ACOUSTIC SIDE-CHANNEL ATTACK ON KEYBOARD

Petr Machů
Master Degree Programme (2), FEEC BUT
E-mail: xmachu02@stud.feec.vutbr.cz

Supervised by: Zdeněk Martinásek
E-mail: martinasek@feec.vutbr.cz

Abstract: The article is focused od acoustic side channel. Experimental workplace was built to demonstrate the attack and 145 measurements were performed. Waveforms were processed and analyzed in Matlab. The greatest differences were observed in the frequency domain. After finding the most important features will make neural network to perform classification of whole wiritten text.

Keywords: acoustic side channel, side channel atack, keyboard

1 ÚVOD

Se stále zrychlujícím se vývojem moderních komunikačních a počítačových systémů se objevila řada nových typů útoku na kryptografické systémy. Hlavním úkolem pro kryptografické systémy je zajištění bezpečnosti. Tuto úlohu zajišťuje v celém systému kryptografický modul, který je v podstatě fyzickou implementací konkrétního kryptografického algoritmu. Během činnosti kryptografického modulu probíhají uvnitř procesy, které jsou spojeny s šifrováním, dešifrováním, ověřením, autentizací atd. Během těchto činností pracuje modul se senzitivními daty (např. tajný klíč), které bývají uloženy v paměti modulu. Nový způsob kryptoanalýzy postranními kanály, využívá toho, že modul během své činnosti komunikuje se svým okolím nežádoucím způsobem. Modul může vyzařovat do svého okolí např. tepelné nebo elektromagnetické záření, každý reálný modul při své činnosti odebírá určitý proud ze zdroje, každá jeho operace způsobuje různé časové zpoždění, na konkrétní situaci reaguje modul stavovým nebo chybovým hlášením, klávesnice modulu může být mechanicky opotřebená, každá klapka vydává jiný zvukový signál atd. Všechny tyto projevy modulu jsou neodmyslitelně spojeny s jeho činností, při které mohou být vyneseny některé ze senzitivních informací. Každá nežádoucí způsob výměny informace mezi kryptografickým modulem a jeho okolím se nazývá postranním kanálem [2]. Analýzou postranního kanálu je označován postup, při kterém je možné získat užitečné informace, které lze odvodit ze signálu přicházejícím po tomto kanálu. Útok vedený pomocí postranního kanálu je založen na využití takto získané informace k napadení daného kryptografického modulu.

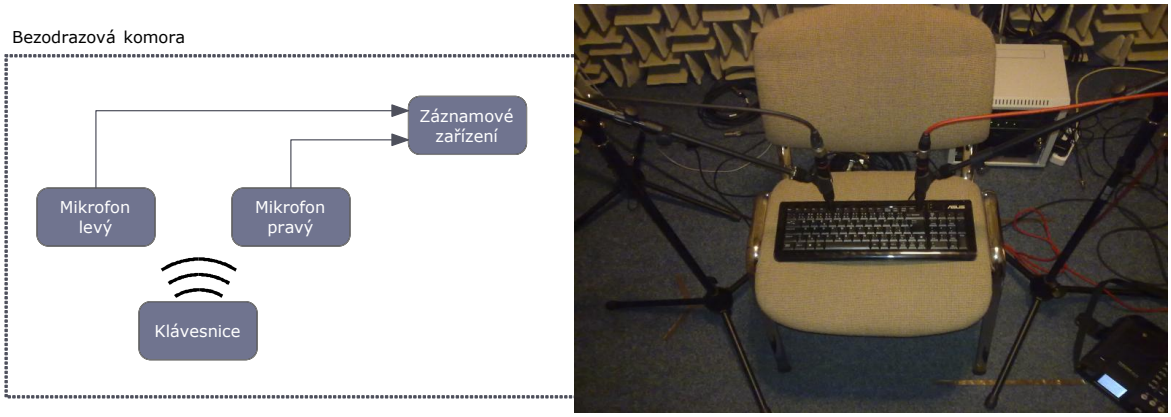
2 AKUSTICKÁ ANALÝZA

Akustický postranní kanál patří k nejstarším postranním kanálům. Byl používán již v době, kdy se definice postranních kanálů ještě nepoužívala např. v roce 1956 Britové získávají informace z egyptského šifrátoru odposlechem zvuků klávesnice a v roce 1961 Američané provádějí akustický odposlech prostřednictvím ústředního topení. Další akustické útoky byly prováděny na klávesy psacího stroje a jehličkové tiskárny. Nyní se tento postranní kanál zaměřuje na zvuky vydávané počítačovými klávesnicemi [4] a také na vnitřní komponenty PC (mikroprocesor, koprocesor...) [3]. V jednotlivých útocích byly použity různé metody pro převod zvukového signálu klávesnice zpět na text. Např. v práci "Dictionary Attacks Using Keyboard Acoustic Emanations" se pro zpětnou analýzu využívá anglický slovník a neuronové sítě [4]. Práce Au Hiu Yan Fiona pouze počítá rozdíly v době příchodu

zvukové vlny na dva mikrofony [1]. Žádná z metod není schopna rekonstruovat stisk více kláves najednou. Mezi nejčastější použití patří psaní velkých písmen a speciálních znaků tedy kombinace klávesy “Shift” s některou jinou klávesou. Práce si klade za cíl realizaci experimentálního pracoviště a získání dostatečného množství akustických vzorů klávesnice. S pomocí této trénovací množiny navrhnout a realizovat metodu, která bude schopna rozeznat psaní klávesových kombinací s klávesou “Shift”.

3 EXPERIMENTÁLNÍ PRACOVIŠTĚ

Pro získání zvukových nahrávek bylo realizováno experimentální pracoviště. Blokové schéma a skutečná podoba pracoviště je zobrazena na obr. 1. Pro eliminaci rušivých signálů byla využita bezodrazová komora. Pro záznam zvuků byla použita dvojce měřících mikrofonů MiniSPL a záznamové zařízení TASCAM HD-P2. Pro přesnější výsledky bylo každé měření provedeno pětkrát.

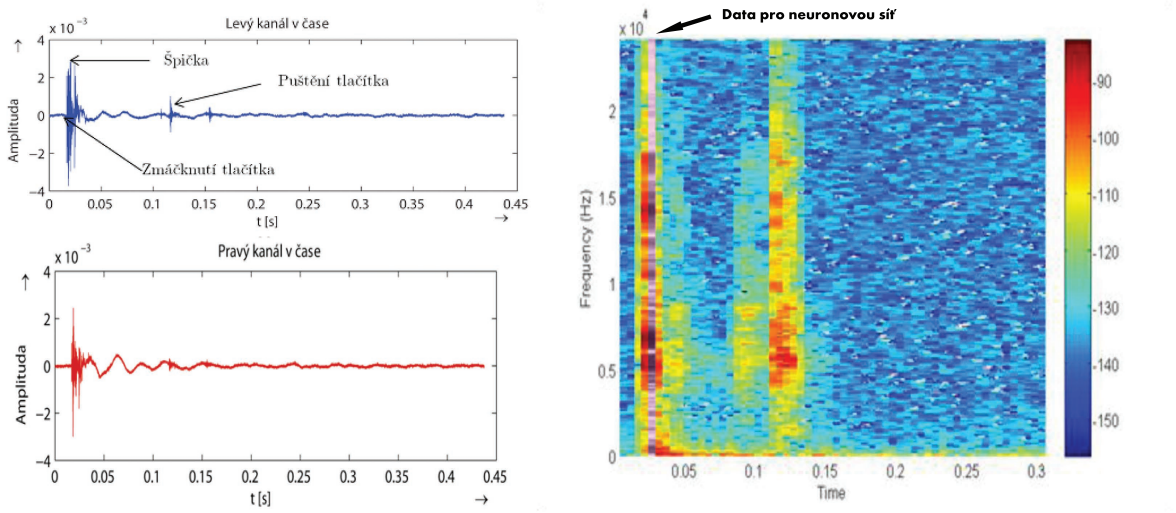


Obrázek 1: Blokové schéma experimentálního pracoviště (vlevo), skutečná podoba pracoviště (vpravo)

Mikrofony byly umístěny 9 cm nad klávesnicí a 12 cm od jednotlivých okrajů. Při měření byly nahrávky ukládány do formátu “wav” se vzorkovacím kmitočtem 48 kHz a hloubkou 16 bitů. Byly zaznamenány jednotlivé klávesy, dále sekvence kláves, ale také kombinace více stisknutých kláves (např. Shift + L). Při prvním měření vzniklo celkem 175 nahrávek. Zpracování nahrávek probíhalo v programu Matlab, který podporuje práci se soubory “wav”. Nejprve byly upraveny jednotlivé nahrávky tak, aby úhoz klávesy začínal ve stejný časový okamžik a celkový čas nahrávky byl konstantní. Časový průběh klávesy “d” je zobrazen na obrázku 2 vlevo. Modrý průběh zobrazuje signál z levého mikrofonu a červený z pravého mikrofonu. Z grafu vidíme, že jednotlivé kanály se liší. To je způsobeno samozřejmě tím, že jednotlivé mikrofony jsou umístěny na různých místech nad klávesnicí. Za povšimnutí stojí zejména fakt, že pravý mikrofon již téměř nezachytil puštění tlačítka. Pro názornost je podrobně okomentován průběh levého kanálu.

Následně byly signály převedeny z časové oblasti do frekvenční (viz. obr 2 vpravo). K tomu byla využita STFT transformace (Short-Time Fourier Transform). Na obrázku je patrný výskyt frekvencí v čase 0,025 s, kdy došlo ke stisku klávesy, kolem 5 kHz a následně kolem 13 kHz, poté při puštění tlačítka frekvence zejména kolem 5 kHz. Z času 0,025 s byly také vybrány vzorky z frekvenční oblasti, pomocí niž by bylo možné hledat klasifikovat jednotlivé klíče pro různé klapky. Na tyto klíče byl následně aplikován klasifikátor s umělou neuronovou sítí.

Z jednotlivých naměřených klapek, byly vždy vybrány vzorky z okna kolem času 0,025 a vytvořen medián, který sloužil jako trénovací množina pro jednoduchou dvouvrstvou dopřednou neuronovou síť s 15-ti neurony ve skryté vrstvě. Pomocí takto vytvořené sítě se podařilo dosáhnout 66% úspěšnosti.



Obrázek 2: Časový průběh klávesy “d” - podrobný popis levý kanál, signál zobrazen ve frekvenční oblasti (vpravo)

Vyšší úspěšnost rozpoznávání by mělo zajistit více naměřených dat, použití vzorků z obou kanálů, přidání dalších trénovacích dat např. v jiný čas, popř. zapojení slovníků jako v práci “Dictionary Attacks Using Keyboard Acoustic Emanations”. Ovšem zda a o jaký přínos se bude jednat se zjistí až z následných experimentálních pokusů [4].

4 ZÁVĚR

Článek nejprve definoval problematikou postranních kanálů a následně se zaměřuje na akustický postranní kanál, který lze využít při útoku na klávesnici počítače. Práce si klade za cíl navrhnout a realizovat útok, který bude schopen rozeznat kompletní psaný text tedy i psaní klávesových kombinací například s klávesou “Shift”. Pro demonstraci útoku bylo vybudováno experimentální pracoviště na kterém bylo provedeno měření celkem 175 nahrávek. Naměřené průběhy byly zpracovány v programu Matlab a byly analyzovány dílčí výsledky práce, které naznačují, že jednotlivé klávesy jsou rozpoznatelné ve frekvenční oblasti. Po nalezení nejvýznamnějších znaků bude natrénována neuronová síť, která bude provádět klasifikaci.

REFERENCE

[1] Hiu, A.; Fiona, Y.: ERG4920CM Thesis II Keyboard Acoustic Triangulation Attack BY.

[2] Klima, V.; Rosa, T.: Side Channel Attacks on CBC Encrypted Messages in the PKCS7 Format. Cryptology ePrint Archive, Report 2003/098, 2003.

[3] Shamir, A.; Tromer, E.: Acoustic cryptanalysis On nosy people and noisy machines @ONLINE. URL `http://people.csail.mit.edu/tromer/acoustic/`

[4] Zhuang, L.; Zhou, F.; Tygar, J. D.: Keyboard acoustic emanations revisited. In *Proceedings of the 12th ACM conference on Computer and communications security*, CCS ’05, New York, NY, USA: ACM, 2005, ISBN 1-59593-226-7, s. 373–382, doi: http://doi.acm.org/10.1145/1102120.1102169.
URL `http://doi.acm.org/10.1145/1102120.1102169`