METODY ODPOSLOUCHÁVÁNÍ KLÁVESNICE

Metods of keyboard eavesdropping

David Swiatek

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David SWIATEK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Metody odposlouchávání klávesnice**

Zásady pro vypracování:

Cílem práce je vytvořit přehled metod používaných pro odposlouchávání dat zadávaných z klávesnice osobního počítače. Jednotlivé metody budou posouzeny z hlediska jejich přesnosti a nákladnosti potřebného vybavení. Součástí práce budou také postupy ochrany před odposlechem používané v praxi, případně návrh dalších postupů.

1. **Proveďte literární rešerši zabývající se metodami odposlechu klávesnice. Vytvořte kategorizaci používaných metod.**
2. **Podrobněji popište metody odposlechu klávesnice, které nevyžadují zásah do softwarového vybavení počítače.**
3. **Zhodnoťte přesnost a finanční náročnost jednotlivých odposlouchávacích metod.**
4. **Uveďte způsoby, kterými lze jednotlivé metody odposlechu detekovat.**
5. **Vytvořte seznam preventivních opatření, kterými lze snížit riziko odposlechu klávesnice.**

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. SALOMON, David. Foundations of Computer Security . 1st edition. [s.l.] : Springer, 2005. 369 s. ISBN 978-1846281938.
2. MCNAMARA, Joel. Secrets of Computer Espionage : Tactics and Countermeasures . 1st edition. [s.l.] : Wiley, 2003. 408 s. ISBN 978-0764537103 .
3. LOCKHART, Andrew.. Network security hacks. 2nd ed. Beijing ; Cambridge : OReilly, c2007. xx, 455 s. : ISBN 978-0-596-52763-1. ISBN 0-596-52763-2.
4. ENDORF, Carl F.,. Detekce a prevence počítačového útoku /. 1. vyd. Praha : Grada, 2005. 355 s. : ISBN 8024710358 (brož.).
5. PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace : jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G /. Vyd. 1. Brno : CP Books, 2005. 179 s. : ISBN 80-251-0791-4 (brož.).
6. CHAPWESKE, Adam. The PS/2 Mouse/Keyboard Protocol [online]. [2003] , 05/09/03 [cit. 2010-01-25]. Anglicky.
7. USB.org - HID Tools [online]. [2009] [cit. 2010-01-25]. Anglicky.

Vedoucí bakalářské práce: **Ing. Petr Chalupa, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Předmětem bakalářské práce je seznámení se s metodami odposlouchávání klávesnice. Práce v úvodu pojednává o počítačové klávesnici všeobecně. V další části následuje seznámení se s keyloggingem – tedy odposlouchávání klávesnic při použití softwarového či hardwarového keyloggingu. Na závěr je zamyšlení nad právními aspekty používání keyloggingu.

Cílem této bakalářské práce je poukázání na nebezpečí, které ohrožuje uživatele PC a dalších zařízení využívajících klávesnici jako vstupních periferii. Odposlech klávesnice za účelem zneužití získaných informací ve výsledku ohrožuje soukromí, finance, knowhow, případně jiné hodnoty uživatelů klávesnice.

Klíčová slova:

Keylogging, odposlech klávesnice, keylogger, zabezpečení klávesnice, softwarové odposlouchávání, elektromagnetické záření, rozložení kláves, hardwarový odposlech, Malware, spyware

ABSTRACT

Subject of this thesis is familiar with methods of eavesdropping the keyboard. This work universally talks about a computer keyboard in the beginning. In the next section followed by a familiarity with keylogging - that is, eavesdropping the keyboard with keylogging software or hardware. In conclusion, there is a reflection about legal aspects of the use of keylogging.

The aim of this work is to highlight the danger for users of PCs and other devices using the keyboard as input peripheral. Eavesdropping the keyboard ultimately threatens the privacy, finance, know-how, or other values of keyboard users.

Keywords:

Keylogging, keyboard eavesdroppin, keylogger, security, keyboard, software eavesdropping, electromagnetic radiation, keyboard layout, a hardware keylogger, malware, spyware

Poděkování

Poděkování patří vedoucímu bakalářské práce panu Ing. Petru Chalupovi Ph.D. za odborné rady, pečlivé posuzování, za vedení a za cenné připomínky. Obzvlášť bych chtěl poděkovat za pružnost a vstřícnou spolupráci. Připojuji také poděkování své ženě a právě se narodivšímu synu za podporu a trpělivost.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Co je to odposlouchávání z klávesnice a k čemu je to dobré? Keylogging, jak se také odposlouchávání klávesnice říká, je činnost vedoucí ke zjištění stisknutých kláves na klávesnici a to způsobem skrytým, před osobou klávesnici používající. Může se jednat o počítačové nebo jiné například bankomatové klávesnice. Jelikož nemáme jednoduchý čistě český výraz pro odposlech klávesnice, budu používat počeštěný anglický keylogging a keylogger pro použitý software nebo jiný nástroj k odposlouchávání klávesnice.

Díky dnešnímu rozšíření internetu se snad každý jeho uživatel zabývá bezpečností svého připojení. Mnoho z nich používá wifi routery k pokrytí svých bytů či firemních prostor pohodlným bezdrátovým připojením. Všichni tito uživatelé řeší bezpečnost svých připojení. Každý uživatel počítače používá klávesnici, ale jen málo lidí tuší, že by se mělo zajímat o její zabezpečení. A nejen o zabezpečení klávesnice, ale i myši a dalších vstupních zařízení. Výrobci nekladou přílišný důraz na zabezpečení takových zařízení a proto je jejich šifrování velmi slabé.

Virové hrozby jsou dnes spíše na ústupu, ale právě keylogging je jedním z velmi jednoduchých a účinných nástrojů k napadení soukromí uživatelů PC. Z právního hlediska nemusí být jejich použití vždy nezákonné, ale zákonné pole působnosti příliš široké není.

Způsoby odposlouchávání lze rozdělit do třech základních skupin podle použité technologie. Zaprvé je to softwarové odposlouchávání, zadruhé odposlouchávání s využitím hardwaru. Třetí skupinu bych nazval „ostatní“ a zařadil bych do ní například využití elektromagnetického záření.

1 POČÍTAČOVÁ KLÁVESNICE

Nejprve bych se chtěl podrobněji zabývat počítačovou klávesnicí, neboť je třeba znát určitá specifika. Jedná se o rozložení znaků na klávesnici, typy zapojení klávesnice k počítači, způsob, jakým klávesnice s počítačem komunikuje a také bezpečnost klávesnice.

„Počítačová klávesnice je klávesnice odvozená od klávesnice psacího stroje či dálnopisu. Je určena ke vkládání znaků a ovládání počítače. Vyrábí je například firmy KME, Apple, Logitech a další. Standardní počítačové klávesnice jsou napájeny z počítače a komunikují s ním po sériové lince.“[1]

Klávesnice se skládá z tlačítek zvaných klávesy. Při stisku klávesy dochází k odeslání většinou jednoho znaku. Některé klávesy se používají jen jako předvolba. K tomu, abychom odeslali určitý symbol, je třeba stisku či držení i několika kláves současně. Klávesnice je nepostradatelným prvkem k zadávání hesel, psaní zpráv atd.

1.1 Rozložení znaků klávesnice

Je třeba vědět, že existuje několik druhů rozložení kláves na klávesnici. U keyloggingu je nutné znát typ klávesnice, kterou uživatel používá, protože jinak by docházelo ke značnému zkreslení nebo chybnému zaznamenání konkrétních úhozů na klávesnici.

Ve světě se nachází značná řada rozdílných typů rozložení kláves. Jsou vytvářeny proto, že lidé používají různý jazyk, a také proto, že lidé pro svou práci potřebují klávesnice specializované - pro matematické, účetní nebo programátorské použití.

Rozložení znaků na klávesnici bylo vytvořeno v historii a je ustanoveno mezinárodní normou. I tak však najdeme několik obměn tohoto rozložení.

V řadě států se užívá rozložení kláves zvané QWERTY, jinde QWERTZ. Existuje však také jiné rozložení kláves, jako například francouzské AZERTY. Rozložení kláves je upraveno mezinárodní normou ISO/IEC 9995 „Informační technologie – Uspořádání klávesnice pro textové a kancelářské systémy“ z roku 1997. Tato norma upravuje

---

1 http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_kl%C3%A1vesnice#cite_note-0

rozestavění kláves podle národních norem a zvyklostí. „Např.: - možnost obsazení klávesy B01 (na české Y) znakem Z (např. anglický nebo americký standard) nebo znakem Y (např. český standard) či znakem W (např. francouzský standard), D06 (na české Z) Y nebo Z a pro D02 (na české W) W nebo Z.“[2]

V České republice používáme rozmístění kláves QWERTZ, a to v souvislosti s mezinárodní normou určenou národním standardem. Jedná se o ČSN 36 9050 z roku 1994, která určuje rozmístění symbolů na 48 klávesách ve dvou úrovních, tj. základní a po stisknutí Shift. V této normě není striktně řečeno, kde musí být umístěn např. znak obráceného lomítka nebo generované znaky pomocí kláves Alt Ctrl (3. Úroveň). Je zde však uvedeno umístění znaků „Z“ a „Y“.

Také mnozí čeští uživatelé klávesnice upřednostňují anglickou normu, která vychází z rozložení QWERTY. Je tomu tak z důvodu, že používají ke své práci znaky, které na českém rozložení QWERTZ nejsou. Mohou také používat jen upravenou tzv. českou programátorskou klávesnici, nebo českou QWERTY klávesnici, která se odlišuje jen výměnou kláves Z a Y, a to často pouze jen proto, že si již zvykli na anglickou klávesnici.

Existují také zvláštní rozložení kláves (Dvorak, Colemak, XPeRT), která nejsou moc běžná. Byla vytvořena pro psaní v angličtině a nejsou tak vhodná pro psaní v jiném jazyce. Tato rozložení kláves jsou více závislá na národním jazyce než QWERTY.

Běžná klávesnice je docela velká, protože je nutné mít dostatek prostoru pro snadné stisknutí tlačítka prsty. U přenosných zařízení, kde je třeba minimalizace velikosti zařízení, byly vytvořeny redukované druhy klávesnic, protože standardní klávesnice by zde byly moc velké. Rychlým vývojem a zvýšenými požadavky dochází k rozvoji ultramoderních typů klávesnice a kláves, např. gelové nebo obalované měkkými materiály. Jsou ergonomicky vytvarované pro snadnější dosah na tlačítka. Nesmíme také opomenout interaktivní typy klávesnic, kterých stále přibývá a jsou například u interaktivních tabulí, mobilních telefonů nebo také přímo u monitoru.

[2] http://cs.wikipedia.org/wiki/Počítačová_klávesnice

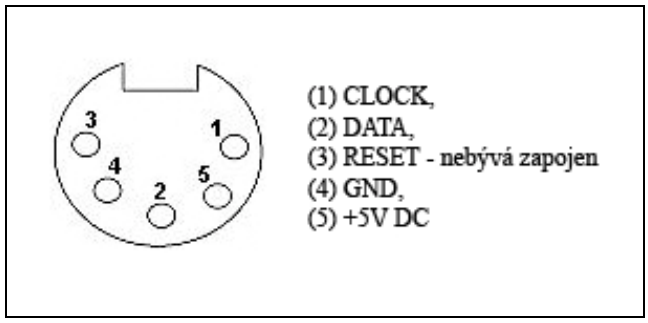
1.2 Připojení klávesnice k počítači

Pro odposlouchávání je důležité znát možnosti připojení klávesnice, a to především u hardwarového odposlechu, kde dochází k propojení odposlouchávaného zařízení s konektorem klávesnice.

1.2.1 **Typy připojení**

a) Konektor DIN

V předešlých letech se používaly pro připojení klávesnice konektory označované „DIN-5“. Konektor DIN má 5 vodičů, ale jen 4 z nich jsou využity. Původní klávesnice s konektorem DIN jsou označeny jako „AT klávesnice“

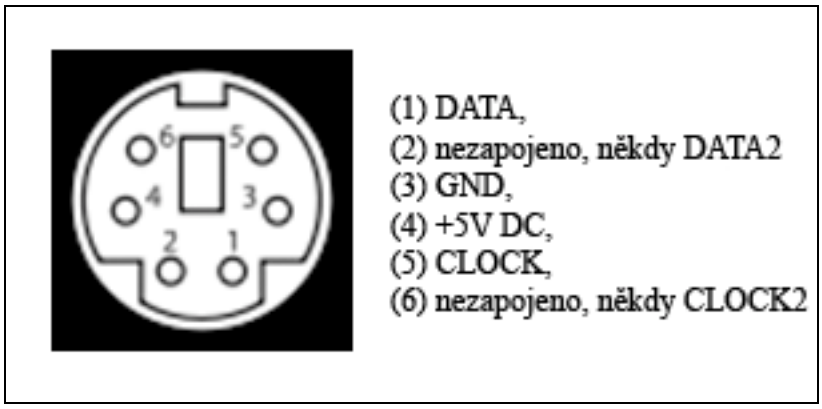


Obrázek 1 Zapojení konektoru DIN-5(samice)

Zapojení konektoru DIN-5 (samice):

b) konektor PS/2 (MiniDIN6)

Konektor PS/2 má 6 vodičů, z nichž 4 využívá. V současné době již všechny nové základní desky počítačů obsahují jen konektor PS/2. Tyto konektory pro klávesnice mají menší nevýhodu v tom, že jsou stejné s konektory pro myš a můžeme je tak lehce zaměnit. Často jsou však označovány barvou, aby k záměně nedošlo.



Obrázek 2 Zapojení konektoru PS/2 (samice)

c) USB

Klávesnici lze připojit také pomocí rozhraní USB. V současné době se jedná o nejběžnější způsob připojení klávesnice a různých dalších zařízení (např. myš. USB flush paměť atd.)[3]

d) Bezdrátová klávesnice

Je sestavena z jednotky, která se zapojí do počítače a ze samotné klávesnice. Komunikace probíhá prostřednictvím infračerveného nebo radiového přenosu, a to ve chvíli, kdy dojde k připojení základní jednotky na rozhraní PS/2 nebo USB. Více se používá radiový přenos než infračervený. Je to z důvodu nutnosti přímé viditelnosti mezi klávesnicí a vysílačem u infračerveného přenosu.

Na různorodost zapojení klávesnic se lze připravit také díky redukci (PS/2 => DIN, DIN => PS/2), kterou si můžeme lehce zakoupit. Nemusíme tak měnit klávesnici a u odposlouchávání z klávesnice můžeme použít jakýkoli typ keyloggeru.

1.3 Mechanismy rozpoznávající stisk a návrat klávesy

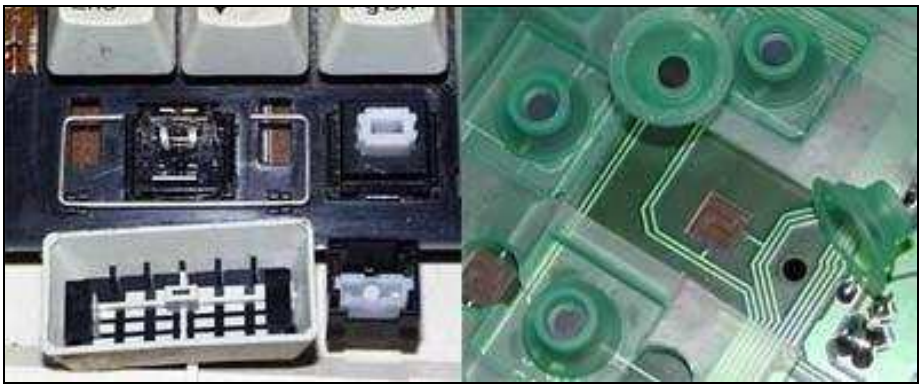
Existují dva základní postupy, díky nimž elektronika klávesnice rozezná, zda byla stisknuta klávesa. První je kontaktní (mechanický) a druhý bezkontaktní (kapacitní).

[3] http://vstupnizarizeni.rames.info/1keyb.html

1.3.1 **Mechanické rozpoznávání stisku klávesy**

V klávesnicích jsou nainstalované obyčejné mechanické nebo membránové spínače. Když uživatel stiskne klávesu, následuje sepnutí spínače a tím uzavření elektrického obvodu. Při povolení stisku klávesy se obvod rozpojí.

Obyčejný mechanický spínač se sepne ve chvíli, kdy dojde ke stysku klávesy. Kdežto membránová klávesnice má pod klávesami tři spojené fólie, kde první a třetí fólie mají na sobě vodivé cesty, které odděluje druhá fólie, ve které jsou díry. Tyto díry slouží k tomu, aby stisknutá klávesa ve chvíli, kdy se dotkne první fólie, se spojila s fólií třetí a uzavřela elektrický obvod.



Obrázek 3 Mechanický a membránový spínač

1.3.2 **Klávesnice s kapacitní vazbou**

U tohoto typu klávesnice dochází pod klávesou k měření kapacity na zvláštní citlivé vrstvě kovu, která tvoří kondenzátor. Ve chvíli, kdy se klávesa přiblíží k vrstvě kovu, přemění se kapacita tohoto prvku. Tato reakce je pro elektroniku signálem toho, že došlo ke stisku klávesy. Klávesnice s kapacitní vazbou se mnoho nepoužívají, protože jsou drahé. Ovšem jejich kladem je vysoká životnost. Je to dáno především minimálním obsahem mechanických prvků, kterými jsou vlastně pouze samy klávesy.

1.4 Bezpečnost zadávaných dat na klávesnici

„Podle výsledků výzkumu uveřejněných v říjnu 2008 pracovníky švýcarské vysoké školy EPFL v Lausanne představují klávesnice slabé místo z hlediska bezpečnosti zadávaných údajů. Signály o tom, které klávesy byly stisknuty, lze totiž v naprosté většině případů

zachytit s použitím antény a potřebného technického zařízení na vzdálenost až 20 metrů, a to i tehdy, pokud mezi klávesnicí a odposlouchávacím zařízením stojí překážka, např. zeď.“[4]

Tímto tématem se budu podrobněji zabývat v kapitole o kompromitujícím vyzařování, které je právě důsledkem malé bezpečnosti při používání klávesnic.

[4] http://cs.wikipedia.org/wiki/Počítačová_klávesnice...

2 SOFTWAROVÝ KEYLOGGING

Softwarový keylogging je odposlouchávání pomocí softwaru neboli programu, který je umístěn v počítači, ze kterého hodláme odposlouchávat, a který je nainstalovaný způsobem, aby nebyl při běžném používání počítače odhalitelný. Je to program sloužící ke vniknutí nebo poškození počítačového systému. Takový program je malwarem, což je souhrnný název pro počítačové viry, trojské koně, spyware a adware. Slovo malware vzniklo složením anglických slov „malicious“ (zákeřný) a „software“ a popisuje záměr autora takového programu spíše než jeho specifické vlastnosti. Výhodou SW keyloggerů (které jsou jedním z druhů nebezpečného spyware) je pak zejména to, že umožňují sledování více faktorů, nikoliv pouze stisknutých kláves - například zaznamenávají a ukládají aktuální stav obrazovky, pohyb a kliknutí myší, navštěvované webové stránky apod. Výsledky odposlechu pak v případě připojení počítače k internetu přes něj posílají předem určeným způsobem na dané místo. Úspěšnost, nenápadnost a zejména náročnost odposlechu do jisté míry závisí na místě umístění takového softwaru. Podle umístění dělíme tuto kategorii na pět skupin.[5]

1) Na základě hypervisoru
2) Na základě Kernelu
3) Na základě „zachycení se“
4) Pasivní metody
5) Způsob sledování webových formulářů

2.1 Rozdělení softwarového keyloggingu

2.1.1 **Na základě Hypervisoru**

Keylogger se může teoreticky usadit v malwarovém hypervisoru běžícím na nižší úrovni než operační systém, který zůstane nedotčen. Pak se skutečně stává virtuálním strojem. Takovým nástrojem je například Blue Pill.

[5] http://en.wikipedia.org/wiki/Keystroke_logging

Hypervisor je software umožňující virtualizaci přístupu k hardwaru počítače, čímž umožní běh více operačních systémů na jednom počítači. Rozlišujeme dva typy hypervizorů a to nativní a hostované.[6]

Nativní hypervizor je nástroj běžící přímo na hardwaru a plní jakéhosi prostředníka mezi hardwarem a virtualizovaným operačním systémem. Virtualizovaný operační systém běží nad nativním hypervisorem, kterému předává všechny svoje volání hardwaru například požadavky na paměť či procesor. Mezi takové hypervisory patří XEN,Hyper-V a další. Tyto hypervisory pohánějí cloud computing, což je sdílení hardwarových i softwarových prostředků pomocí sítě.

Takzvaný hostovaný hypervisor funguje pod standardním operačním systémem a chová se jako proces, při kterém je spuštěn virtualizovaný operační systém. Pro tento druh virtualizace stačí nainstalovat hypervisor. Například VMWare, QEMU, Microsoft Virtual PC, Microsoft Virtual Server, VirtualBox, Parallels Workstation nebo Parallels Desktop.

2.1.2 **Na základě Kernelu**

Tato metoda je obtížná jak na použití, tak na boj proti ní. Keylogger se usadí na kernelové úrovni, a je tedy obtížné jej zjistit, zejména v uživatelské verzi aplikace.

Kernel je jádro operačního systému. Jádro je zavedeno do operační paměti při startu (bootování) počítače a je mu předáno řízení. U pokročilých operačních systémů jádro nikdy neztrácí kontrolu nad počítačem a po celou dobu jeho běhu koordinuje činnost ostatních běžících procesů.[7]

Keylogger často tvoří koordinovaný soubor programů určených k získání kontroly nad počítačovým systémem nebo sítí počítačových systémů, tzv. rootkit. Ten rozvrátí jádro operačního systému, a získá neoprávněný přístup k hardwaru. V tom je jeho síla. Keylogger pomocí této metody může fungovat například, jako ovladač klávesnice, čímž

---

[6] http://en.wikipedia.org/wiki/Hypervisor

[7] http://cs.wikipedia.org/wiki/Kernel

získá přístup ke všem informacím zadaným na klávesnici, a tak se dostane do operačního systému.

2.1.3 **Na základě „zachycení se“**

Takový keylogger pomocí standardních funkcí operačního systému zachytává všechny události z klávesnice. K tomu jsou využívány tzv. hook funkce API operačního systému. Operační systém oznámí keyloggeru pokaždé, když je zmáčknuta klávesa a keylogger si ji jednoduše zaznamená.

2.1.4 **Pasivní metody**

Keylogger využívá API (Application Programming Interface) funkcí operačního systému (v MS Windows např. GetAsyncKeyState, GetForegroundWindow) a neustále zjišťuje aktuální stav klávesnice. Tato metoda je jednoduchá na naprogramování, ovšem nevýhodou je, že pokud je požadováno zaznamenání stisku každé klávesy, může dojít k nápadnému zvýšení využití procesoru a k propásnutí nahodilého stisku klávesy.

2.1.5 **Způsob sledování webových formulářů:**

Keylogger se připojí jako doplněk k webovému prohlížeči a čeká na odeslání dat z webového formuláře pomocí události – onSubmit (skriptování). Data formuláře si keylogger uloží, ještě než jsou předána přes internet, a tak obejde i http šifrování.

2.2 Možnosti softwarového keyloggingu

2.2.1 **Vzdálený přístup**

Jednou z dalších možností softwaru pro keylogging je rozšíření o možnost vzdáleného přístupu. Dotyčná osoba nemusí být v bezprostředním dosahu sledovaného zařízení, přesto může získávat data v reálném čase na větší či menší vzdálenost podle zvoleného způsobu předání informací.

Získaná data lze odeslat na webovou stránku, uložit do databáze nebo na FTP účet. Další, vzdáleností neomezenou možností, je odesílání informací na předem určenou emailovou adresu. Pokud jsou data ukládána přímo na sledovaném počítači lze využít software, který umožní přihlásit se do místního počítače přes intranet nebo internet a vstoupit do protokolů zde uložených. Čtvrtou možností, tentokrát s omezenou vzdáleností přístupu k datům, je

jejich přenos pomocí bezdrátových prostředků připojených k hardwarovému systému, který je odposloucháván.

2.2.2 **Záznam bez stisku kláves**

Nejen záznam stisku klávesy může být zdrojem citlivých dat. Pro získání informací lze využít například tzv. schránky. Cokoliv bylo zaznamenáno do schránky lze odposlechnout.

Další možností je snímání obrazovky neboli screenshot. Slouží k zachycení grafických informací. Lze je zaznamenávat pravidelně v určitých časových úsecích nezávisle na chování uživatele nebo naopak jako reakci na jeho chování a to například při kliknutí myší. Tímto způsobem lze překonat on-line klávesnice používané některými bankami.

Text zachycený při kontrole. Microsoft Windows API umožňuje programům požadovat kontrolu hodnoty textu. Díky tomu mohou být odposlechnuta některá hesla, i když jsou skryta za maskovací znaky, kterými jsou obvykle hvězdičky.

2.3 Monitorovací systémy

Monitorovací systémy jsou určeny k detailnímu pozorování všech činností uživatele PC a k jeho vzdálené obsluze. Takový program nabízí obrovské množství možností. Kvůli tomu je poměrně velký a v počítači by byl těžko přehlédnutelný. Právě proto není běžně viditelný a svá data si šifruje. S tím je spojená i jeho obtížná nenápadná instalace. Problém s instalací řeší sám monitorovací systém, který umožňuje vytvoření instalátoru maskovaného za jiný program nebo možnost tzv. bezdotykové či tiché instalace. Další variantou je možnost spuštění bez instalace pomocí login skriptu. Odposlech stisknutých kláves je jen jednou z možností jeho použití. V kombinaci s jeho dalšími funkcemi se takový program může stát velmi účinným a nebezpečným nástrojem.

Vzdálené operace lze provádět se souhlasem uživatele nebo bez jeho vědomí. Podobné programy se používají zejména ve firmách k provádění analýz o vytíženosti a aktivitě zaměstnanců. Připojení vzdáleného počítače je realizováno pomocí lokální sítě nebo FTP serveru. V druhém případě je možné připojení se k počítači z jakéhokoliv bodu internetové sítě. Další možností je zasílání získaných dat v určitém čase a dni v týdnu pomocí emailu. Získaná data jsou vložena do přílohy, kterou je možné prohlížet pouze v softwaru daného monitorovacího systému.

Přehled základních funkcí vztahujících se k monitoringu PC:

Sledované události:

- provoz počítače, vč. sledování nesprávného ukončení Windows

- spuštěné a ukončené programy

- zobrazená a zavřená okna

- přepnutí na program

- otevřené dokumenty

- monitoring tiskových úloh

- spuštění, ukončení, přechod do režimu spánku a probuzení Windows

- vložení textu do schránky

- vložení a vyjmutí jakéhokoli disku, vč. detailních informací s možností získání výpisu obsahu disku

- nastavitelný monitoring souborového systému (změny v souborech a adresářích na vybraném disku) včetně možnosti zadání nesledovaných souborů a adresářů

- navštívené WWW stránky definovaných internetových prohlížečů a dalších programů

- stisknuté klávesy včetně hesel

- události myši

- instalovaný a odinstalovaný software

- vytížení procesoru

- využití paměti

- další neomezené možnosti sledování (např. chatování) při použití reakcí na události

Reakce na události

Další možnosti monitorovacích systémů jsou v reakcích na dané události. Na většinu výše zmíněných událostí lze nastavit konkrétní reakci. Tou může být například získání otisku obrazovky, záznam zvuku pomocí mikrofonu, spuštění definovaného programu a podobně. U všech takových událostí lze nastavit další podrobnosti jako je přidání data a času, zápis polohy kurzoru a jiné. Všechny tyto funkce se nemusí vázat na předdefinovaný úkon

uživatele, ale mohou být také spouštěny ve zvolený čas nebo po uplynutí daného časového úseku.

Zdálo by se, že tak obsáhlý program musí mít vysoké nároky na hardwarové vybavení počítače. Už při samotném vývoji programu je však kladen důraz právě na minimalizaci zatížení počítače. Hodnota zatížení procesoru se pohybuje v rozmezí 2-20 MHz, tj. 0.1-1% vytížení na 2 GHz procesoru. Nároky na operační paměť jsou 3-10 MB.[8]

[8] http://www.dozorce.cz

3 HARDWAROVÝ KEYLOGGING

Všechny předchozí metody vyžadovaly oprávněný či neoprávněný přístup do odposlouchávaného zařízení a jistý zásah do jeho programového vybavení. Hardwarové odposlouchávání má dvě možnosti přístupu k datům. První možností je připojit nějaké zařízení přímo k počítači. Výhodou použití HW keyloggeru je jeho nezávislost na operačním systému, nevýhodou však nutnost jeho fyzické instalace, snadná odhalitelnost, a možnost snadno jej obejít za pomocí softwarové klávesnice. Druhou možností je bezkontaktní odposlech. To však vyžaduje prostor, řekněme místnost více či méně vzdálenou od odposlouchávaného zařízení, ve které budeme mít možnost instalovat a obsluhovat odposlouchávací zařízení. Tato metoda také klade mnohem vyšší požadavky na znalosti a schopnosti keyloggera.

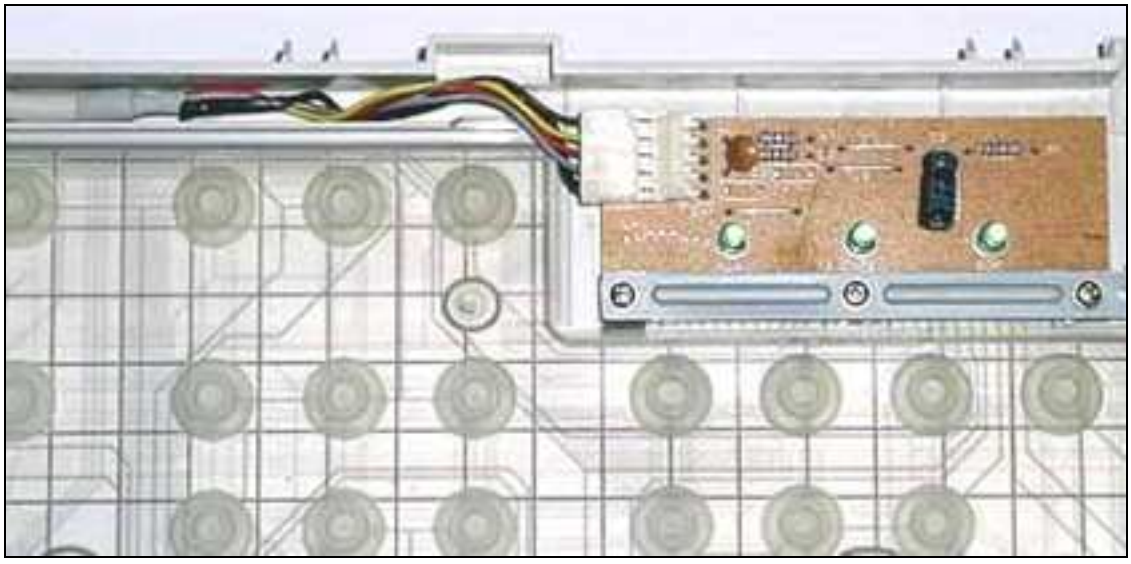
3.1 Vložení hardwarové součástky

Odposlech lze realizovat například pomocí zařízení vloženého mezi klávesnici a počítač. Zařízení vypadá jako drobná redukce mezi konektory. Dokáže do své interní paměti zaznamenávat veškeré stisky kláves. Kapacita dnes vyráběných zařízení je zhruba sedmdesát pět stran A4 psaného textu. Jistým nebezpečím je možnost vizuálního odhalení zařízení. Podobné zařízení se však dá kamuflovat přímo do klávesnice. Takové provedení je prakticky neodhalitelné, ale vyžaduje složitější přípravu. Zařízení se ovládá pomocí textového editoru. Lze jím odhalit například hesla do Windows, BIOSu a jiná hesla zadávaná před spuštěním operačního systému. Pořizovací náklady na takové zařízení se pohybují kolem tří tisíc korun.

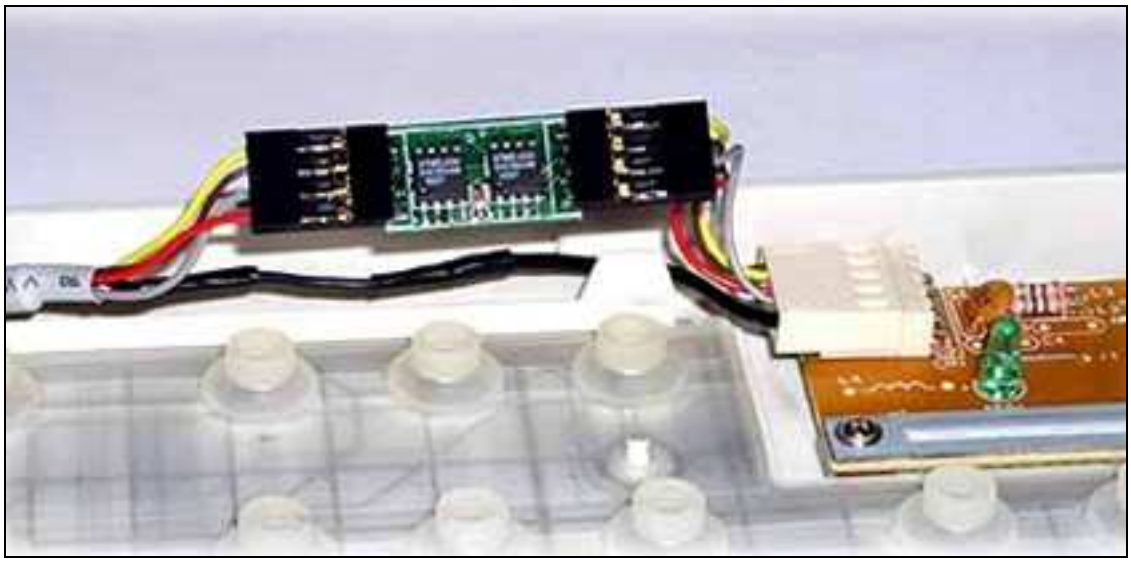
Obrázek 4 Keylogger určený k vložení do PS/2, USB

Jiná verze stejného zařízení svou stavbou a velikostí umožňuje instalaci přímo uvnitř těla klávesnice. Postup instalace je velmi jednoduchý a zvládne ho i amatér. Výsledek je vidět na obrázcích 6 a 7. V případě použití této verze odpadá riziko odhalení zařízení, které je zapojeno mezi klávesnici a PC, protože běžný uživatel nemá šanci poznat na klávesnici, že byla jakkoliv upravena.

Obrázek 5 Modul keyloggeru



Obrázek 6 Klávesnice před vložením modulu



Obrázek 7 Klávesnice s instalovaným modulem

Další možností využívanou zejména u klávesnic bankomatů jsou takzvané překryvné klávesnice. Jde o zařízení, které vypadá jako pravá součást bankomatu. Zákazník si ho ani nevšimne, protože je zdánlivě integrován přímo ve stroji. Při zadávání PINu nejsou však stisknuty jen klávesy pravé, ale také nastražené. Ty pak zadaný PIN zaznamenají či odešlou na další zařízení.

Heslo lze nejen odposlechnout, ale i odkoukat. A to doslova. K takovému odposlechu se použije vhodně strategicky umístěná kamera, které vidí na klávesnici a ruce zákazníka bankomatu. Takto získaný PIN neb heslo je v kombinaci s následným ukradením karty volnou cestou k účtu neopatrného zákazníka. Tato metoda se však netýká pouze bankomatů. Stejně se dá využít například nevinně vyhlížející webkamera.

3.2 Využití elektromagnetického záření

Slovní spojení kompromitující elektromagnetické vyzařování je doslovným překladem anglického „compromising electromagnetic emanations“. Je to poměrně výstižný, leč poměrně krkolomný výraz, který se úspěšně usadil v českém jazyce. Je to záření, které je druhotným efektem přenosu dat po kabelu nebo bezdrátovým přenosem. Toto záření není vytvářeno úmyslně a jeho zachycením a příslušným dekódováním je možné získat data, která jsou velmi citlivá a měla by být dobře chráněna. Takovými daty mohou být přístupová hesla do počítače, internetového bankovnictví nebo informace tvořící firemní knowhow.

Praktický výzkum možností odposlechu elektromagnetického vyzařování klávesnic pomocí antény a dalšího vybavení provedli Martin Vuagnoux a Sylvain Pasini. Prezentovali jej na konferenci/symposiu USENIX Security ´09 v Montrealu.

3.2.1 **Metody zachytávání elektromagnetického záření**

3.2.1.1 ***Standardní metody***

Standardní metoda využívá spektrálního analyzéru k detekci přenosu signálu. Ten lze využít pouze, je-li doba přenosu dostatečně dlouhá a proto je s jeho pomocí těžko odhalitelný přenos kompromitujícího signálu složený pouze ze signálů, které mají tvar špiček.

Druhá standardní metoda je založena na širokopásmovém přijímači naladěném na určitou frekvenci. Proces detekce signálu spočívá v testování signálu v celém frekvenčním rozsahu přijímače a demodulaci signálu v závislosti na jeho frekvenční nebo amplitudové modulaci. Když je objevena frekvence, která nás zajímá, tak se pomocí úzkopásmové antény a příslušných filtrů oddělí signál o hodnotách kompromitujícího elektromagnetického signálu. V praxi se používají širokopásmové přijímače R-1250 a R-1550. Tato zařízení odpovídají normě NACSIM-5000 známé také jako TEMPEST. Proto jsou velmi drahá a nedostupná. Je však možné použít zařízení levnější a volně dostupná. Jsou to zařízení založená na platformě USRP (Universal Software Radio Peripheral) a GNU Radio project. USRP je hardwarové zařízení, které umožňuje vytvořit softwarové rádio pomocí počítače s USB portem. S různými daughterboardy je schopno skenovat signály od stejnosměrného napětí až po frekvenci 2.9 GHz se vzorkovací frekvencí 64 MS/s při rozlišení převodníku 12 bitů. GNU Radio project je výkonná softwarová knihovna používaná USPR zařízením pro zpracování různých modulací (AM, FM, PSK, FSK, atd.) a analýzu signálů pomocí optimalizovaných filtrů, FFT a jiných dalších. Spojení USPR a GNU Radio project může fungovat jako širokopásmový přijímač a spektrální analyzér.

3.2.1.2 Nestandardní metoda

Některé přímé a nepřímé vyzařování může zůstat u standardních metod skryto. Především je-li signál složen z nepravidelných špiček nebo proměnných nosných frekvencí. Spektrální analyzéry potřebují především neměnnou nosnou frekvenci. Podobně příjem

širokopásmových přijímačů není okamžitý a potřebuje dost času na pokrytí celého frekvenčního rozsahu. Navíc demodulační proces může část elektromagnetického vyzařování skrýt.

Proto byla navržena třetí metoda k zachycení záření z klávesnic. Nejprve je získán surový signál přímo z antény namísto filtrování a demodulace signálu s omezenou šířkou pásma. Potom je vypočítána krátkodobá Fourierova transformace, která dává trojrozměrný signál s časem, frekvencí a amplitudou. Moderní analogově digitální převodníky poskytují velmi vysoké vzorkovací frekvence. Připojením převaděče přímo do širokopásmové antény je možné přenést surový vzorek signálu do počítače a použít softwarového radia k okamžitému upozornění na potencionální kompromitující vyzařování. Výpočet krátkodobé Fourierovy transformace odhalí nosné frekvence a špičky, i když jsou jen krátkodobé. Bohužel pro přenos velkého objemu dat do počítače v reálném čase v současné době neexistuje žádné řešení. Objem dat je pro rozhraní USB 2.0, IEEE 1394, Ethernet nebo SATA příliš velký. Nicméně s některými inteligentními spouštěmi (trigger) je možné vzorkovat malou zajímavou část signálu a uložit ji v rychlopřístupové paměti. Osciloskopy poskytují spouštěné AD převodníky s rychlou pamětí. Použit byl Tektronix TDS5104 s 1Mpt pamětí a vzorkovací frekvencí 5 GS/s. Je schopen zaznamenat elektromagnetické záření až do 2.5 GHz (podle Nyquistova teorému). Kromě toho, má tento osciloskop vyhlazovací filtry a podporuje IEEE 488 GPIB komunikaci. Byl vyvinut nástroj na definici některých specifických spouští (v podstatě detektor špiček) a k exportu získaných dat do počítače přes ethernet rozhraní pod GNU/Linux. Pak může být signál zpracován pomocí softwarového rádia a některých dalších mocných nástrojů jako je Baudline. Výhodou této metody je zpracování surového signálu, který je vzorkován přímo anténou bez jakékoliv demodulace. Navíc jsou zachycena všechna kompromitující elektromagnetická vlnění do frekvence 2,5 GHz. Díky této technice je možné upozornit na všechna kompromitující vlnění rychleji a snadněji. Toto řešení je vhodné pro počítačové klávesnice používající velmi krátké datové přenosy.

3.2.2 **Odposlech klávesnice – popis experimentu**

Tato podkapitola obsahuje stručný popis odposlechu klávesnice pomocí kompromitujícího elektromagnetického záření. Detailní popis experimentu lze nalézt v práci autorů MartinaVuagnoux a Sylvaina Pasini nazvané „Compromising Electromagnetic Emanations of Wired andWireless Keyboards“[9]

3.2.2.1 Experimentální nastavení

3.2.2.1.1 Prostředí

Účelem experimentu bylo dokázat existenci kompromitujícího elektromagnetického záření počítačových klávesnic při stisknutí klávesy. Samozřejmě elektromagnetické vlnění je závislé na prostředí. Proto byla zvolena čtyři různá prostředí

1. Polo-zvukotěsná komora.

Byla použita profesionální polo-zvukotěsná komora o rozměrech 7x7 m. Cílem nebylo odrušit ozvěnu ale odstínit vnější elektromagnetické znečištění. Anténa byla umístěna pět metrů od klávesnice zapojené do počítače. Testovaná klávesnice byla na stole metr vysokém a počítač byl na zemi.

2. Kancelář

Kvůli důkazu proveditelnosti útoku s šumem v pozadí, bylo měřeno kompromitující záření klávesnice v malé kanceláři o rozměrech 3x5 metrů se dvěma napájenými počítači a třemi LCD displeji. Elektromagnetický šum v pozadí tvořilo 40 počítačů vzdálených 10 m od kanceláře, více než 60 počítačů na patře a 802.11 wifi router minimálně 3 m od kanceláře. Anténa byla posouvána zpět skrz otevřené dveře až do desetimetrové vzdálenosti od klávesnice, s cílem určit maximální vzdálenost.

3. Přilehlá kancelář

[9] http://lasecwww.epfl.ch/keyboard/

Toto nastavení podmínek bylo podobné předchozímu v kanceláři, ale elektromagnetické vlnění bylo měřeno ze sousední kanceláře přes 15 cm širokou zeď ze dřeva a sádrokartonu.

4. Budova

Ve čtvrtém případě byl použit byt, který se nacházel v budově s pěti podlažími v centru středně velkého města. Klávesnice byla v pátém patře. První měření proběhlo s anténou umístěnou na stejném patře, poté byla přesunuta do nejvzdálenějšího přízemí minimálně 20 m od klávesnice

3.2.2.1.2 Zařízení

Anténa

Vzhledem k tomu, že kompromitující elektromagnetické záření se pohybuje mezi 25 MHz a 300 MHz, byla použita dvoukuželová anténa, aby se zlepšil poměr signálu šumu. Také bylo ozkoušeno, zda je možné záření zachytit menší anténou jako například smyčkou z 1m dlouhého měděného drátu.

Klávesnice

Bylo testováno 12 různých modelů klávesnic nacházejících se momentálně v laboratoři. 7 kusů klávesnic s PS/2 připojením, 2 klávesnice s USB připojením, dvě notebookové klávesnice a jedna bezdrátová klávesnice. Všechny byly zakoupeny mezi lety 2001 a 2008. Byly naměřeny také hodnoty u klávesnic připojených k notebooku, který byl napájen z baterie. Dělo se tak, aby se vyloučila vodivá spojení přes napájecí kabel.

3.2.2.2 Metody

Za účelem zjištění kompromitujícího vyzařování, byla klávesnice umístěna v polo-zvukotěsné komoře a k odposlechu byla použita dvoukuželová anténa. Pomocí osciloskopu byl získán surový signál, jak je vysvětleno výše. Vzhledem k tomu, že paměť osciloskopu je omezená, bylo třeba přesně spustit datový výběr. Za prvé byly použity nejbližší sestupné hrany signálů dat vyslaných při stisku klávesy. Sonda byla připojena k datovému vodiči mezi klávesnicí a počítačem. S pouhým jedním zachycením je možné reprezentovat celé spektrum po celou dobu zachytávání. Kromě toho byl k dispozici vizuální popis všech elektromagnetických vyzařování. Zejména byly známy některé nosné (vertikální linky) a

širokopásmové impulzy (horizontální linie). První tři metody jsou založeny na těchto kompromitujících vyzařováních a jsou podrobně popsány v následujících oddílech. Úkolem bylo využít elektromagnetické spouště, protože za normálních okolností nemají přístup k údajům na lince. Objevené širokopásmové impulzy horizontální čáry mohou být použity jako spouště. Tudíž jen s anténou je možné vyvolat získání ohrožujícího elektromagnetického vyzařování. Podrobnější informace jsou uvedeny níže. Některé klávesnice nevysílají elektromagnetické vyzařování, když je klávesa stisknuta. Ale s různými modely spouští, založenými na detektoru špičky, byl objeven další druh emisí, neustále generovaných (i když nestisknete žádnou klávesu). Tato poslední technika je podrobně popsána v oddílu „Technika skenování matice“.

3.2.2.2.1 Technika sestupné hrany signálu

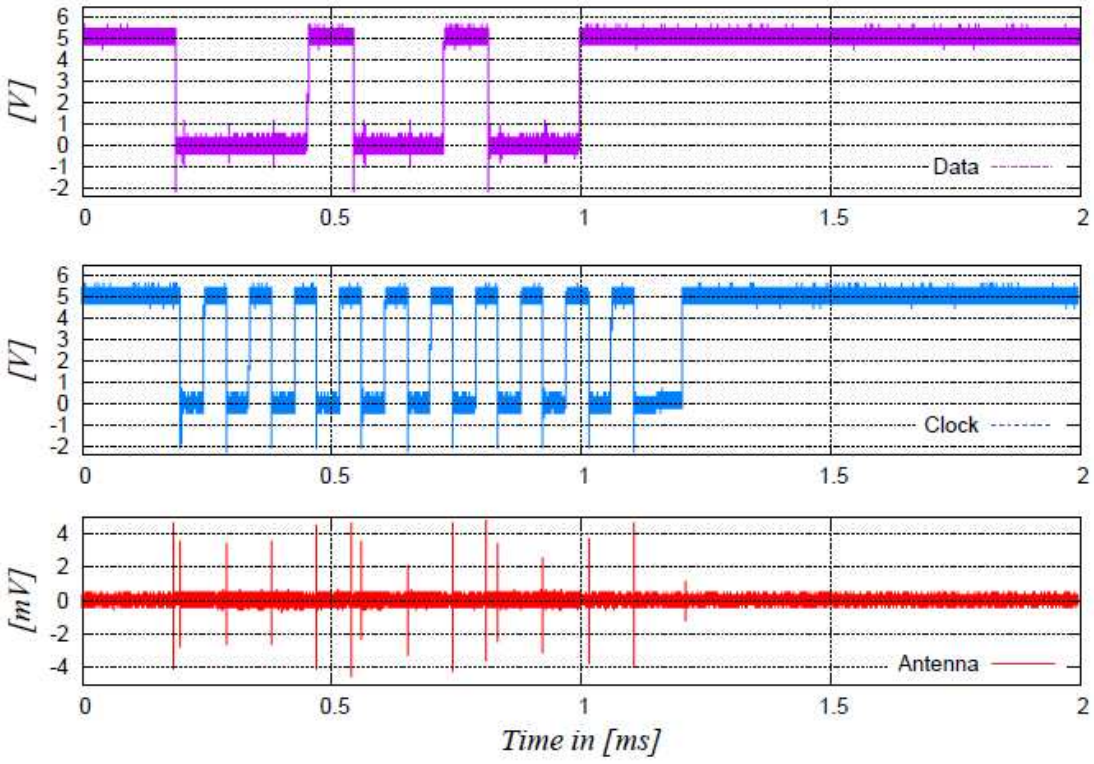
Na začátek je potřebné se zmínit o protokolu a sběrnici PS/2. Sběrnice je starší více než dvacet let a v současné době se používá pouze pro připojení vstupních periferií PC tedy klávesnice a myši. PS/2 je zkratkou anglického Personal System/2. Je to nízkorychlostní sériové rozhraní umožňující obousměrnou komunikaci řízenou tzv. master (nadřazeným) zařízením s jedním (slave) podřízeným zařízením připojeným ke sběrnici. Spolu s dvěma kontakty napájení VCC (5 V), GND je rozhraní tvořeno dalšími dvěma kontakty pro přenos datového signálu.

Prvním z nich je CLK (clock) - hodinový signál, který určuje okamžik vzorkování dat. Jeho kmitočet se pohybuje mezi 10 kHz a 16,7 kHz. Hodiny generuje vždy podřízené zařízení. Nadřízené zařízení pomocí signálu CLK přerušuje, povoluje nebo zakazuje přenos dat. Slave může zahájit přenos jednoho bytu, pokud jsou obě linky (CLK i DATA) v úrovni high po dobu nejméně 50 μs.

Datový rámec se skládá z jedenácti bitů. Přenos je zahájen start bitem s úrovní low, následuje 8 bitů dat řazených od nejméně významného, dále je zde paritní bit (lichá parita - high pro sudý počet jedniček v datech a konečně stop bit s úrovní high.[10]

[10] http://elektronika.kvalitne.cz/ATMEL/necoteorie/tutorial/PS2/PS2_mouse.html

Při stisku tlačítka E na americké klávesnici, které odpovídá na klávesnici pozici 0x24 je počítačem přijat signál 0 00100100 1 1 graficky zobrazený na obrázku 9. Ne vždy však musí dané pozici odpovídat klávesa E, jak již bylo dříve zmíněno v kapitole o klávesnici.



Obrázek 8 Datový, hodinový a kompromitující signál při stisku klávesy 0x24

Tato metoda je založena na rozpoznání sestupných hran signálu trvajících 200 ns na rozdíl od náběžných hran, které trvají 2 µs. Proto by mělo být kompromitující vyzařování mnohem silnější s vyšší maximální frekvencí právě na sestupné hraně. Jelikož jsou signály hodin i dat generovány společně, je i kompromitující záření jejich kombinací. Porovnáním grafu datového signálu a kompromitujícího záření bylo však zjištěno, že vrcholy zachycené anténou nemusí generovat sestupné hrany datového a hodinového signálu, ale jsou pravděpodobně vytvářeny při sepnutí tranzistoru. Nicméně zachycené vrcholy popisují stav datového signálu a mohou být zneužity. Mohou se však objevit i kolize znaků. Pokud vezmeme v úvahu jen sestupné hrany signálu, mají například znak E (0x24) a G (0x34) stejnou stopu. V případě slova „password“ je výsledkem všech možných kombinací záměn znaků 7776 slov. Pokud jsou v úvahu brány jen alfanumerické klávesy, je počet kombinací několikanásobně snížen. Dalšího snížení je možné dosáhnout filtrací pouze slov ve slovníku předpokládaného jazyka.

3.2.2.2.2 Technika zobecněného přenosu

Výše popsaný způsob odposlechu je limitován částečným obnovením stisků kláves, což je významné omezení. Jestliže je známo, že mezi dvěma stopami je jedna vzestupná hrana datového signálu a je možné ji zachytit, pak je také možné stisky kláves plně obnovit.

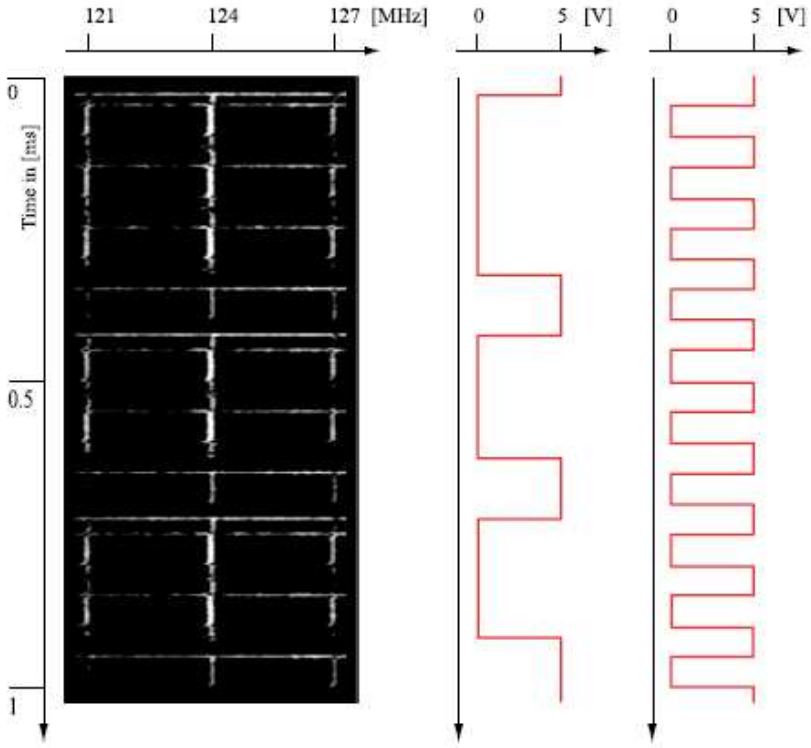
Pro zvýraznění kompromitujícího vyzařování na vzestupné hraně datového přenosu lze použít softwarovou pásmovou propusť, která izoluje frekvence širokopásmových impulsů. Filtrační proces také výrazně zlepšuje odstup signálu od šumu (SNR), čímž se zvyšuje také efektivita algoritmu detekce vrcholů. Je známo, že hodinové vrcholky mají více energie, když stav datového signálu nabývá hodnoty *high.* Potom vrcholy vytvářené sestupnou hranou hodinového signálu skutečně kódují logický stav datového signálu, protože mezi dvěma sestupnými okraji stopy je pouze jeden vzestupný okraj.

Jednoduše považujeme nejvyšší vrchol hodin za vzestupnou hranu datového přenosu. Například na obrázku 9, na vzestupnou hranu datového přenosu přísluší hodinové špičky 5 a 9.

3.2.2.2.3 Modulační technika

Některé elektromagnetické emise pocházejí z neúmyslného vyzařování emitovaného hodinami, nelineárními prvky, pozemním znečištění, atd. Určení teoretických důvodů těchto kompromitujících záření je velmi složitý úkol. Proto je možné pouze načrtnout některé pravděpodobné příčiny. Původ těchto harmonických odpovídá nosné frekvenci přibližně 4 MHz, což jsou velmi pravděpodobně vnitřní hodiny mikrokontroléru klávesnice. Zajímavé je, že pokud byly tyto harmonické srovnány jak s hodinovými tak datovými signály, jasně byly vidět modulované signály (v amplitudě a frekvenci), které plně popisují stav hodinového i datového signálů, viz Obrázek 9. To znamená, že scan kód může být kompletně získán z harmonických. Stojí za povšimnutí, že i když se objeví některá silná elektromagnetická rušení, může útočník využít harmonických frekvencí, které nejsou ovlivněny interferencí, aby získal jasný signál. Ve srovnání s předchozími technikami, modulace založená na nosných frekvencích se stává mnohem zajímavější pro vzdálený příjem. AM a FM přenosy jsou obecně méně rušeny šumem a překážkami, jako jsou stěny, podlahy, atd. Kromě toho je tato technika schopna plně zotavit úhozy. Tato nepřímá vyzařování, která nemají formální vysvětlení a jsou pravděpodobně založena na

přeslechu se zemí, vnitřních hodinách mikroprocesoru, datových a hodinových signálech, nechají útočníka obnovit úhozy na klávesnici.



Obrázek 9 Amplituda a frekvence modulace harmonické frekvence 124 MHz

Tento experiment ukazuje, že levná zařízení jako klávesnice může vyzařovat nepřímé vyzařování, které je mnohem nebezpečnější než přímé vyzařováním. I v případě kdy je SNR menší, použití frekvenční modulace významně zlepšuje rozsah odposlechu. Kromě toho se útočník může vyhnout nějakému zašuměnému frekvenčnímu pásmu výběrem pouze nejsilnější harmonické. Nepřímé vyzařování kompletně popisuje, jak hodinový, tak datový signál.

Funkce extrakce je založena na demodulaci zachyceného signálu zaměřeného na nejsilnější harmonické. V daném případě odpovídá 124 MHz. Bylo použito rádio knihovny k demodulaci signálu. Je však třeba použít spoušťový model založený na detekci vrcholu, protože paměť osciloskopu je omezená. Další možností je přímo zachytit signál s USRP. Nižší, ale kontinuální vzorkování USRP je dostačující k obnově úhozů. Bohužel, citlivost USRP je slabší než osciloskopu a dosah odposlechu je omezen na méně než 2 metry v polo-zvukotěsné komoře.

3.2.2.2.4 Technika skenování matice

Techniky popsané výše jsou vázány na použití PS/2 a některé laptopové klávesnice. Nicméně, nové klávesnice inklinují k použití USB nebo bezdrátového připojení. V tomto oddílu, jsou představena další kompromitující záření, která se týkají všech typů klávesnic. PS/2, USB, klávesnice notebooků a dokonce i bezdrátové klávesnice. Téměř všechny klávesy sdílejí stejný způsob detekce stisknutí. Hlavní technické omezení je, aby byla klávesa považována za stisknutou, je-li stlačena na dobu 10 ms. Během této doby by měl být zjištěn každý stisk. Z pohledu výrobce, je dalším hlavním omezením náklady na přístroj. Naivní řešení pro detekci stisku klávesy je zachytit každou klávesu v řadě. Toto řešení zjevně není optimální, protože vyžaduje velkou skenovací rutinu a také větší zpoždění. Kromě toho jeden okruh pro každou klávesu zvyšuje náklady na zařízení.

Chytré řešení je uspořádat klávesy do matice. Klávesnicový kontrolér, často 8-bit procesor, analyzuje sloupce jeden po druhém a získává stav osmi tlačítek najednou. Proces skenování matice lze popsat jako 192 kláves uspořádaných v 24 sloupcích a 8 řádcích. Sloupce jsou spojeny s řídícím čipem, zatímco řádky jsou připojeny k detekčnímu čipu. Klávesy jsou umístěny v průsečíku sloupců a řádků. Každý klíč je analogový přepínač mezi sloupci a řádky. Matice vytvořená stiskem klávesy je přenášena do počítače. K tomu využívá klávesnice podprogram a ten vyžaduje určitý čas. Sloupce v matici vytvářejí dlouhé vedení, protože spojují zpravidla osm tlačítek. Díky tomu trvá přenos alespoň 3μs a vytváří elektromagnetické záření. Pokud toto záření je útočník schopen zachytit, může snadno obnovit sloupce stisknutých kláves. Ve skutečnosti budou tyto impulzy zpožděné.

Pro částečné obnovení úhozů, je třeba průběžně sledovat kompromitující elektromagnetické vyzařování způsobené rutinou skenovací matice konkrétním spoušťovým modelem. Šest prvních špiček je vždy přítomno stejně jako poslední tři. Nikdy nechybí ani se nezpožďují. Proto se tato pevná struktura používá k definici spoušťového modelu. Kromě toho čtení matice nepřetržitě vyzařuje kompromitující záření od stisku klávesy. Když je zjištěna podmnožina úhozu, získává se více příkladů až do zjištění dalšího vzoru. Proto je vybírán nejčastěji zachycený vzor.

Tato metoda je vzhledem k zaměnitelnosti hledem k zaměnitelnosti znaků o něco méně účinná než metoda první.

3.2.2.3 Zhodnocení výsledků

I když byly ukázány techniky, kterými je možné získávat informace z vyzařování klávesnice, není prozkoumané, jak jsou ovlivněny různými prostředími. Tato část se zabývá zkoumáním přesnosti přístupů ve všech popsaných prostředích. Analýza ukazuje, že vyzařování z klávesnice je v praktickém scénáři skutečně problematické. Vyhodnocení rizik způsobených elektromagnetickým zářením není snadné. Ve skutečnosti výsledky velmi závisí na anténě, modelu spouště, pásmové propusti, detekci špiček, atd.

Kromě toho byly použity triviální filtrační procesy a základní techniky zpracování signálu. Tyto metody by mohly být výrazně zlepšeny pomocí tvarování paprsku, lepší anténou, lepšími filtry a komplexními spouštěmi. Kromě toho měření v reálném prostředí, až na polo-zvukotěsné komory, byla výrazně ovlivněna elektromagnetickým rušením. Tabulka 1 ukazuje seznam ohrožených klávesnic ve všech nastaveních, podle čtyř dříve popsaných technik. Všimněme si, že všechny testované klávesnice (PS/2, USB, bezdrátové a laptop) jsou citlivé na alespoň jeden z těchto útoků. Za prvé je uváděno měření v nastavení 1 (polo-zvukotěsné komoře) pro zajištění stabilních výsledků.

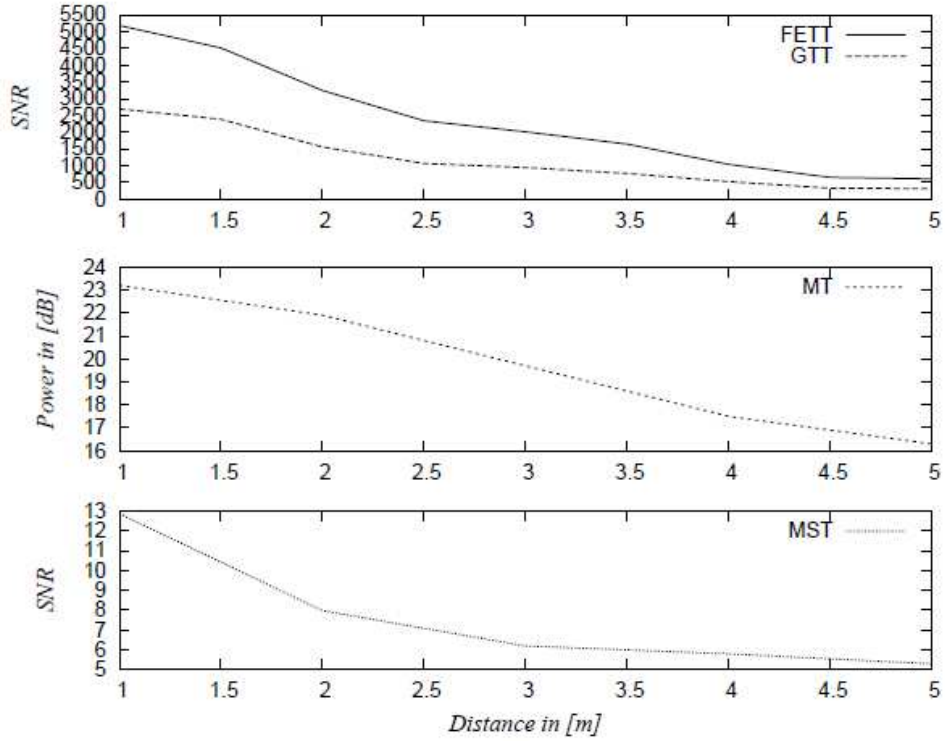
Tabulka 1 Přehled účinnosti metod

klávesnice	typ	metoda 1	metoda 2	metoda 3	metoda 4
A1	PS/2	x	x	x	x
A2	PS/3	x	x		x
A3	PS/4	x	x	x	x
A4	PS/5	x	x	x	
A5	PS/6	x	x	x	x
A6	PS/7	x	x		x
A7	PS/8	x			x
B1	USB				x
B2	USB				x
C1	Laptop	x	x		x
C2	Laptop				x
D1	Wi				x

3.2.2.3.1 Výsledky v ideálním prostředí

Útok lze považovat za úspěšný, když je možné správně obnovit alespoň 95% z více než 500 úhozů. Technika přechodu sestupné hrany, Technika všeobecného přechodu a modulační technika jsou úspěšné v polo-zvukotěsné komoře u všech testovaných klávesnic. To znamená, že lze obnovit úhozy (zcela nebo částečně) nejméně do pěti metrů (maximální vzdálenost uvnitř polo-zvukotěsné komory). Nicméně, Technika skenování matice je omezena na rozmezí od 2 do 5 metrů, v závislosti na klávesnici.

Obrázek 10 představuje úspěšnost Techniky skenování matice v závislosti na vzdálenosti mezi testovanou klávesnicí a anténou. Můžeme si všimnout, že přechod mezi úspěšným a neúspěšným napadením je rychlý. Ovšem správnost obnovy je založena na spoušti osciloskopu. Není-li špička detekována, zachycený signál není úplný a obnovený úhoz je špatný. Pokud je odstup signálu a šumu (SNR) menší než 6 dB není skoro žádná šance úspěšně detekovat špičky. Pokud uvažujeme 6 dB SNR jako minimum, je možné odhadnout teoretickou maximální vzdálenost k úspěšnému obnovení úhozů pro všechny techniky v polo-zvukotěsné komoře.

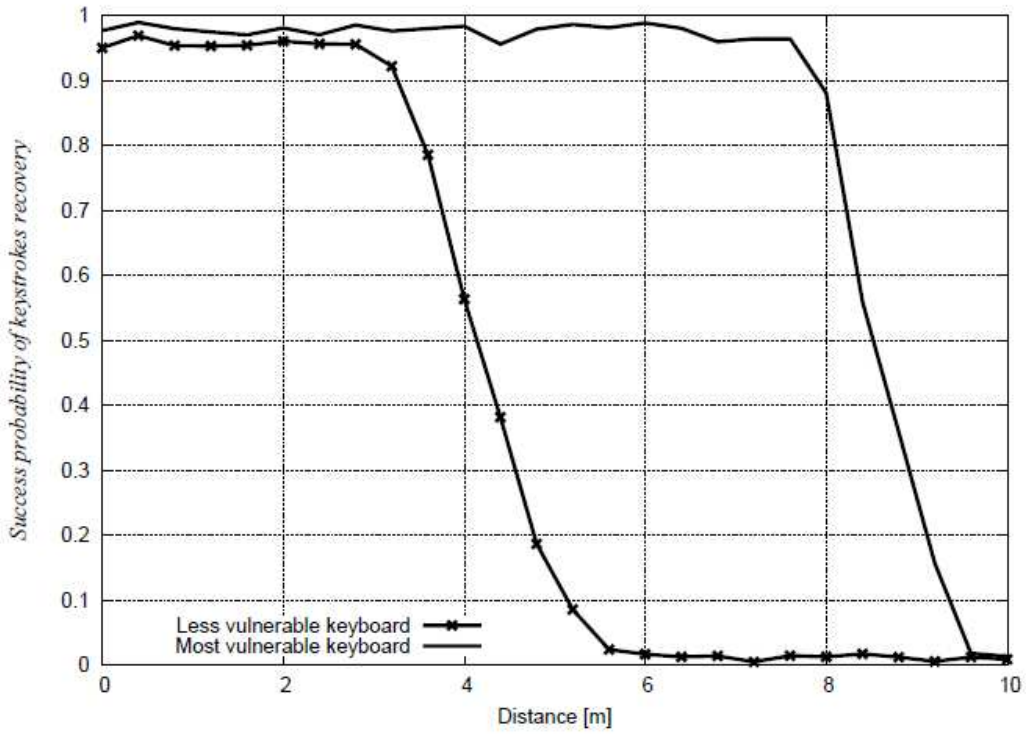


Obrázek 10 SNR s použitím různých metod

V obrázku 10 horní graf udává SNR podle techniky přechodu sestupné hrany a techniky všeobecného přechodu s přesností od 1 metru do 5 metrů. Prostřední graf detailně ukazuje SNR (v dB) nejsilnější nosné frekvence pro modulační techniku pro stejnou klávesnici. Lze tedy odhadnout maximální rozsah těchto útoků podle jejich SNR. Spodní graf udává SNR technikou skenování matice pro stejnou klávesnici. Všechna měření byla shromážděna v polo-zvukotěsné komoře.

3.2.2.3.2 Výsledky ve skutečném prostředí

Druhou fází bylo vyzkoušení těchto technik v některém ze skutečných prostředí. Hlavním rozdílem je přítomnost silného elektromagnetického šumu v pozadí. Nicméně, všechny techniky zůstávají použitelné.



Obrázek 11 Pravděpodobnost úspěchu odposlechu vzhledem ke vzdálenosti

Situace 2: Kancelář. Obrázek 11 udává pravděpodobnost úspěchu techniky všeobecných přechodů na klávesnici č. 1 měřené v kanceláři v závislosti na vzdálenosti mezi anténou a klávesnicí. Bylo zjištěno, že i zde existuje ostrý přechod při SNR pod 6 dB. Maximální rozsah tohoto útoku je mezi 3 a 7,5 metry v závislosti na testované klávesnici. Tyto

hodnoty byly nestabilní vzhledem k měnícímu se šumu v pozadí. Odpovídají průměru u více měření.

Modulační technika je založena na signálu nosné frekvence. SNR nosné frekvence by mělo určit rozsah útoku. Nicméně bylo dosaženo lepších výsledků se stejným modelem spouště použitým v technice přechodu sestupné hrany a technice všeobecného přechodu než jen na základě nosné frekvence. Vzhledem k tomu, že se technika skenování matic vztahuje k detekci vrcholů, byl zaznamenán stejný útlum, když SNR spadl pod 6 dB.

Situace 3: Přilehlá kancelář. Výsledek v této situaci je v podstatě stejný jako u předchozí situace (kancelář), kromě toho, že zeď ze sádrokartonu a dřeva ubírá 3 dB ze SNR.

Situace 4: Budova. Při tomto měření bylo zaznamenáno několik neočekávaných výsledků. Opravdu je možné zachytit signál a úspěšně rozpoznat úhoz klávesy s pravděpodobností vyšší než 95% ve vzdálenosti dvaceti metrů od klávesnice (tj. největší vzdálenost uvnitř budovy). Někdy může být prostředí velmi výhodné pro odposlouchávací proces. Například, kovové struktury, jako jsou trubky nebo elektrické vodiče mohou působit jako antény a výrazně zlepšit rozsah odposlechu. V tomto případě je kompromitující vyzařování vysíláno společnou zemí elektrického vedení. Proto je rozsah definován vzdáleností mezi klávesnicí a společnou zemí a vzdáleností mezi společnou zemí a anténou. Technika skenování matic je snadno narušitelná šumem na společné zemi, neboť spouštěcí model je složitější a vyzařování slabší. Při této technice se podařilo úspěšně zachytit kompromitující vyzařování, jen pokud byla klávesnice méně než jeden metr od společné země. Toto nastavení je zajímavé, protože odpovídá skutečnému scénáři, kde je ten co odposlouchávající v suterénu budovy a snaží se obnovit stisky kláves na klávesnici v pátém patře. Bohužel nebylo možné zajistit stabilní měření, protože velmi závisí na prostředí. Bylo zjištěno, že hlavní (kovové) vodovodní potrubí v budově slouží také jako anténa a může být dobře použito místo společné země. Mimoto tato anténa je méně „znečištěna“ elektronickými zařízeními. Proběhl pokus o stejný experiment v kanceláři, ale šum v pozadí byl příliš silný. Nebylo možné úspěšně rozpoznat kompromitující vysílání. Nicméně, se sondou fyzicky připojenou k datovému vodiči, bylo měření elektromagnetického vyzařování spuštěno správně. Kompromitující elektromagnetické vysílání je přítomno ve společné zemi. Omezení se týká pouze spouště. Všechny techniky byly použitelné na celé patro (cca 20 metrů) s klávesnicí jeden metr od společné země. Je

zřejmé, že za účelem odposlouchávání, lze připojit osciloskop přímo ke společné zemi budovy. Staré PC sloužící k napájení testovaných klávesnic přenášelo kompromitující vyzařování přímo přes společnou zem. Aby se předešlo takovému vodivému spojení přes napájecí zdroj, což nebylo cílem výzkumu, byla měření provedena s klávesnicemi připojenými k notebooku, který byl napájen jen baterií.

3.2.2.4 Závěr experimentu

Experiment přinesl důkazy, že moderní klávesnice vyzařují kompromitující elektromagnetické vyzařování. Čtyři techniky prezentované v tomto dokumentu dokazují, že tato levná zařízení nejsou obecně dostatečně chráněna proti kompromitujícímu vyzařování. Kromě toho bylo prokázáno, že toto vyzařování lze snímat s relativně levným zařízením a úhozy kláves jdou obnovit nejen v polo-zvukotěsné komoře, ale stejně tak v některých skutečných prostředích. Důsledkem těchto útoků je, že ohrožení elektromagnetickým vyzařováním z klávesnic stále představuje bezpečnostní riziko. PS/2, USB laptop a bezdrátové klávesnice jsou zranitelné. Navíc neexistuje žádná softwarová záplata, která by zabránila těmto útokům. Pro získání bezpečného zařízení je třeba nahradit hardware. Kvůli tlaku na výši ceny při konstrukci nemohou výrobci klávesnice systematicky chránit. Nicméně, některé (dražší) bezpečné klávesnice již existují, ale jsou pořizovány především vojenskými organizacemi nebo vládou. Objev těchto útoků byl přímo spojen s výše představenou metodou založenou na analýze celého spektra a výpočtu krátkodobé Fourierovy transformace. Tato technika má některé výhody, vizuální detekci kompromitujícího vyzařování (odhalenou zrakem člověka), velká spektra šířky pásma, využití surového signálu, post-demodulace pomocí softwarové knihovny. Nevýhodou je omezení paměti a obtížnost získat účinnou spoušť. Nicméně, pro krátké shluky dat se zdá toto řešení významné. Budoucí práce by se měly zaměřit na podobná zařízení, jako jsou klávesnice používané u bankomatů (ATM), klávesnice mobilních telefonů, digicodes, tiskárny, bezdrátové routery atd. Dalším hlavním bodem je, aby nebylo využíváno algoritmu pro detekci špiček, protože tento představuje hlavní omezení uváděných útoků. Algoritmy pro extrakci význačných rysů mohou být také zdokonaleny. Souvztažnost těchto útoků s útoky neelektromagnetického vyzařování jako jsou optické, akustické nebo časové útoky by mohly významně zlepšit proces obnovy stisků kláves.

4 PŘESNOST A FINANČNÍ NÁROČNOST METOD

Jednotlivé metody se pochopitelně liší svou náročností na provedení a zejména přesností. Za nejpřesnější a nejsnazší způsob odposlechu považuji nasazení hardwarových keyloggerů. Možnost odhalení je sice vyšší než u ostatních metod, ale po důkladném zhodnocení rizik, znalostí prostředí a pohybu osob v okolí se dá vytipovat bezpečné místo pro jeho nasazení. Přesnost spočívá především v jednoduchosti zařízení, které odebírá data přímo z konektoru klávesnice a zaznamenává je do poměrně velké vnitřní paměti. Jeho přesnost je přitom stoprocentní a možnosti zneužití získaných dat velmi široké. Cena takového zařízení je podle použitého rozhraní od tří tisíc do osmi tisíc korun.

Z hlediska finanční náročnosti jsou pochopitelně nejdostupnější vlastní programy, ale ne každý je schopný příslušný program vytvořit. To však není velkou překážkou. Na internetu se dnes dá sehnat v podstatě cokoliv a podobný program není výjimkou. Cena takových programů může být zanedbatelná, ale podle dokonalosti a možností nasazení se může vyšplhat až na několik tisíc korun za monitorovací systém s kompletní nabídkou služeb. Spolehlivost a přesnost softwarových keyloggerů se liší podle prostředí, ve kterém je použit. Jiné zabezpečení bude mít domácnost, drobná soukromá firmička nebo velká nadnárodní společnost. Zabezpečení pochopitelně odpovídá možným škodám způsobeným únikem informací.

Metoda odposlechu kompromitujícího záření pomocí antény a dalších příslušných zařízení, je sice po zvolení vhodné varianty k příslušnému prostředí celkem přesná, až devadesát pět procent, ale požadavky na znalosti a vybavení jsou poměrně vysoké. Použití podobných metod bych řadil spíše do kategorie profesionálního odposlechu. Tomu odpovídá i cena a dostupnost jednotlivých zařízení.

5 OCHRANA PROTI ODPOSLECHU

V této části jsou doporučena některá možná opatření k ochraně klávesnice proti čtyřem útokům. První řešení k zabránění kompromitujícího vyzařování se zdá triviální. Uživatel by měl odstínit klávesnici, aby došlo k výraznému snížení veškerého elektromagnetického záření. Mnoho součástek uvnitř klávesnice vytváří vyzařování: vnitřní elektronické součástky klávesnice, komunikační kabel, a součásti základní desky uvnitř počítače. Tudíž k odstranění těchto vyzařování musí dojít k odstínění celé klávesnice, kabelu, a součásti základní desky počítače. Výrobce klávesnice poukazuje na skutečnost, že cena odstínění celé klávesnice je nejméně dvakrát vyšší než cena zařízení. Toto řešení proto z důvodu vysokých nákladů není použitelné. Na trhu je možné najít klávesnici, která odpovídá standardu NATO SDIP-27. Ovšem příslušné dokumenty jsou tajné a k dispozici nejsou žádné informace o skutečném limitu vysílání nebo podrobné měřící postupy.

Druhým možným řešením je chránit místnost, kde jsou zranitelné klávesnice používány. Místnost může být odstíněna nebo může být vymezen bezpečnostní perimetr okolo místnosti, například 100 metrů. Útoky 1, 2 a 3 jsou přímo spojené s protokolem PS/2. Jedním z řešení, které předejde nechtěným únikům informací, je šifrování dvousměrnou sériovou komunikací. V moderní klávesnici jeden čip obsahuje řadič, ovladač, detektor, a komunikační rozhraní. Je možné, aby šifrování bylo implementováno v tomto čipu, a žádné přímé kompromitující vyzařování související se sériovou komunikací se neobjeví. Útok 4 souvisí se smyčkou skenování matic. Řešením by mohlo být navrhnout nový skenovací proces algoritmu. I když klávesnice i nadále používá smyčku skenování matice, existuje několik možných řešení. Smyčka může být náhodná. Ve skutečnosti jsou sloupce snímány v dílčím pořadí 1, 2, 3, …, 23, 24, ale je možné pořadí náhodně měnit. Navíc je možné přidat náhodné zpoždění během skenování smyčky. Obě řešení nezabraňují elektromagnetickému vyzařování, ale dělají proces rozpoznání úhozů teoreticky nemožný.

Další možné řešení je založeno na vysokofrekvenční filtraci signálu matice před tím, než se vloží do klávesnice. Toto významně omezuje kompromitující elektromagnetické vyzařování.

6 PRÁVNÍ ASPEKTY POUŽÍVÁNÍ KEYLOGGINGU

Krátce se chci dotknout také právnické stránky užívání keyloggingu. Můžeme se setkat s keyloggingem nelegálním, avšak také legálním.

Na legální užití keyloggerů můžeme narazit například při ochraně vlastního počítače. Jedná se o situace, kdy chceme zabránit neoprávněnému užívání počítače jinou osobou; při kontrole aktivit dětí na počítači, ve chvíli, kdy jsou rodiče mimo dosah; při zálohování dat; nebo při monitoringu činnosti zaměstnanců na počítačích v práci. Legální stránka keyloggingu však tvoří jen zlomek jejich celkového využití. Více se s keyloggery setkáme jako se spyware, který je nainstalován do počítače bez vědomí uživatele za účelem poskytování důvěrných dat (nejčastěji hesla a kódů) třetím osobám.

Samotné vytvoření keyloggeru ještě není v rozporu se zákonem. Protizákonným se stává ve chvíli užití za účelem neoprávněného nabytí informací a jejich využití.

Používání keyloggeru bez vědomí uživatele počítače se v každém případě dotýká práv, které jsou chráněny několika právními předpisy.

6.1 Zásah do zákonných práv člověka

Určitým promítnutím Ústavních zásad do zákonných norem je ustanovení § 11 občanského zákoníku o ochraně osobnosti. Je zde uvedeno, že fyzická osoba má právo na ochranu své osobnosti, mimo jiné i soukromí. Dodržování telekomunikačního tajemství je ochranou soukromí, a pokud je keylogger používán bez vědomí uživatele počítače, je toto právo na soukromí porušeno.[11]

Neoprávněné použití keyloggeru se dotýká také práva na ochranu osobních údajů. Osobním údajem podle zákona č. 101/200 Sb. (O ochraně osobních údajů) je jakákoliv informace týkající se určitého subjektu údajů, podle níž lze tento subjekt spolehlivě identifikovat. Přesnou definici nalezneme ve výše uvedeném zákoně § 4 písm. a). Při použití keyloggeru tak mohou být neoprávněně získány osobní údaje o určité osobě/ subjektu. Děje-li se tak bez souhlasu subjektu, dopouští se uživatel keyloggeru přestupku

[11] http://www.pravoit.cz/article/pravni-aspekty-pouzivani-keyloggeru

na poli ochrany osobních údajů. Za tento přestupek může být Úřadem pro ochranu osobních údajů udělena pokuta až 1.000.000,- Kč.[12]

6.2 Zásah do Ústavních práv člověka

V Listině základních práv a svobod v článku 10 odst. 2 je základní právo každého člověka na ochranu před neoprávněným zasahováním do soukromého a rodinného života. Na základě tohoto článku musíme jakékoli utajené sledování činnosti uživatele počítače, o němž uživatel neví nebo s ním nesouhlasí, posuzovat jako zásah do práva člověka.

Dále je v čl. 13 uvedeno právo nedotknutelnosti listovního tajemství a tajemství jiných písemností nebo záznamů, uchovávaných v soukromí nebo zasílaných poštou nebo jiným způsobem (s výjimkou případů, stanovených zákonem).[13] V případě, že je pomocí keyloggeru sledována e-mailová nebo jiná komunikace, jedná se nejen o porušení práva na soukromí, ale také porušení práva listovního tajemství. Listovní tajemství se totiž dle čl. 13 vztahuje i na zprávy po telefonu nebo jiným podobným zařízením.

6.3 Trestněprávní odpovědnost

Při jistých okolnostech může být neoprávněné užití keyloggingu klasifikováno jako trestný čin. Trestní zákoník tuto skutečnost řeší především v § 230 – 232. Ustanovení o porušování tajemství dopravovaných zpráv je možno aplikovat vždy, když je s pomocí keyloggeru monitorována elektronická komunikace uživatele kontrolovaného počítače s jinou osobou. Vzhledem k tomu, že keylogger může velice snadno posloužit k získání přístupových hesel např. do internetového bankovnictví, této problematiky se snadno mohou dotýkat i trestné činy krádeže případně podvodu ve smyslu ustanovení trestního zákona.[14]

6.4 Kontrola zaměstnanců a zákoník práce

V současné době nejvíce diskutovanou otázkou je používání keyloggerů na pracovišti ke kontrole zaměstnanců. Zaměstnavatel má při používání keyloggerů tu výhodu, že si může na svém počítači jednoduše nainstalovat HW i SW keyloggery a zaměstnanec má velmi

[12] Zákon na ochranu osobních údajů č. 101/2000 Sb. v platném znění
[13] http://www.psp.cz/docs/laws/listina.html
[14] Trestní zákoník č. 40/2009 Sb. v platném znění

malou šanci jej odhalit. Nejčastěji zaměstnavatelé volí určitou formu kontroly z důvodu ochrany obchodního tajemství a sledování řádného výkonu zaměstnanců.

Zaměstnavatel má toto právo kontroly do určité míry upraveno v ust. § 301, zákoníku práce. Zde je uvedeno, že zaměstnanci nesmějí bez souhlasu zaměstnavatele používat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Zaměstnavatel je kompetentní k tomu, aby tuto kontrolu přiměřeným způsobem prováděl.

Zde se však dostáváme do rozporu se zájmem zaměstnance, který má právo na soukromí a ochranu osobních údajů. Tohoto bodu se dotýká § 316 odst. 2 zákoníků práce – „zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci“.[15]

Použití keyloggeru zaměstnavatelem je tudíž teoreticky možné jen v případě, že by si zaznamenával pouze údaje, ke kterým nepotřebuje souhlas zaměstnance. Z povahy keyloggingu však plyne, že jím těžko půjdou zaznamenat jen určité údaje, když se jedná o zachycení každého stisku klávesy a přesného stavu obrazovky (např. v situaci, kdy je na obrazovce zobrazen soukromý e-mail zaměstnance). Proto je při použití keyloggingu pro zaměstnavatele příliš složité a rizikové. Navíc je toto riziko pro zaměstnavatele zbytečné, protože v současné době je spousta programů, které monitorují činnost zaměstnanců na počítači, a nedochází u nich ke konfliktu se zájmy zaměstnanců na ochranu soukromí.

[15] Zákoník práce č. 262/2006 Sb. v platném znění

ZÁVĚR

Možnosti ochrany před keyloggery v podobě spyware jsou omezeny účinností antikeyloggerů a uživatel musí spoléhat zejména na celkové dodržování zásad internetové bezpečnosti. Pokud již keylogger na svém počítači zjistí, je nepochybné, že jeho instalací a užíváním dochází k porušení práv uživatele, zmíněných v této práci. Neplatí absolutní zákaz použití keyloggerů, nicméně toto použití musí mít vždy podklad v zákonném oprávnění.

ZÁVĚR V ANGLIČTINĚ

Possibilities of protection against keyloggers like a spyware, are limited by effectiveness of antikeyloggers and the user must rely mainly on general principles of internet security. If you already find a keylogger on your komputer, there is no doubt that the installation and use of it infringing the users rights mentioned in this work. Not an absolute prohibition on the use of keyloggers, but such use must always have a basis in legal authority.

SEZNAM POUŽITÉ LITERATURY

[1] *Cs.wikipedia.org* [online]. 2004. 2010 [cit. 2010-05-9]. Počítačová klávesnice. Dostupné z WWW:

<http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%A1_kl%C3%A1vesnice#cite_note-0>.

[2] *Cs.wikipedia.org* [online]. 2004 [cit. 2010-05-9]. Počítačová klávesnice. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Počítačová_klávesnice>.

[3] RAMEŠ, Jiří. *Vstupnizarizeni.rames.info* [online]. 2010 [cit. 2010-04-14]. Vstupní zařízení PC. Dostupné z WWW: <http://vstupnizarizeni.rames.info/1keyb.html>.

[4] *Cs.wikipedia.org* [online]. 2004 [cit. 2010-05-9]. Počítačová klávesnice. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Počítačová_klávesnice>.

[5] *En.wikipedia.org* [online]. 2002 [cit. 2010-05-17]. Keystroke logging. Dostupné z WWW: http://en.wikipedia.org/wiki/Keystroke_logging

[6] *En.wikipedia.org* [online]. 2004 [cit. 2010-04-12]. Hypervisor. Dostupné z WWW: <http://en.wikipedia.org/wiki/Hypervisor>

[7] *Cs.wikipedia.org* [online]. 2004 [cit. 2010-04-13]. Kernel. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Kernel>.

[8] w*ww.dozorce.cz* [online]. 2010 [cit. 2010-05-12]. Dostupné z WWW: <http://www.dozorce.cz>.

[9] VUAGNOUX, Martin; PASINI, Sylvain. *Lasecwww.epfl.ch* [online]. 2007-2009 [cit. 2010-05-01]. Dostupné z WWW: <http://lasecwww.epfl.ch/keyboard>.

[10] *Elektronika.kvalitne.cz* [online]. 4.7.2004 [cit. 2010-05-03]. Řízení PS/2 myši. Dostupné z WWW:

<http://elektronika.kvalitne.cz/ATMEL/necoteorie/tutorial/PS2/PS2_mouse.html>.

[11] MALIŠ, Petr. *Www.pravoit.cz* [online]. 2009 [cit. 2010-05-17]. Právní aspekty používání keyloggerů. Dostupné z WWW: <http://www.pravoit.cz/article/pravni-aspekty-pouzivani-keyloggeru>.

[13] *Www.psp.cz* [online]. 2006 [cit. 2010-05-08]. Poslanecká sněmovna parlamentu. Dostupné z WWW: <http://www.psp.cz/docs/laws/listina.html>.

Použitá znění zákonů:
[12] Zákon na ochranu osobních údajů č. 101/2000 Sb. v platném znění
[14] Trestní zákon č. 40/2009 Sb. v platném znění
[15] Zákon na ochranu osobních údajů č. 101/2000 Sb. v platném znění

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ADC	Analog-to-digital converter
AM	Amplitude modulation
API	Application Programming Interface
ATM	Automated teller machine
CLK	Clock
dB	Decibel
DIN	Deutsches Institut Für Normung
FFT	Nástroj pro změnu hlasitostí jednotlivých frekvencí, druh ekvalizéru
KME	Key Mouse Elektronic
FM	Frequency modulation
FPGA	Field-programmable gate array
FPGA	Field programmable gate array
FSK	Frequency-shift keying
FTP	File Transfer Protocol
GHz	Gigahertz
GPIB	General Purpose Interface Bus
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
LCD	Liquid Crystal Display
MB	Megbyte
Mb	Megabit
MHz	Megahertz
Mpt	Mega points
MS/s	Million of samples per second

PC	Personal komputer
PIN	Personal identification number
PS/2	Personal systém 2
PSK	Phase-shift keying
SNR	Signal-to-noise ratio
STFT	Short-Time Fourier Transf
SW	Software
USB	Universal Seriál Bus
USRP	Universal Software Radio Peripheral
WWW	World Wide Web

SEZNAM OBRÁZKŮ

SEZNAM TABULEK