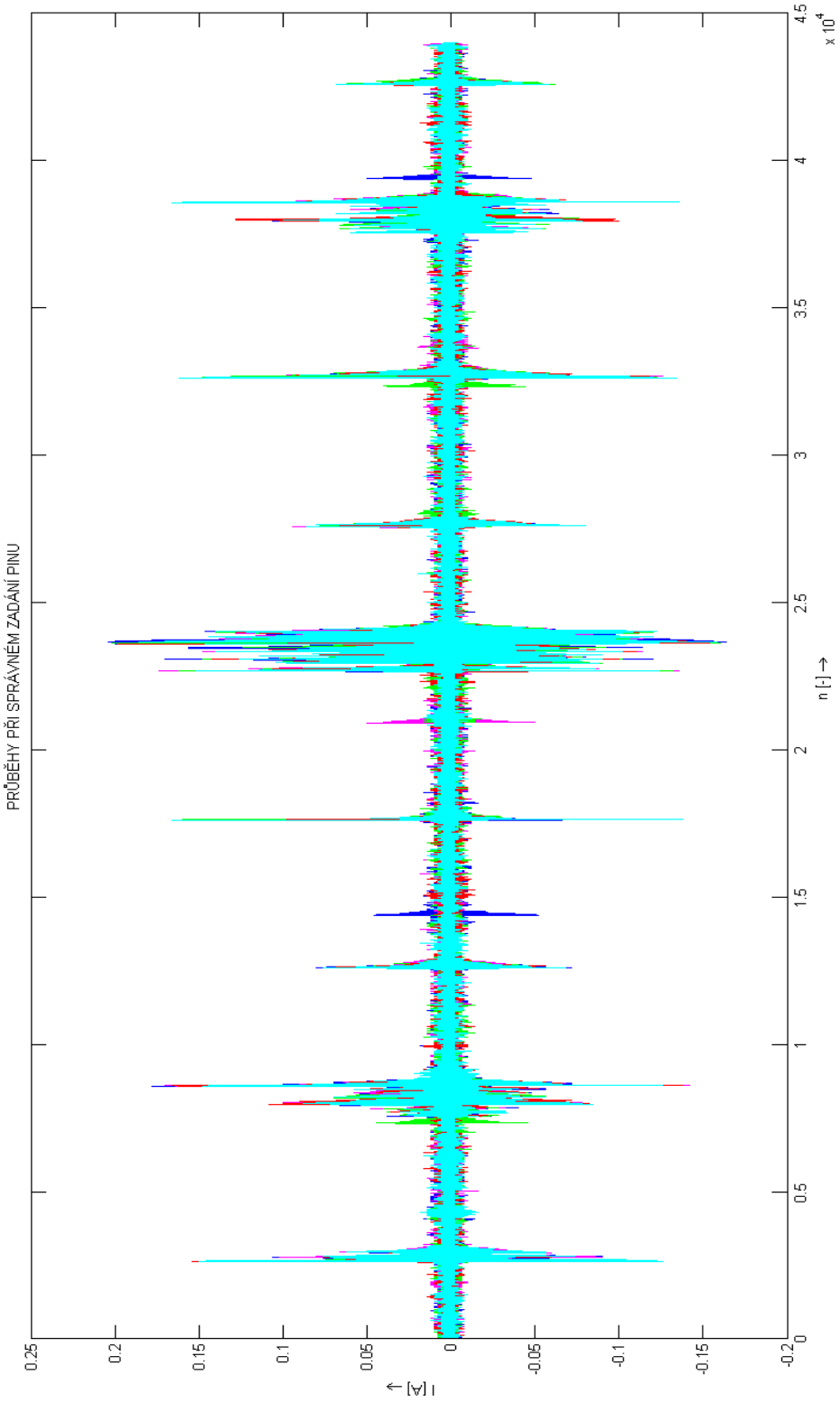
[14] CT-6 High Frequency AC Current Probe. In: *PEWA* [online]. 1998 [cit. 2014-05-28]. Dostupné z: http://www.pewa.de/DATENBLATT/DBL_TEK_CTX-SERIE_MANUAL_ENGLISCH.pdf

[15] TrueCrypt zřejmě končí, jeho používání prý není bezpečné. *ŽIVĚ* [online]. 2014 [cit. 2014-06-04]. Dostupné z: http://www.zive.cz/clanky/truecrypt-zrejme-konci-jeho-pouzivani-pry-neni-bezpecne/sc-3-a-173899/default.aspx

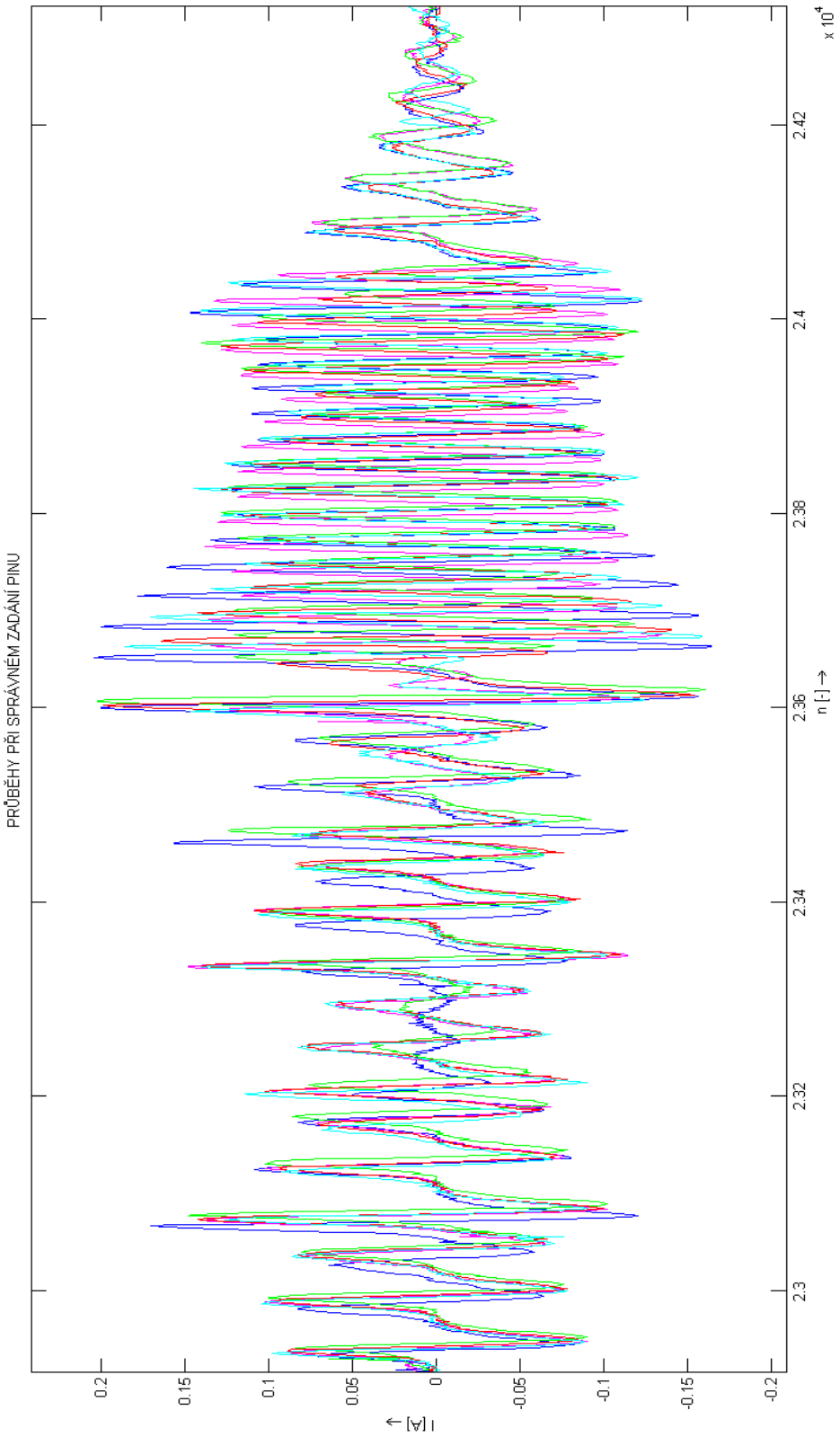
SEZNAM PŘÍLOH

A SNÍMÁNÉ PRŮBĚHY PROUDOVÉ SPOTŘEBY

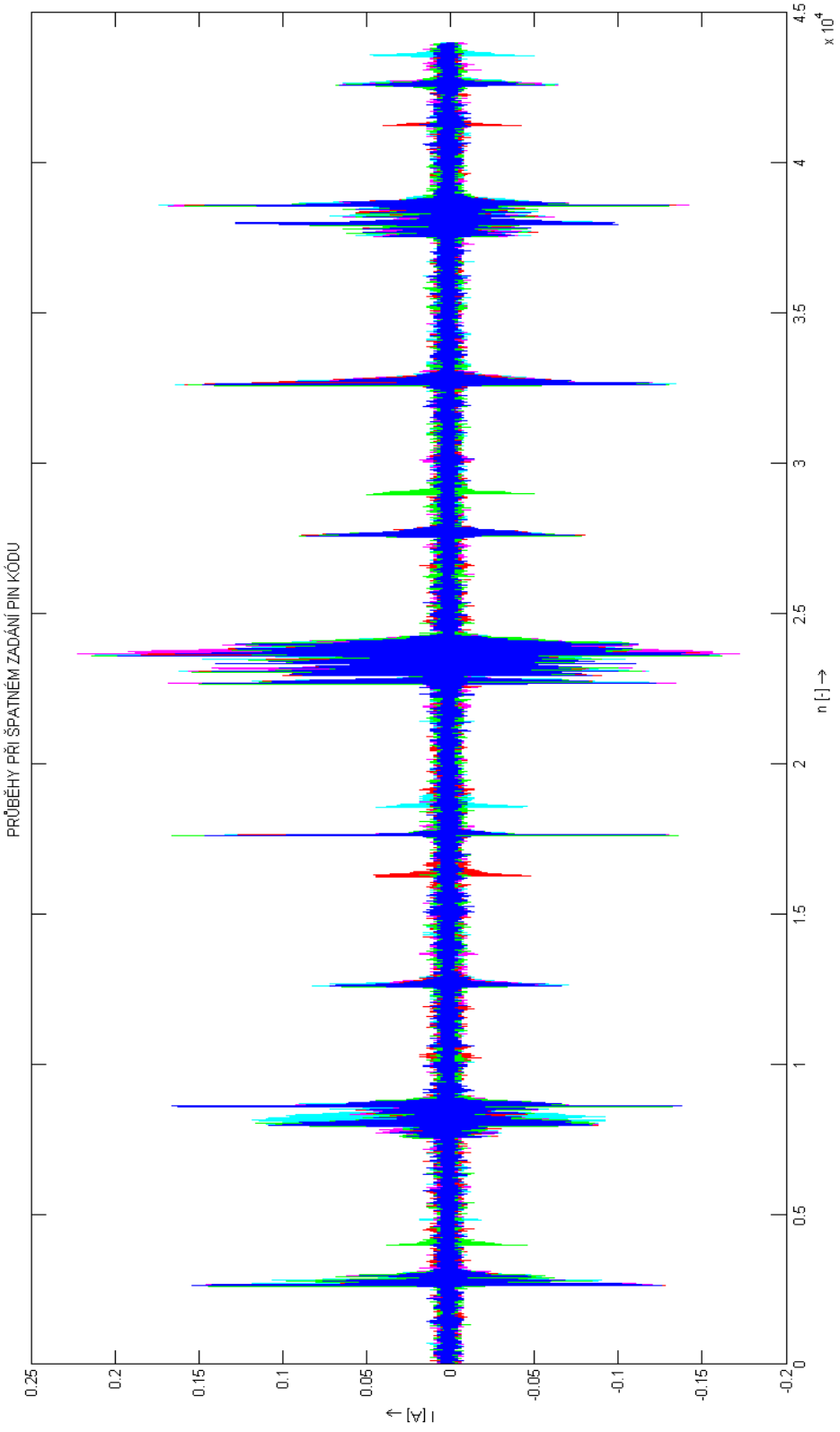
A.1 Zadání správného PIN kódu



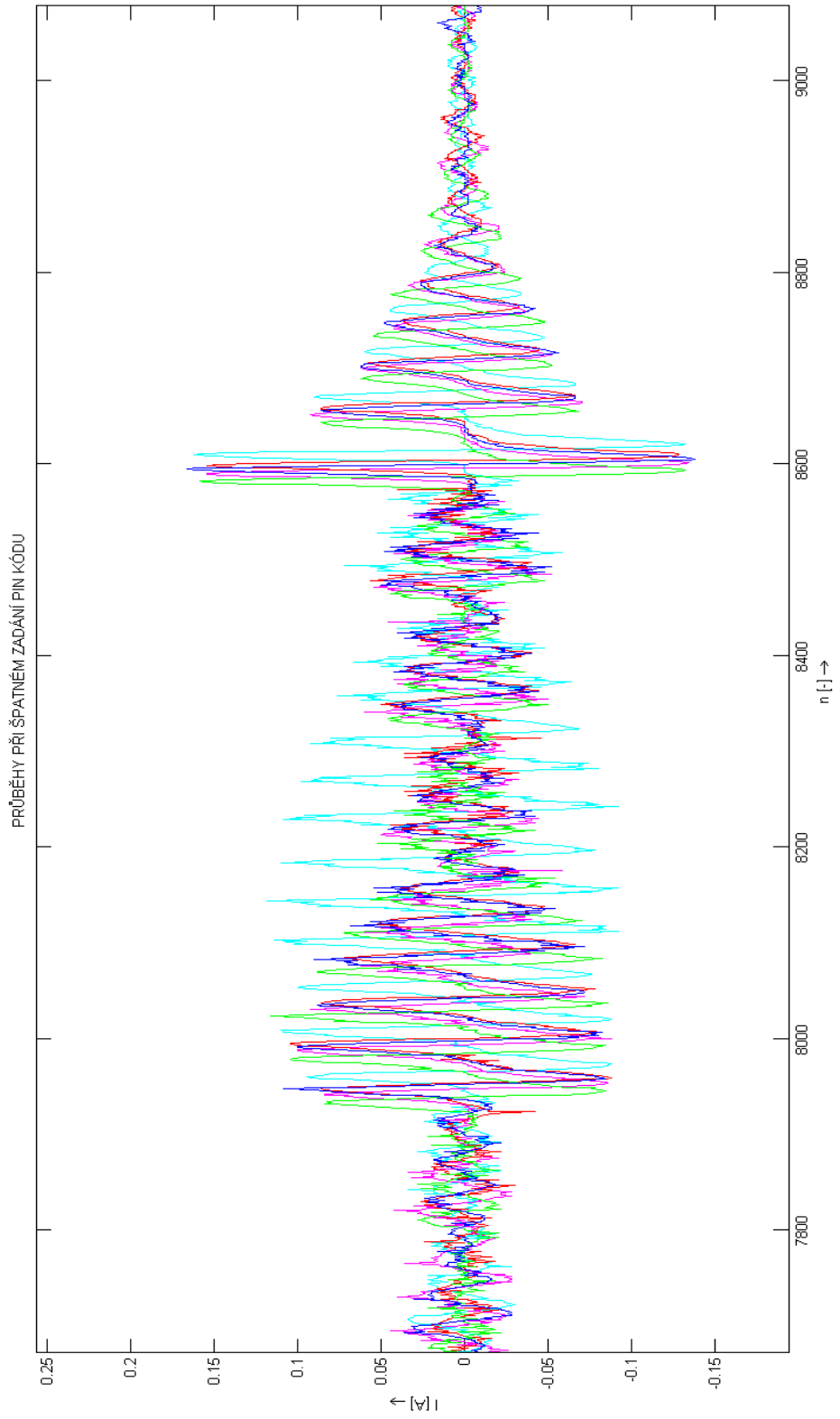
A.2 Zadání správného PIN kódu - bližší pohled



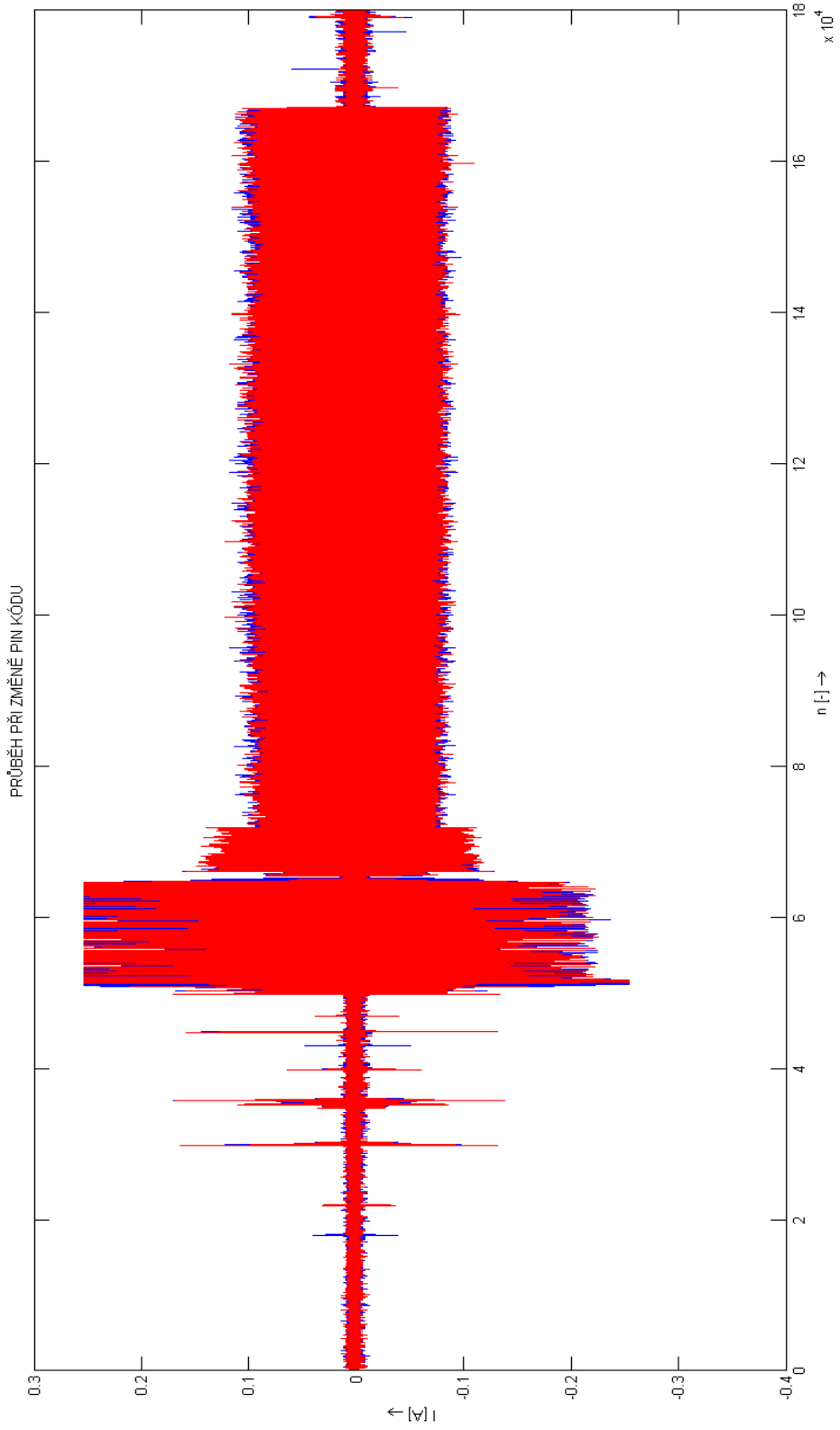
A.3 Zadávání špatného PIN kódu



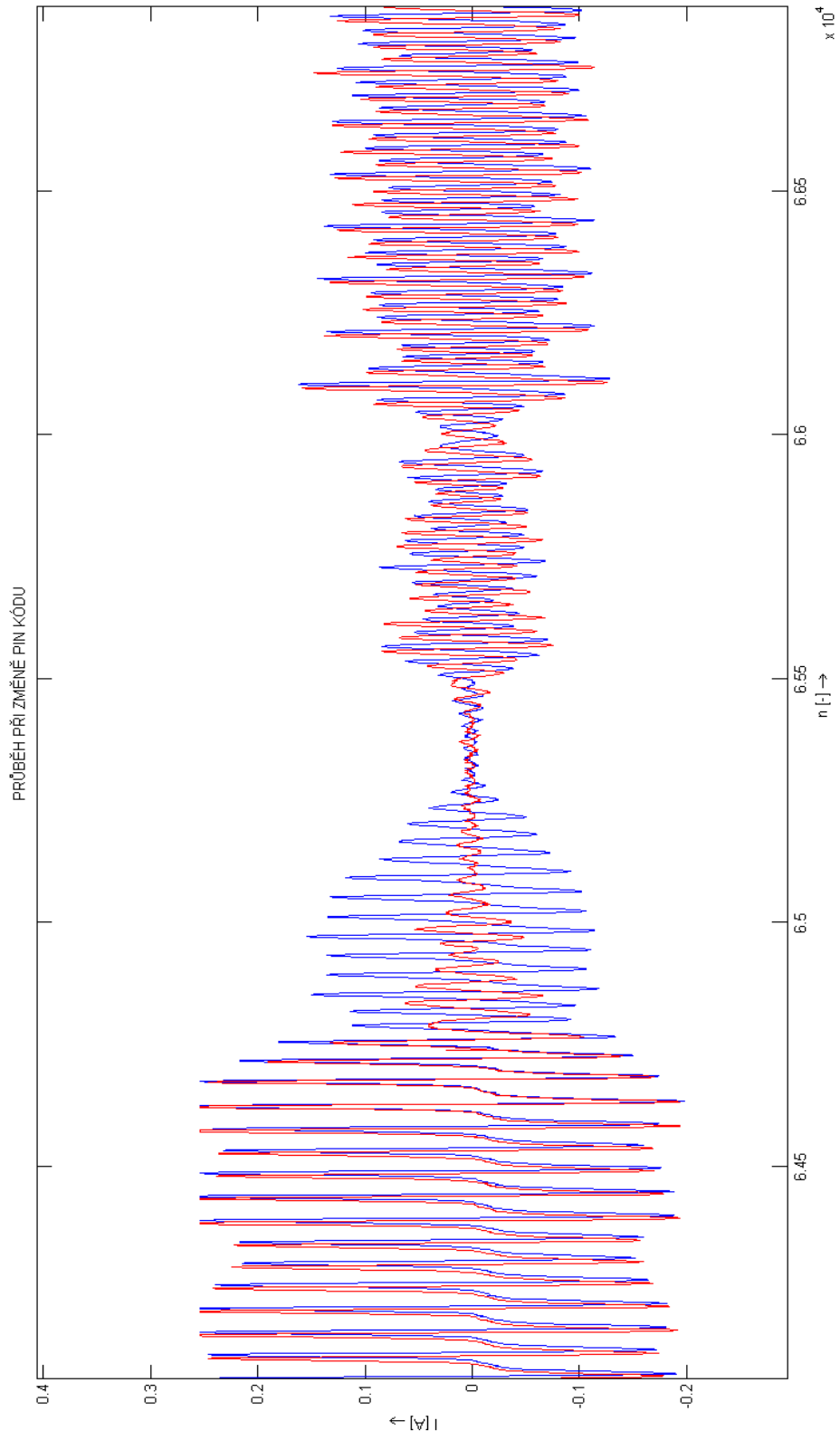
A.4 Zadávání špatného PIN kódu - bližší pohled



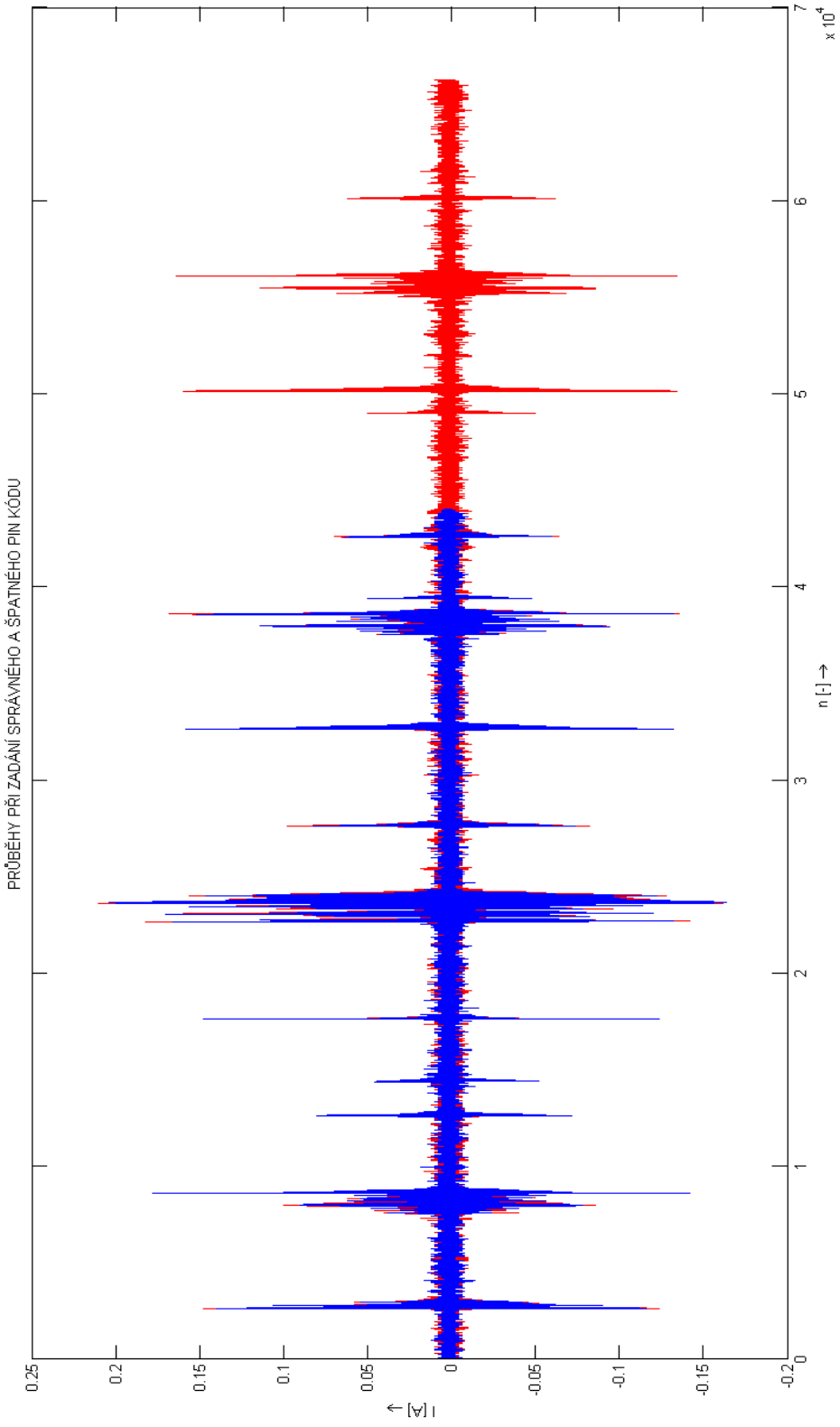
A.5 Změna PIN kódu



A.6 Změna PIN kódu -bližší pohled



A.7 Porovnání průběhů při zadání správného a špatného PIN kódu



A.8 Průběhy zadání správného a špatného PIN kódu - bližší pohled