KAPITOLA 1 - Špionážní a protišpionážní technika

Tato kapitola není určena pro agenty 007, nýbrž pouze odráží reálný stav v používání špionážní a protišpionážní techniky v České republice. Bohužel nejasná úprava této oblasti v našem právním řádu umožňuje její masové nasazení bez větší obavy z případného postihu. Pokud by jste se snad domnívali, že se bez základních znalostí z tohoto oboru klidně obejdete, musím vás zklamat. Dle odhadů bezpečnostních exportů se předpokládá, že asi každá desátá kancelář vrcholného manažera některé z českých firem je odposlouchávána. Sami po prvotním výčtu oblastí použití špionážní techniky pochopíte, že se toto téma týká bezprostředně i vás samotných.

Oblasti použití (proti) špionážní techniky:
1) odposlechy hlasové komunikace v objektech (kanceláře...);
2) odposlechy telefonních hovorů;
3) odposlechy faxových zpráv;
4) čtení e-mailových zpráv;
5) zhotovení fotografií a videozáznamů (např. diskreditace, plánování loupeže...);
6) zkopírování písemných materiálů;
7) zkopírování obsahu harddisku počítače či paměťových médií;
8) „čtení“ obrazovky počítače;
9) sledování osob a vozidel;
10) kontrola řádného využití pracovní doby;
11) zamezení komunikace mobilními telefony;
12) odhalování plagiátů prací na vysokých školách.

Jaký si myslíte, že je základní důvod k použití špionážní techniky? Zajisté jste uvažovali správně – je to především ZÍSKÁNÍ INFORMACÍ. Právě informace se stávají v našem uspěchaném světě velmi lukrativním zbožím, které je možné výhodně zpeněžit. A peníze přece hýbají světem.

1.1. Odposlechy hlasové komunikace v objektech

Ve svých bytech anebo kancelářích se cítíme velmi bezpečně, neboť jsme na „domácí půdě“. Většinou si ani nepřipouštíme možnost, že je někdo schopen poslouchat, případně i nahrávat, vše co se zde řekne. Komunikace v takových prostorech může zahrnovat například:

1) rozhovory zaměstnanců
Asi nikoho z konkurenční firmy nebude zajisté zajímat co si myslí soustružník o firmě ve které je zaměstnán. Avšak rozhovory vedoucích pracovníků, případně top-manažerů již pro konkurenci budou více než zajímavé. Mohou se z nich dozvědět základní informace o nových strategických úmyslech svého konkurenta, o potížích se kterými se tento potýká a naopak o úspěších kterých v poslední době dosáhl. A vědět dopředu to co udělá nebo může udělat konkurence by si přece přála vědět každá firma.

2) průběh porad
Právě na poradách jsou vyřčeny ty nejzávažnější informace, navíc ve zhuštěné formě. Porad se zpravidla zúčastňují vedoucí pracovníci z různých oddělení a to na jednom místě. Tedy není nutné odposlouchávat složitě každou kancelář dílčího vedoucího, stačí prostě „napíchnou“ zasedací místnost.

3) **reakce zaměstnanců na „návštěvy“**
   Psychologové by vám potvrdili, že po odchodu návštěvy má člověk tendenci podělit se s manželkou či spolupracovníkem o své pocity z této návštěvy. Při znalosti této skutečnosti lze velmi snadno zapomenout v obývacím pokoji anebo kanceláři kabát či deštník obsahující štěnici a pomocí jednoduchého zařízení si za rohem vše v klidu vyslechnout, aby se pak s odstupem několika minut pro zapomenutou věc vrátil.
4) **rozhovory s „návštěvami“**
   Také znalost obsahu rozhovoru s návštěvou může znamenat strategickou výhodu. Nemusí se jednat pouze o rozhovory vedoucí představitelů podniků se spolupracujícími firmami (odběratelé a dodavatelé), kdy se mohou uzavírat různé dohody, cenové zvýhodnění, protislužby apod., ale též návštěva milenky u ředitele podniku může poskytnout velmi zajímavý zvukový materiál, který konkurenční firmě později umožní tuto osobu vydírat.
5) **předávání informací konkurenci**
   Nejjednodušší metodou jak získat informace od konkurence je získat pro spolupráci některého z jejích zaměstnanců. Peníze se většinou stávají dostatečným motivem pro zradu. Skutečnost, že někdo z firmy vynáší informace je známa jejímu vedení poměrně záhy. Jenže kdo je ten zrádce? A právě monitorování vlastních prostor může být dobrým preventivním opatřením k zjištění loajálnosti vlastních zaměstnanců.
6) **rozhovory úředníků s klienty**
   Každý nás by si přál setkat se na úřadě s ochotným úředníkem a v obchodě s vlídným prodavačem. Stejné přání jistě mají i vedoucí oněch úřadů a majitelé obchodů, neboť právě spokojenost nás občanů je to, oč by jim mělo jít. Nasazením příslušné techniky tak mohou získat nezkreslený obrázek toho jak situace skutečně vypadá a případně se s pracovníky, kteří nenaplňují jejich představy včas rozloučit. Zvukové záznamy pak mohou sloužit též jako důkazní prostředek proti úředníkům, kteří by si snad chtěli ze státního orgánu udělat společnost s ručením omezeným.

Obrana proti umístění štěnice v objektu, kanceláři nebo bytě však není vůbec jednoduchá, neboť existuje v současné době velmi mnoho různorodých možností kam štěnici umístit a jak zajistit dálkový přenos snímané informace.

Protiodposlechová detekční a vyhledávací souprava RFDS-3

Prvním krokem, který je nutno učinit, je zjištění zda již nebyla štěnice v zájmové místnosti umístěna. K vyhledání takového nechtěného vysílače slouží právě RFDS-3. Jedná se o soupravu, která obsahuje vf detektor RFD-2 s teleskopickou anténou k automatické detekci nejsilnějšího blízké vysílače se zobrazením intenzity radiového signálu v pásmu 1 MHz – 10 GHz. Dále obsahuje:

a) externí sondu EXTSOND zvětšující rozsah až do 20 GHz s nastavitelnou tyčí 2,4 m pro kontrolu stropů;
b) speciální generátor WHG k vyhledávání průchodu neznámých vodičů ;
c) linkový adaptér LTA pro odhalení mikrofonních, linkových a síťových odposlechových prostředků;
d) sluchátka a dvě antény pro příjem generátoru.

Souprava je umístěná v diplomatickém kufříku pro utajené přenášení. Cena soupravy je pak cca 40.000,- Kč.

Firmy poskytující služby spojené s vyhledáváním štěnic si většinou účtují za prohlédnutí místnosti cca 30 m^2 částku pohybující se okolo 4.000,- Kč a musíte počítat s několikahodinovou práci jejích techniků.

Paměťový radiový analyzátor MRA-3

Pokud máte jistotu, že v zájmové místnosti žádný odposlech není instalován, je nutné dlouhodobě zajistit aby to tak zůstalo. MRA-3 je speciální scanovací přijímač určený k nepřetržité ochraně prostoru a k okamžitému zjištění radiového odposlechu. Ultrarychlý vyhodnocovací systém odhalí do místnosti vnesený nebo dálkově aktivovaný odposlech i v podmínkách silného vysokofrekfenčního pole místních rozhlasových a televizních vysílačů.

MRA 3 umožňuje odhalení přítomnosti nového signálu během 6 sekund a uživatel je na přítomnost podezřelého signálu okamžitě upozorněn. K omezení falešných poplachů je MRA-3 vybaven tříúrovňovým poplachovým hlášením předpoplach – poplach – minulý poplach. Díky malým rozměrům a zcela kompaktnímu provedení přístroje, který obsahuje vestavěnou teleskopickou anténu a vnitřní baterii, lze MRA-3 snadno umístit jak na nábytku kanceláře, tak i skrytě. Pro skryté použití je z přístroje vyveden signál alarm umožňující připojení externí LED.

Technická specifikace:

Kmitočtový rozsah:	43 – 2.700 MHz
Automatické scanování:	6 sekund
Rozlišení:	0,1 MHz (přesnost měření lepší než 10^{-4})
Poplach:	po 1-20 min. přítomnosti trvalého signálu
Spotřeba (SCAN):	44 mA
Napájení:	12 – 25 V DC (vnitřní baterie 9 V)
Měření vzdálenosti vysílače:	1 mW (1-50 m)
Rozměry:	136 x 49 x 137 mm
Cena:	cca 30.000,- Kč

Nasazením MRA-3 sice odposlechu nezabráníte, ale včas dostanete informaci, že například během noci někdo odposlech ve vaší kanceláři nainstaloval anebo, že návštěvník, který právě vstupuje do vaší kanceláře má aktivní štěnici ve své aktovce.

SNG – inteligentní šumový generátor

Pokud si nemůžete dovolit pouhé oznámení, že se vás někdo snaží odposlouchávat, můžete použít SNG, což je inteligentní výkonový šumový generátor umožňující připojení až 100 piezoelektrických akustických měničů, 2 – 12 nízkoimpedančních reproduktorů nebo jejich vzájemnou kombinaci.

Účelem zašumění je zajistit ochranu prostoru proti odposlechu využívajícího všech forem snímání zvuku z oken, zdí, případně i z jiných předmětů, pokud útočníkův systém využívá jako průnik do prostoru okna nebo zdi místnosti.

Účinnost SNG optimalizuje vestavěný procesor, který v automatickém režimu analyzuje zvuky z místnosti a zajišťuje jen takovou úroveň zašumění, která je nutná v závislosti na hlasitosti konverzace. Nejvýznamnějším přínosem z hlediska bezpečnosti je podstatně zjednodušená obsluha. Pracovník není rušen šumem, pokud je v místnosti klid, přístroj nevypíná, čímž je následně stoprocentně zajištěn automatický náběh šumu například při náhlé návštěvě, zahájení jednání, telefonního hovoru, atd. Časové konstanty náběhu i zániku šumu obdobně jako kritéria výběru charakteristických znaků lidského hlasu a jeho rytmu jsou optimalizovány zejména s ohledem na vysokou bezpečnost, především na spolehlivý náběh šumu v širokém rozsahu zcela odlišných lidských hlasů.

SNG je konstruován k zavěšení na zeď nebo bok pracovního stolu, nejlépe v přímém dosahu uživatele. Z předního panelu lze pomocí tří ovládacích přepínačů zvolit buď „malý“ nebo „velký“ výkon a obě výkonové úrovně lze provozovat buď v manuálním nebo automatickém režimu. Pět barevných LED signalizuje nastavený režim včetně vnitřního testu činnosti procesoru. Cena cca 15.000,- Kč.

Rušička mikrofonů a GSM – mobilních telefonů

Asi nejjednodušší formou odposlechu je využití klasického mobilního telefonu, který má dnes již téměř každý školák. Aby zájmový prostor nemohl být touto formou odposloucháván je možné použít elegantní kufříkovou rušičku, která je určena k zarušení všech mikrofonů v jejím dosahu. Tedy znemožňuje pořízení jakéhokoliv zvukového záznamu přes mikrofon, diktafon, mikrofon kamery, radiomikrofon (štěnici) apod.

Kufříková rušička mikrofonů je doplněna i rušičkou mobilních telefonů, tedy v jednom kufříku jsou dvě rušičky na dálkové ovládání.

Skořepinový diplomatický kufřík s vestavěnými rušičkami mikrofonů a GSM má zamykání numerickým kódem.

Rušička mikrofonů vyzařuje rušivé pole směrovou anténou pod úhlem cca 75°. Směrovou anténou se zvyšuje její účinnost. Rušička GSM – mobilních signálů vyzařuje rušení s všesměrovou charakteristikou.

Technika pro prostorový odposlech

Pro provádění prostorového odposlechu je možné využít různé radiomikrofony – štěnice (přenos zvuku radiovou cestou). Tyto radiomikrofony jsou v různých provedeních a samozřejmě i různých vlastností a technologií. I v případě, že je použit nejlevnější analogový nestabilizovaný radiomikrofon, je zajištěn perfektní a věrný přenos zvuku, který zachytí i šepot, dýchání apod.

Cena této techniky, přijímaček a scannerů není běžně zveřejňována na internetu. Rozmezí cen speciálních přijímaček je pak od 2.000,- do cca 22.000,- Kč včetně DPH.

1.2. Odposlechy telefonních hovorů

Bez telefonního přístroje si dnes těžko svůj život dokážeme představit. Při pohledu na sumarizaci svých hovorů od mobilního operátora se většinou pouze divíme, že jsme toho „tolik prokecali“. V zaměstnání pak používáme telefon k vyřizování většiny služebních záležitostí. Tedy i monitorování telefonní komunikace konkurenční firmy je velmi lákavé. Odposlechy telefonních hovorů lze provádět:

1) pomocí volně přístupných telefonních rozvaděčů umístěných;
   a) v suterénech činžovních domů;
   b) v plotech rodinných domků;
   c) na sloupech;
   d) v rozvodnách;
2) instalací „štěnic“ přímo do zájmového telefonního přístroje;
3) přímo na ústředně operátora.

Z výše uvedeného je zřejmé, že provádění odposlechů telefonních hovorů není nijak složité a vzhledem ke skutečnosti, že většinu přenosové cesty nejste schopni kontrolovat je jediným efektivním opatřením nesdělovat prostřednictvím telefonu ostatním nic podstatného a zneužitelného.

Pokud však z jakéhokoliv důvodu musíte telefonní linky využívat k řešení závažných a zneužitelných hovorů pak jedinou ochranou je jejich šifrování. K tomuto můžete využít např. ARGUS-2 (pevné linky) nebo speciální mobilní telefony s kryptovacími funkcemi.

Speciální mobilní telefony s možností šifrovat hovory jsou poměrně finančně náročné a není o těchto na internetových stránkách mnoho bližších informací.

ARGUS - 2

Digitální scrambler ARGUS-2 je určen pro utajení telefonních hovorů v místní i meziměstské síti:

1. pracuje s libovolným standardním telefonním přístrojem, homologovaným pro ČR
2. má jednoduché ovládání, většina operací se provádí automaticky
3. v otevřeném režimu hovoru zůstávají všechny funkce telefonu zachovány
4. v utajeném režimu se hovorový signál zpracovává digitálně

Pro možnost kryptování hovorů na pevných linkách musí být k dispozici nejméně dva přístroje Argus 2 (jeden šifruje a druhý dešifruje). Podobně jako u počítačových sítí musí být softwarově nastavena příslušnost k dané síti. K tomu slouží tzv. MASTER KEY, který bezpečnostní správce nastaví shodně na obou přístrojích. Argus 2 se zapojuje tak, že přívodní telefonní linka se zapojí do konektoru LINE a telefonní přístroj do konektoru PHONE. Argus 2 je tak vlastně předřazen telefonnímu přístroji. V případě běžného (nekryptovaného) hovoru pak Argus 2 nijak tento hovor neovlivňuje. Programování digitálního scrambleru se provádí prostřednictvím telefonního přístroje (klávesnice).

Po klasickém navázání telefonního hovoru je vhodné mít domluvené kódové slovo, např. Je u tebe všechno O´KEY? Po tomto vyslovení kódového slova některým z účastníků hovoru pak každý z nich stiskne tlačítko MODE a půvabným dívčím hlasem ze sluchátka (hovoří Argus 2) je vyzván aby zadal PIN kód pro konkrétní spojení. Na zadání mají oba účastníci hovoru přibližně 4 sekundy. ARGUSy si pak vzájemně zkontrolují nastavení MASTER KEY a PIN kódu a zjistí-li shodu spustí kryptovací režim Argus 2, dívčí hlas oznámí: „Váš hovor je kódován, hovořte!“ a rozsvítí se červená LED dioda na čelním panelu. Po skončení hovoru stačí položit klasicky telefonní sluchátko a Argus 2 se přepne do režimu STAND BYE.

Technické parametry

- hovorová srozumitelnost v plném duplexním režimu min. 90 %
- zpoždění hovorového signálu - vysílání/příjem max. 0,32 sec.
- doba přechodu do kódového režimu max. 10 sec. (poměr signál/šum 12 dB)
- utajení hovorových informací se provádí :
  a) časovým přemístěním signálu
  b) inverzí spektra signálu
  c) změnou časového měřítka vzorkování hovorového signálu
- klíčovací systém využívá metody veřejných klíčů se :
  a) spojovým klíčem unikátním pro každý hovor
  b) hlavním klíčem (MASTER KEY) programovatelným uživatelem
  c) heslem, volitelným z číselnice telefonního přístroje
    - řád spojového klíče 128 bit
    - řád hlavního klíče 128 bit
    - řád hesla 4 dekadické číslice
- střední počet zkoušek na rozkrytí klíčů - min. 10 na 15
- automatický test funkčnosti při zapnutí přístroje
- napájení 220 V / 50 Hz, příkon max. 10 VA
- vnější rozměry 200 x 280 x 40 mm
- hmotnost 1,5 kg

1.3. Odposlechy faxových zpráv

Pro odposlechy faxových zpráv platí prakticky vše co bylo uvedeno v bodu 1.2. Specifikou však může být, že faxové přístroje v sobě uchovávají přehled o:

a) volaných telefonních číslech;
b) datu a času volání;
c) délce přenosu;
d) počtu přenesených dokumentů;
e) úspěšnosti přenosu (ERROR, O.K.).

Takový REPORT sice nemůže poskytnout informace o obsahu odfaxovaných dokumentů, ale v některých specifických případech i přesto může mít velmi hodnotnou vypovídací schopnost.

1.4. Čtení e-mailových zpráv

Zasílání e-mailových zpráv zvolna, ale jistě, vytlačuje klasické dopisy. Se zavedením elektronického podpisu je pak ještě umožněno pomocí e-mailů zasílat též dokumenty mimořádné důležitosti, např. i daňová přiznání Finančnímu úřadu.

Vzhledem k tomu, že e-maily jsou zasílány prostřednictvím internetu, tedy nekontrolovatelným datovým kanálem, vzniká možnost jejich přečtení neautorizovanou osobou.

E-mailové zprávy lze číst pomocí:

1. speciálního softwaru instalovaného přímo na zájmovém počítači;
2. sledování komunikace počítače;
   a) v síti LAN (interní počítačová síť);
   b) v síti WAN (externí počítačová síť);
3. jednorázovým proniknutím do počítače;
   a) obsluhou;
   b) hackerem.

1.5. Zhotovení fotografií a videozáznamů

Noviny jsou sedmou velmocí světa. Tisk v mnohém ovlivňuje veřejné mínění a následně i chování obyčejných lidí ale i politiků. Přitom stačí někdy tak málo – jeden článek v novinách doplněný fotografií a politik si může balit v úřadě svoje věci do papírové krabice, protože jednou provždy jako politik končí. Soutěžící reality show je vyřazen ze soutěže, protože např. BLESK uveřejní jeho fotografii coby pornoherce. Manželka podá žádost o rozvod, protože vyjde najevo nevěra jejího manžela. Sumarizace této kapitoly by mohla vypadat například takto:

1. nahrávky tzv. neoficiálních prohlášení (reportáže do TV, rádia...);
2. činnost tzv. paparazzi (fotografie, které by jste rozhodně nechtěli zveřejnit ...);
3. přijímání úplatků, říkání si o úplatek;
4. zachycení trestné činnosti (materiál k vydírání);
5. získávání kompromitujících materiálů (milenky, homosexualita...);
6. skrytá kamera (nahota, krádeže v podniku, melouchy, špatná práce...);
7. činnost bezpečnostních složek, vzhled a uspořádání objektů (plánování loupeží...).

Minikamera se zvukem v krabičce od cigaret

Videoštěnice zabudovaná do krabičky od cigaret – přenáší radiovou cestou obraz i zvuk na místo, kde je přijímač propojený například s videem, videokamerou, videowalkmanem, nebo televizorem. Je možné okamžitě sledovat živě obraz i zvuk, nebo nahrávat.

Vzhledem k ceně paměťových nosičů je možné prakticky časově neomezeně možné takový záznam dlouhodobě uchovávat pro další použití (DVD, Blue disk ray, harddisk počítače).

Sada obsahuje minikameru s mikrofonem v krabičce od cigaret, v níž je pouze dírka pro objektiv o velikosti 1 mm!, dále přijímač, adaptér na napájení přijímače a propojovací kabely do TV, nebo videa. Cena dle provedení od 35.900,- Kč výše.

Objektiv AF-S 200-400 mm f/4G VR/IF-ED

Digitální fotoaparát s tzv. teleobjektivem umožní zhotovení fotografie i na vzdálenost několika kilometrů v dostatečné kvalitě.

Technická data:

Nejkratší zaostřovací vzdálenost:	2.000 m
Světelnost objektivu:	f/4
Cena s DPH:	186.190,- Kč

Příklad:

Pokud mám objektiv o průměru 50 mm a ohniskové vzdálenosti 150 mm, tak světelnost je 50/150 = f1/3. Správně bychom měli světelnost psát ve tvaru zlomku, ale v praxi se používá samotný jmenovatel, takže se v praxi používá tvar f3, popř. můžeme říci, že „světelnost je jedna ku třem“. Čím je číslo vyjadřující světelnost menší, tím lepší. Například objektiv se světelností 2,8 má lepší světelnost než objektiv se světelností 4,8.

Dalekohled s digitálním fotoaparátem

V některých případech není použití fotoaparátu možné. V daném objektu je například fotografování zakázáno nebo by taková činnost mohla vzbudit nežádoucí pozornost. Kombinace digitálního fotoaparátu a dalekohledu s 10ti násobným zvětšením se tak může stát dobrým východiskem. Díky zabudovanému fotoaparátu budete moci pořizovat i snímky vzdálených objektů. Napájení je řešeno pomocí 2 baterií typu AAA baterií nebo akumulátorů. Digitální fotoaparát má rozlišení 640x480, interní paměť 8 MB. Dalekohled: zvětšení 10x, průměr objektivu 25 mm, zorné pole 101/1000 m. Systémové předpoklady: operační systém Windows 98 a vyšší, USB 1.1 a vyšší. Cena cca 1.300,- Kč.

Měřicí přístroj Bosch PLR 30

Fotografie má dobrou vypovídací schopnost, avšak byť by jste měli několik fotografií zájmové místnosti nebude asi nijak jednoduché z těchto zhotovit její půdorysné schéma. K takovému účelu bude výhodnější použít měřicí přístroj např. od firmy BOSCH.

Technická data:

Měřicí rozsah:	0,20 – 30,00 m
Přesnost měření:	typ. $\pm$ 2,0 mm
Doba měření:	typ. < 0,5 s
Hmotnost:	cca 0,18 kg
Rozměry:	110 x 66 x 32 mm
Cena:	cca 3.000,- Kč

1.6. Zkopírování písemných materiálů

Byť žijeme v době počítačů, přesto většina firem uchovává množství dokumentů též v papírové podobě. Pokud je na papírovém nosiči zaznamenána nějaká důležitá informace bude i tento cílem vašich protivníků.

Jakými prostředky lze zhotovit kopii dat uvedených na papíře:

1. digitální fotoaparát (mobilní telefon s digitálním fotoaparátem);
2. kopírka;
3. scaner (stolní, ruční);
4. fax (s funkcí COPY);
5. digitální kamera (fotografický režim);
6. namluvení textu na diktafon (do mobilního telefonu, vysílačky);
7. opsání textu do počítače (do PDA);
8. ruční opsání textu na papír (zrychlení možné využitím těsnopisu).

Rozhodujícím faktorem jaký z výše uvedených prostředků využít bude způsob střežení daného objektu, čas který na provedení zkopírování máte a v neposlední řadě i charakter kopírovaných dat (např. stavební výkres lze jen velmi těžko opsat anebo nadiktovat jiné osobě).

1.7. Zkopírování obsahu harddisku počítači či paměťových médií

Firmy, státní úřady a dokonce i obyčejní občané dnes většinu dat ukládají na harddisk svého počítači či paměťová média. Je to jednodušší, umožňuje jim to jejich rychlejší vyhledávání, nezabírají příliš místa a vytisknout je lze koneckonců kdykoliv, že?

Zkopírovat obsah harddisku nebo paměťových médií lze:

1. vypálením na CD-ROM, DVD, Blue Ray Disc) – až 50 GB/disk;
2. zkopírování na externí harddisk;
3. zkopírování na USB klíčenku, paměťovou kartu;
4. zkopírování pomocí FTP protokolu;
5. zkopírování dat na jiný počítač (propojení PC do sítě);
   a) kabelem;
   b) WI-FI;
   c) Bluetooth.

1.8. „Čtení“ obrazovky počítače

To, že lze snímat obsah displeje z poměrně velké vzdálenosti, to, že ***elektromagnetické vyzařování*** počítače vyzařuje i užitečnou informaci o zpracovávaných datech, je známo dost dlouho.

Že by se to mohlo dít i ***akusticky***, napadlo jenom „bláznivé kryptology“ – Adi Shamir a Eran Tromer dali mikrofon k počítači a potvrdil to experimentálně! Postranní kanály jsou novou revoluční metodou v kryptoanalýze, která přináší velmi účinné a neobvyklé útoky. Jedním z prvních typů postranních kanálů, který využívaly tajné služby, byl „odposlech“ psaní na klávesnici mechanického psacího stroje (na zahraničních diplomatických zastoupeních). Zjistilo se, že každá klávesa má charakteristický zvuk, a že lze velmi jednoduše z akustického záznamu zjistit, co bylo na stroji psáno. Na tuto několik desítek let starou metodu se zapomnělo a byla oživena před několika dny (na Eurocrypt 2004) překvapivým výsledkem zmíněných kryptologů. Zjistilo se, že PC svými zvukovými projevy dává najevo jaké operace právě provádí.

1.9. Sledování osob a vozidel

1.9.1. Sledování osob

Za základ objektové bezpečnosti lze považovat nutnost mít přehled o osobách, které se pohybují po vašem objektu.

1. Kombinace radiových čipů (RFID) a bezdrátové wi-fi sítě umožňuje podle sledování osob nebo předmětů v reálném čase. Tato technologie pomůže například při požáru nebo jiném nebezpečí v areálu univerzity.

Systém totiž on-line informuje o poloze lidí vybavených odpovídajícím zařízením. Tento systém dokáže sledovat objekty nebo lidi. Bateriemi napájené RFID čipy jsou umístěny například na zboží a komunikují s nejméně třemi přístupovými body bezdrátové sítě. Právě tři přístupové body jsou k vypočítání polohy dostačující. Čipy jsou vybaveny softwarem, který vyhodnotí sílu signálu z různých přístupových bodů. Informace jsou posílány na server, kde se modeluje pohyb objektů na základě změn síly signálu z čipů. Aby systém bez problémů fungoval, musí být sledovaná stavba nebo monitorované území vybaveno bezdrátovou sítí, a to přesně kalibrovanou a zmapovanou.
Má-li systém fungovat efektivně, musí být na každých třiceti metrech přístupový bod. Za těch podmínek Siemens garantuje určení polohy předmětu nebo člověka s přesností jednoho metru.

2. Docházkové systémy, které mohou být doplněny různými druhy vstupníků (karty, přívěšky, PIN kódy...).
3. Kamerové systémy (systémy CCTV) mohou být doplněny speciálními zařízeními vyhledávajícími shodu se záznamy nacházejícími se v příslušné databázi.
4. Vizuální pozorování – klasickými dalekohledy, infračervenými kamerami, noktovizory (dalekohled pro noční vidění), fotoaparáty s teleobjektivy.
5. Sledováním detektivem.
6. S využitím jeho mobilního telefonu.
7. Akustické sledování.
8. Využití detektorů EZS.
9. Pachové pozorování.

1.9.2. Sledování vozidel

Získat přehled o vozidlech vjíždějících či vyjíždějících z areálů firem, podniků a úřadů je dnes naprosto nevyhnutelné. Kromě informací o cizích vozidlech je však nutné monitorovat pohyb svých vlastních služebních vozidel. Nebyli bychom asi Češi, pokud bychom se nesnažili využít například sklápěcí TATRU k nějaké té fušce, při které dovezeme sousedovi třeba písek. Co na tom, že naftu platí náš zaměstnavatel a že peníze za dopravu si jaksi ponecháme my.
Ke sledování vozidel lze využít:

1. GPS přijímač
   a) bez vysílacího modulu (nutno stáhnout data a vyhodnotit na počítači);
   b) s vysílacím modulem (rádio, mobil);
2. lokalizace vozidla pomocí mobilního telefonu;
3. vysílače elektromagnetických vln (zaměření);
4. radaru;
5. sledování pomocí jiného dopravního prostředku (auto, motocykl, letadlo, loď...).

1.10. Kontrola řádného využití pracovní doby

Lidská práce se v posledních desetiletích stává pro firmy významnou položkou v jejich nákladech. Právě proto se manažeři takových firem snaží o její maximální využití a pro lelkování a nicnedělání jaksi nemají pochopení.

Jenže nad každým zaměstnancem nemůže stát „policajt“ a když víme, že kontrola chybí rozhodně své pracovní nasazení nepřeháníme.

Jak tedy zaměstnavatel může kontrolovat své zaměstnance:

1. software monitorující práci na PC (internet, hry...);
2. docházkové systémy;
3. multifunkční karty (průkaz zaměstnance);
   a) hardwarový klíč;
   b) přístupový vstupník (dveře);
   c) elektronická peněženka (platby za oběd);
4. kamerové systémy (systémy CCTV);
5. přidělování pořadových čísel (přepážky na úřadě).

1.11. Zamezení komunikace mobilními telefony

V některých objektech je zapotřebí zajistit nemožnost fungování mobilních telefonů. Jako příklad mohu uvést objekty věznic. Z hlediska zákona o elektronických komunikacích je nasazení takové techniky velice problematické, neboť legální použití rušiček mobilních telefonů nesmí negativně ovlivňovat okolí takto zajištěného objektu. Většina soukromých firem si však s tímto problémem hlavu příliš neláme a při jejím jednorázovém použití má velkou šanci uniknout postihu Českého telekomunikačního úřadu.

Rušička mobilních telefonů – GSM JAMMER pro 3 pásma

Tento nenápadný malý přístroj spolehlivě ochrání byt, nebo kancelář proti nežádoucímu odposlechu formou zapnutého mobilního telefonu, nebo jiného zařízení, které pracuje na frekvencích používaných pro GSM přístroje (např. GSM pagery, nebo zabezpečovací systémy s přenosem informace o napadení GSM cestou), tedy znemožní i lokalizaci polohy vašeho mobilního telefonu...

Jeho účinek v blízkém okolí je takový, že mobilní telefony nemají signál, nelze provádět hovory, ani přijímat a odesílat SMS zprávy, MMS, používat GPRS, lokátory polohy apod.

1.12. Odhalování plagiátu prací na VŠ

Odhalování plagiátů nebo ochrana autorských práv je letité a stále aktuální téma, které získalo na intenzitě a významu právě s rozvojem informačních technologií, zejména s rozvojem elektronické podpory výuky a ukládáním závěrečných prací do studijních systémů.

Masarykova univerzita jako první vysoká škola v České republice zavedla nový systém kontroly plagiátorství bakalářských, diplomových prací, ale též „obyčejných“ seminárních prací. V případě prokázání plagiátorství čeká studenta bezpodmínečný „vyhazov“ z vysoké školy.