Crypto-World

Informační sešit GCUCMP

ISSN 1801-2140

Ročník 10, číslo 11/2008 **15. listopad 2008**

11/2008

Připravil: Mgr. Pavel Vondruška

Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1304 registrovaných odběratelů)

Obsah :

A. Podzimní *Soutěž v luštění 2008* skončila

Pavel Vondruška (pavel.vondruska@crypto-world.info)

Soutěž v luštění 2008 (http://soutez2008.crypto-world.info/), která byla doprovázena příběhem Johna Wellingtona a byla spojena s luštěním důležité zprávy zaslané šifrátorem Lorenz SZ40, přesně po jednom měsíci bojů skončila. Možnost vkládat správné výsledky řešení jednotlivých úloh byla uzavřena dnes (15.11.2008) ve 14.00 hod.

Stručná statistika letošní soutěže:
Celkem soutěžících: 120
Počet soutěžících, kteří vyřešili aspoň 1 úlohu: 90
Počet soutěžících zařazených do slosování: 55

Úlohy
Celkem publikovaných úloh: 15
Maximální počet bodů za publikované úlohy: 80

Ceny pro vítěze a vylosované hráče

Všechny úlohy letos vyřešili pouze 4 soutěžící (!):

1 ony 80 08.11 (21:47)
2 MD5Mir 80 09.11 (18:48)
3 koc 80 10.11 (06:29)
4 rhoracek 80 11.11 (22:26)

Redakční rada se proto rozhodla udělit ceny všem řešitelům, kteří zdolali všech patnáct soutěžních úloh a stejně jako hlavní postava příběhu John Wellington dešifrovali důležitou šifrovou zprávu (začátek jejího textu viz obrázek).

1.cena
Matyáš,V., Krhovják, J. a kol.: Autorizace elektronických transakcí a autentizace dat i uživatelů, Mas. univerzita, 2008
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros,
Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
SOOM tričko

2.cena
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
SOOM tričko

3.cena
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
David Meerman Scott: Nová pravidla marketingu a PR,. Zoner Press, 2008

4.cena
P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006
David Meerman Scott: Nová pravidla marketingu a PR,. Zoner Press, 2008

Další ceny pak obdrží ještě tito vylosovaní hráči (losovalo se ze všech hráčů, kteří dosáhli alespoň 15 bodů):

11 Snehurka 40 10.11 (19:24)
39 Senator 26 06.11 (18:39
51 Labakan 16 29.10 (19:59)

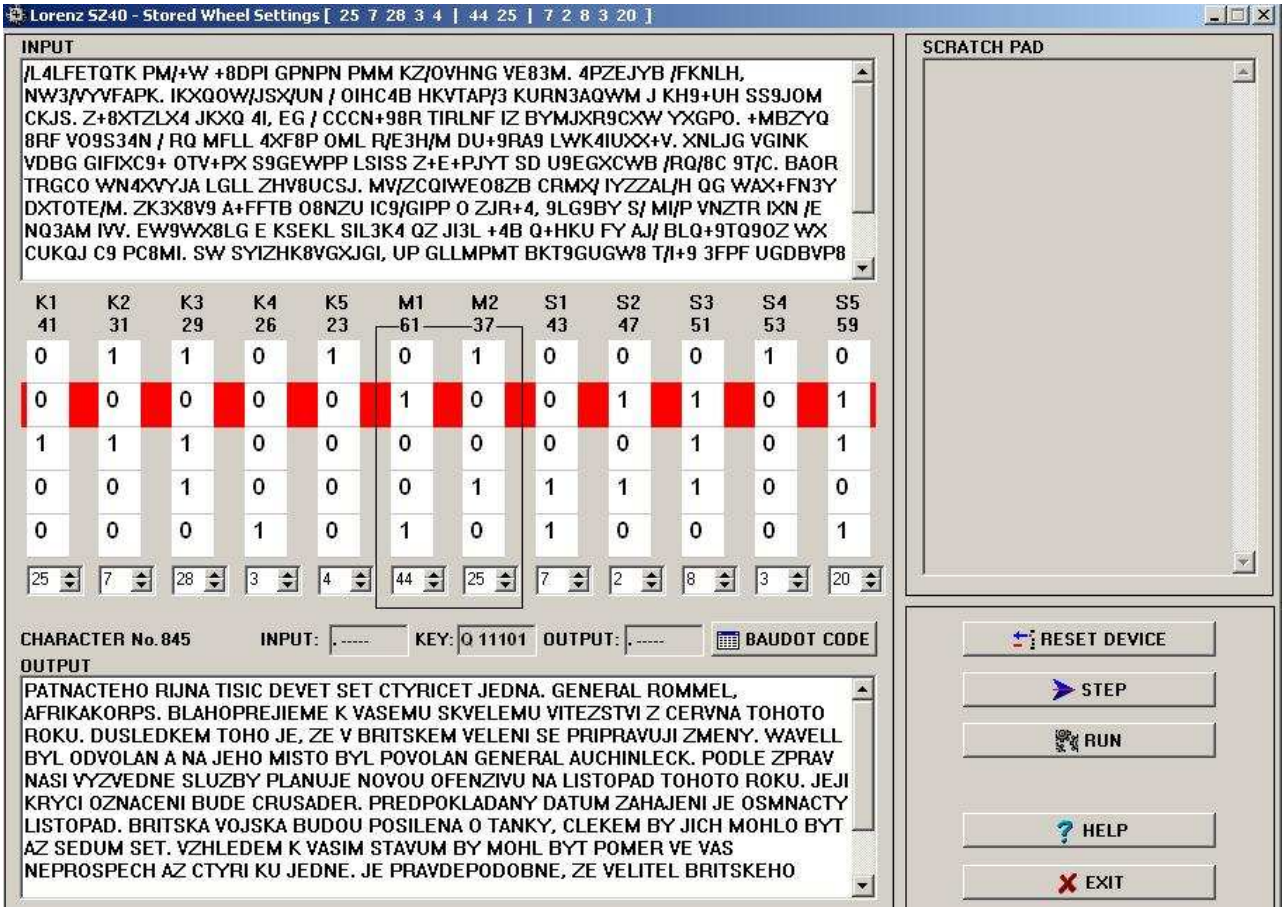
Ceny pro 3 náhodně vylosované řešitele

Snehurka: Jon Masters, Richard Blum: Linux PROFESIONÁLNĚ - programování aplikací, Zoner Press, 2008
Senator: David Meerman Scott: Nová pravidla marketingu a PR, Zoner Press, 2008
Labakan: P.Vondruška: Kryptologie, šifrování a tajná písma, edice OKO, nakladatelství Albatros, 2006

Děkuji sponzorům soutěže:

- Bezpečnostní laboratoř Brno, http://www.buslab.org/
- Zoner Press, http://www.zonerpress.cz/
- Soom.cz, http://www.soom.cz

Informace pro vítěze. V současné době se ještě čeká na dodání knih od firmy Zoner. Jakmile tato dodávka dorazí, budou ceny zkompletovány a ihned rozeslány!



Řešení všech úloh, včetně postupů a návodů na jejich luštění, budou uvedeny v prosincovém čísle 12/2008, které vyjde 15.12.2008.
Zatím jen stručný přehled správných výsledků, odkazů na vzorky kola a některých dalších detailů k použitým soutěžním šifrám:

úloha	body	slovo	Web
1	25	VYDRZTE	zpráva Lorenz SZ 40
2	1	LETO	http://sojka.cz/
3	1	DINOSAURU	http://www.nature.com/nature/journal/v416/n6878/extref/416314a-s1.doc
4	2	POZORNE	v každém příspěvku v Crypto-News , vpravo dole, vedle reklam Google (přesně news.doc)

5	2	BERGAMO	http://akce.nejlevnejsi-letenky.info/
6	3	ZJISTIT	http://www.linkbuilder.cz/
7	3	CVICNY	zpráva Lorenz SZ 40
8	4	NAVSTEVE	http://www.austerlitz-siberian.cz/kocouri.html
9	4	KOREN	http://root.cz/
10	4	CASOPISE	http://soom.cz/
11	3	RADY	WEB soutěže
12	4	PRACUJI	http://odvykani.cz/
13	3	JAPONSKA	http://www.itl.dm.u-tokai.ac.jp/~hiroshi/cgi-bin/crypto.cgi
14	6	PRIPRAVENI	zpráva Lorenz SZ 40
15	15	PROTEKTORAT	http://www.nbu.cz/ko/kontakty.php
CW	80		Crypto-World 10/2008

úloha	kolo	vzorek kol
1	šifrový text	úloha
2	29/3	10001000101010000111101010101
3	61/6 (1,0)	11111111100001110010010110000110?11010011?100110101110010100
4	47/9	01010101110101010100010101001001010010100101001
5	43/8	11100000110000010010100010010101001010101 00
6	53/11	01000011010100001010100001011100101000001110001010100
7	51/10	01001001110010110000011100010100010100100100 1010
8	23/5	10100001110100011110010
9	31/2	00101101000101010001011011 00100
10	41/1	11000111010101001110001001000100010010100
11	37/7	10001110001001110000100100100000100100
12	26/4	00000111000001111100001010
13		falešná stopa
14	59/12	00100001010010000001101001010110001100100001110001010100000
15	počáteční nasta-vení	25 7 28 3 4 44 25 7 2 8 3 20
CW	šifrátor	dodán s e-zinem Crypto-World10/2008

Úloha č.7 – konfigurace (vzorky kol + počáteční nastavení) shodná s příkladem, který je u simulátoru šifrátoru (zmugset.txt)
Úloha č.14 – konfigurace (vzorky kol + počáteční nastavení) : vzorky kol dle nastavení zmugset.txt, počáteční nastavení odvozené z hlavičky úlohy (nastaveni dle čísla telegramu 14/1141 z 8.11.1941 tedy: 14 1 1 4 1 8 1 1 1 9 4)
Úloha č.15 – konfigurace (vzorky kol + počáteční nastavení) vyluštěné vzorky kol (otazníky u vzorku 61/6 nahrazeny 0,1), počáteční nastavení odvozené z hlavičky úlohy (nastavení dle čísla telegramu 15/1141 z 8.11.1941 tedy: 15 1 1 4 1 8 1 1 1 9 4)
Úloha č.1 – konfigurace (vzorky kol + počáteční nastavení) vyluštěné vzorky kol (otazníky u vzorku 61/6 nahrazeny 1,0 !!!!), počáteční nastavení dle telefonu a faxu NBÚ (25 7 28 3 4 44 25 7 2 8 3 20)

Všem úspěšným řešitelům blahopřeji !

B. KYBERNETICKÉ ÚTOKY: RUSKO? – GRUZIE a SVĚT

Mgr. Tomáš Sekera, Security Director, Logica CEE,
(tomas.sekera@crypto-world.info)

Informační válka „INFOWAR“

Jedná se o soubor aktivit, často vzájemně zkoordinovaných co do cíle, místa a času, které slouží k vytěžení, znepřístupnění, pozměnění, poškození až likvidaci informací anebo jejich zdrojů, s cílem dosáhnout významné výhody v boji nebo vítězství na konkrétním protivníkem. Útoky nejsou jednotlivé, ale většinou kombinované, masivní a zasahující celé vybrané geografické území. Nezanedbatelný je rovněž dominový efekt takového útoku.

Infowar lze podle cílů kategorizovat např. tímto způsobem:

1. charakteristická infowar – omezení efektivní činnosti napadeného subjektu,
2. „hacktivism“ – použití metod hackingu k prosazení politických cílů, spočívající v degradaci či porušení obsahu informačního systému napadeného subjektu, který způsobí neschopnost činnosti subjektů na tomto informačním systému závislým anebo naopak vyvolá nežádoucí reakci na základě dezinformace, včetně šíření poplašných zpráv,
3. zpravodajský (skrytý) charakter napadení, smyslem je získání a analýza informačních zdrojů napadeného subjektu,
4. „perception management“ – vedená za účelem skrytého ovlivnění rozhodování nebo veřejného mínění na základě upravovaných informací,
5. pro úplnost – fyzická likvidace informačních prostředků pomocí bojové akce.

Mimo tyto sofistikované akce stojí tvz. elektroničtí sprejeři, výraz „vypůjčený“ od p. Vondrušky, kteří přepisují webové stránky čistě pro vlastní potěšení, jako důkaz své dovednosti překonat bezpečnostní opatření.

Informační válka v pojetí výše uvedených bodů 2-4 může zásadním způsobem přispět např. až k destabilizaci politické situaci v dané napadené zemi, ovlivnění volebních preferencí. Nástroje informačních technologií ve spojení s PR aktivitami poté dostávají naprosto jiný, silnější náboj. Stávají se rovněž účinným nástrojem propagandy, pozitivní i negativní.

Konflikt Gruzie - Rusko

(dále uváděná zjištění vycházejí z otevřených zdrojů)

Konflikt mezi Gruzií a Ruskem se vedl i na úrovni kybernetického prostoru. V současné době nelze s jistotou říct, jde-li o oficiální útoky vedené jednotlivými stranami na příkaz státní moci, nebo jen o méně či více organizované skupiny lidí – útočníků. Užití pojmu hacker v tomto případě nebylo úplně správným označením útočníka, neboť většinou nešlo o vlámání se do cizích systémů, ale jen o jejich napadení.

Provedení většiny útoků bylo metodou DDoS – tento způsob napadení vzdáleného systému neškodí systému samotnému, ale spíše využívá zahlcení služby, kterou systém provozuje a tím znemožní její normální fungování. Jako příklad lze uvažovat o napadení třeba domény www.www.com :
Útočník, který chce systém napadnout, ovládá tzv. C&C server (command and control). K tomuto serveru jsou pomocí tzv. Botnet sítě připojeni klienti, kteří vykonávají příkazy C&C

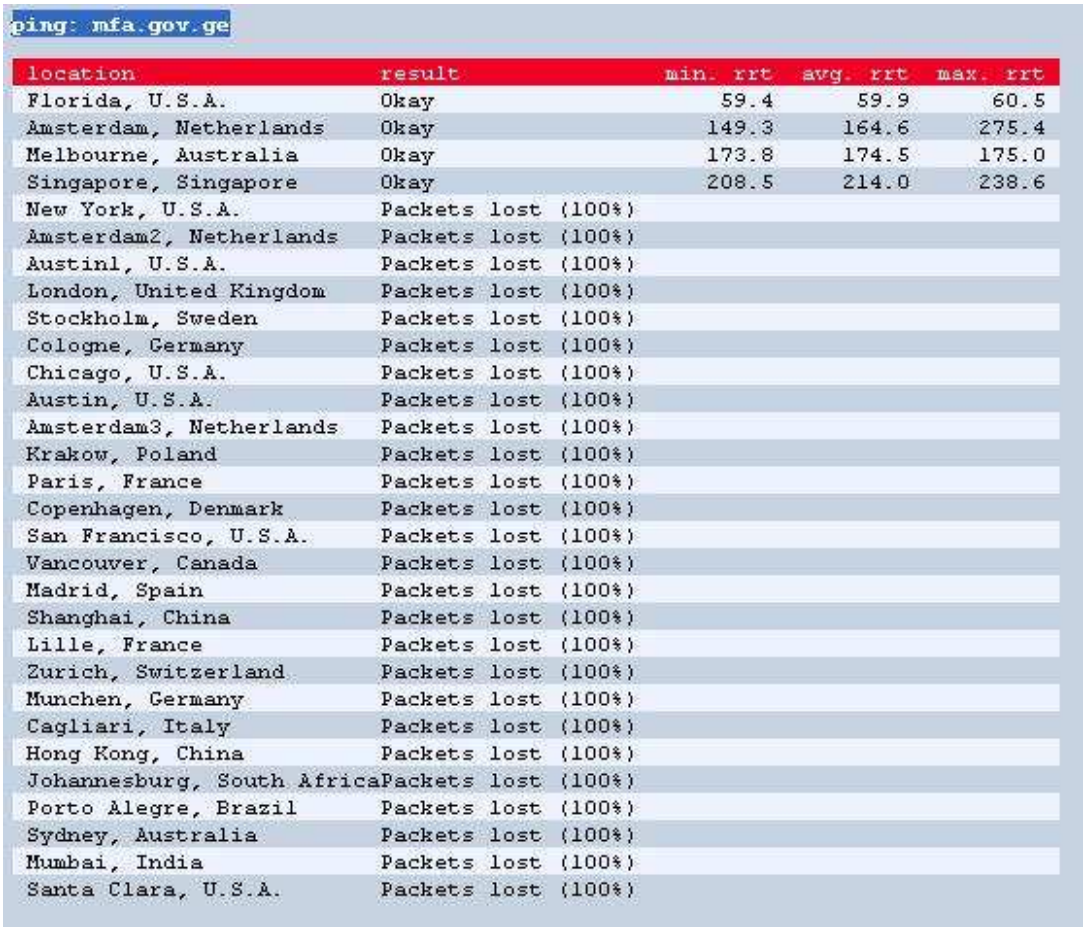
serveru. Těmito klienty mohou být nedostatečně zabezpečené stanice umístěné po celém světě, jejíž majitelé ani nevědí, že jejich počítač je připojen do Botnet sítě nebo, že napadá jiné systémy. Útočník vydá příkaz, aby se tyto počítače začali automaticky dotazovat webových stránek www.www.com na nesmyslné dotazy. Následkem toho webový server nestíhá odbavit všechny dotazy, neboť jich v krátkém období přichází velké množství a buď se zastaví anebo neodpovídá na dotazy regulérních návštěvníků. Tento typ útoku vyžaduje dostatečné množství klientů botnetu kteří útočí na napadený systém. Uváděná/odhadovaná cena takového útoku je 0.04 US Cent na jeden útočící počítač.

Útoky na gruzínské webové stránky probíhaly již od cca 19.-20. července 2008. Bezpečnostní experti z USA potvrzují rozsáhlé útoky na oficiální webové stránky Gruzie. Podle mluvčího Gruzínského velvyslanectví nabraly útoky vyšší obrátky v okamžiku napadení Jižní Osetije. Útokům z ruské strany předcházela distribuce veřejného seznamu vládních webových stránek po ruských fórech. Tímto způsobem byla zajištěna informovanost zejména ruský hovořících uživatelů Internetu, které webové stránky budou atakovány. Jednou ze skupin, která se podílí na kyber útocích, je stopgeorgia.ru, v případě nedostupnosti www.stopgeorgia.info . V další fázi došlo k distribuci velmi jednoduchého nástroje na http zahlcení zvolené IP adresy. O víkendu 9.-10. srpna byla většina gruzínských webových stránek nedostupná. Gruzie musela požádat o podporu z jiných zemí, aby mohla o vojenském zásahu informovat okolní svět pomocí Internetu. Většina webových stránek velkých firem a státních orgánů byla přesunuta na hosting do jiných zemí. Na základě napadení stránek prezidenta Saakašviliho (zobrazení fotografie Hitlera), které byly také přesunuty (USA - Georgie), lze nyní hovořit až o „otevřené válce mezi mocnostmi“, neboť američtí hackeři si toto nenechali líbit a provedli odvetné útoky na stránky umístěné v Rusku. Zároveň je ale nutné podotknout, že z pohledu míst zdrojů útoku se jedná o celosvětovou „válku“ neboť útočící počítače jsou z různých zemí světa.

Stojí Rusko opravdu za útoky v Gruzii?

Dle analýz U.S.CERT nejsou tyto kybernetické útoky součástí žádného většího plánu k napadení země. V minulosti se toto projevilo např. v Estonsku, Litvě a dalších zemích, které se jakýmkoliv způsobem dotkly cítění ruských hackerů. Nelze s jistotou potvrdit či vyvrátit, má-li Rusko či jiný stát organizovanou skupinu útočníků. Problematika cybercrime a zpravodajských her je kapitola sama pro sebe. Jako pravděpodobnější se vzhledem k charakteru útoku jeví možnost neorganizovaných skupin dostatečně kvalifikovaných (ale i nekvalifikovaných) jedinců, kteří berou útoky jako svou “vlasteneckou” povinnost ke svému státu a mohou se tak zapojit do samotného aktu kybernetické války. Dle informací z webových stránek zabývajících se touto problematikou je pravděpodobné, že za masivní částí útoku stojí skupina RBN (Russian Business Network). Nicméně je nutné na základě komplexního útoku a protiútoků připustit organizovanost těchto skupin.

Zda útočníky jsou hackeři izolovaní od státní moci, či při konkrétním napadení byla uplatněna státní vůle, může ukázat vyšetřování jednotlivých caus. Pravděpodobnějším se jeví, že fakta vyjdou najevo až otevřením archivů bezpečnostních složek, ovšem po uplynutí doby určené k možnosti zveřejnit jejich obsah. Z pohledu bezprostředního zajištění bezpečného Internetu není rozhodné, kdo jej napadá.



ping: mfa.gov.ge

location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	59.4	59.9	60.5
Amsterdam, Netherlands	Okay	149.3	164.6	275.4
Melbourne, Australia	Okay	173.8	174.5	175.0
Singapore, Singapore	Okay	208.5	214.0	238.6
New York, U.S.A.	Packets lost (100%)			
Amsterdam2, Netherlands	Packets lost (100%)			
Austin1, U.S.A.	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Stockholm, Sweden	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Austin, U.S.A.	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Paris, France	Packets lost (100%)			
Copenhagen, Denmark	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Vancouver, Canada	Packets lost (100%)			
Madrid, Spain	Packets lost (100%)			
Shanghai, China	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Zurich, Switzerland	Packets lost (100%)			
Munchen, Germany	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Hong Kong, China	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			
Sydney, Australia	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			

Obrázek převzat z článku: Coordinated Russia vs Georgia cyber attack in progress http://www.infowar-monitor.net/

Odvetné útoky Gruzie a její obrana

Gruzie provedla odvetné útoky na webové stránky ruských médií avšak s daleko menšími následky než pocítila sama. V současné době provádí Gruzie filtrování, cenzuru a monitorování internetu na úrovní ISP. Caucuses On-Line, největší Internet Service Provider, nemá díky omezením přístup k doménám s koncovkou ".ru" Podobný filtrovací systém byl zaveden i v GRENA (Georgian Academic and Research Network (obdoba naší akademické sítě). Není zřejmé, zda jde o rozhodnutí jednotlivých ISP nebo o součást státního plánu v případě ohrožení. Gruzie požádala o odbornou pomoc z okolních států. Polsko a Estonsko nabídlo Gruzii odbornou pomoc a kapacitu k přemístění důležitých internetových stránek. Dva z estonských odborníků CERT se vypravili do Gruzie, aby pomohli se zabezpečením internetové sítě v zemi. Estonsko tak pomáhá vytvořit jakousi kybernetickou alianci zemí, které byly napadeny ruskými hackery. Gruzie tvrdí, že nedošlo jen k napadení stránek prezidenta a státních institucí, ale také bankovního systém, který musel být na několik dní vyřazen. Většinu odborníků znepokojuje fakt, že za všemi útoky pravděpodobně stojí civilní skupiny hackerů a kybernetická válka se tak dostává do nové roviny. Nelze tedy obviňovat přímo jednotlivé státy, z nichž hackeři zřejmě pocházejí. Proto nelze ani požadovat nápravu stavu po těchto státech. Maximálně prevenci – jejíž návrh částečného řešení je dále uveden.

Zdroj: Moscow *Moskovskiy Komsomolets* in Russian 12 Aug 08 p3

Obrázek převzat z Information Warfare Monitor http://www.infowar-monitor.net/

Další související útoky v Gruzii

Došlo také k zneužití emailových adres gruzínských politiků, seznam byl původně vytvořen lobbistickou organizací. Emailové schránky byly zahlceny (SPAM) a cíleně byly podstrčeny URL s malware přes live exploity.

Byl zaznamenán útok na mobilní telefon gruzínského premiéra, který spočíval v zahlcení telefonu nesmyslnými textovými zprávami a voláním.

Dalším typem útoku bylo přerušení běžných komunikačních kanálů. Jedno z nejpopulárnějších hackerských fór v Gruzii bylo nedostupné 24 hodin pod stálým útokem DDoS, aby byla znemožněna komunikace mezi gruzínskými hackery.

Cílem útoků byla kompromitace několika vládních www stránek zejména:

- www.president.gov.ge
- www.rustavi2.com
- www.parliament.ge
- www.government.gov.ge/eng/
- www.mfa.gov.ge
- www.mod.gov.ge
- www.police.ge
- www.nsc.gov.ge
- www.mof.ge
- www.nbg.gov.ge

Cíle gruzínských hackerů:

- osinform.ru – jihoosetinská televizní a rozhlasová stanice
- osradio.ru – jihoosetinská televizní a rozhlasová stanice

Ovládací C&C servery jsou zejména:

79.135.167.22

- emultrix.org
- yandexshit.com
- ad.yandexshit.com
- a-nahui-vse-zaebalo-v-pizdu.com
- killgay.com
- ns1.guagaga.net
- ns2.guagaga.net
- ohueli.net
- pizdos.net

Symantec: Kybernetický útok na Litvu byl veden z Ruska

Společnost Symantec se prostřednictvím svého country managera pro ČR Radka Smolíka vyjádřila k červencovému (2008) koordinovanému kybernetickému útoku na několik tisíc litevských webových serverů, a to jak vládních institucí, tak i soukromých společností.

„Podle našich analýz, kterými disponujeme, se jedná s nejvyšší pravděpodobností o útok cíleně vedený z Ruska. To, že za útokem stojí ruští hackeři, potvrzuje i podvržený obsah plný komunistických a nacistických symbolů a nacionálních replik. Ostatně napjaté vztahy mezi Litevci a silnou ruskou menšinou žijící v Litvě tuto domněnku potvrzují."

Pravděpodobnou příčinou útoků je přijetí litevským parlamentem nového zákona (ze všech post-sovětských republik dosud nejpřísnější), který zakazuje a přísně trestá publikování komunistických a nacistických symbolů, jako jsou obrazy představitelů těchto režimů, emblémy, vlajky, odznaky a označení, ale také srp a kladivo nebo třeba svastika.

„Z politického hlediska má útok proti několika tisícům litevských webových stránek podobný charakter jako zhruba rok starý útok na Estonsko. Ten byl však svým rozsahem i dopadem mnohem citelnější. Značné dopady loňského útoku na estonský život byly zapříčiněny i velkým pokrokem v oblasti eGovernment, jehož Estonsko dosáhlo – a tím také podstatně větší závislostí na těchto službách."

Zdroj: *SecurityWorld/Internet*, rubrika On-line bezpečnost, 2.7.2008

Obrana – doporučení

Na základě zkušeností se jeví nejdůležitějším v případě napadení internetu takovým to masivním útokem jako v Gruzii, Litvě a Estonsku (dostupnost + integrita), zachovat plné fungování systémů informovanosti občanů, systémů včasného varování, podpůrných systémů kritické infrastruktury (ITC služby, doprava, energetika, finanční služby, vynucování práva, zdravotnictví, sociální zabezpečení, zajištění potravin a vody, ozbrojené síly). Jako malicherné se jeví řešit v danou chvíli nefunkční stránky prezentace hlavy státu (z pohledu

bezpečnosti státu nepřinášejí žádné relevantní informace). Jistě jde o prestižní záležitost, ale v době útoku je důležitější zachovat kritické systémy.

Jednou z cest, jak ochránit provoz vybraných veřejných služeb poskytovaných prostřednictvím Internetu, je přiřazení odpovídajícího technicko-organizační opatření na základě jejich kategorizace. Poskytovatelé těchto služeb přitom nejsou typicky subjekty zařazenými do systému krizového řízení, pro případ války a krizových stavů. Jedná se o běžné služby veřejnosti, jejichž nedostupnost ale způsobuje nemalé problémy – uživatelské, informační, potažmo i politické.

Katalog vybraných služeb by byl analogií, byť významově nižší, mezinárodního, či národního preferenčního schématu (přednostního spojení), kdy se jedná o souhrn technicko-organizačních opatření, která umožňují zařazeným uživatelům v období krizových stavů přístup ke službám elektronických komunikací v mezinárodním nebo národním provozu i v případech, kdy jejich poskytování je omezeno z důvodu narušení infrastruktury sítě nebo její neprůchodnosti. Ochrana by byla poskytována primárně službě, nikoliv subjektu, který ji provozuje, jakkoliv toto spolu úzce souvisí.
Dostupnost služeb zařazených v katalogu by tak byla zvýšenou měrou chráněna i v době mimo krizové stavy. Otázkou je, vzhledem k významu některých služeb, zda i za krizových stavů….

Klasické technické řešení

Státní instituce a významné soukromé subjekty mohou mít mimo vlastní izolovanou krizovou infrastrukturu jako obranu proti DDoS útokům při běžném provozu nasazeny filtry, jež omezí příchod ze shodných adres, či připraveny záložní servery, jež při zvýšeném zatížení převezmou další dotazy účastníků. Smyslem tohoto článku není prezentovat výčet technických možností obrany proti DdoS Attack.

V souvislosti s tímto typem útoků je nutné zmínit problematiku ochrany VoIP systémů. Stává se běžným trendem přechod firem a dalších subjektů na tento typ komunikace a v případě zahlcení serverů obsluhujících tyto služby by byla znemožněna jejich komunikace.

Řešení de lege ferenda

Stát (primárně člen EU – závaznost direktiv EU), pravděpodobně zastoupený regulátorem pro oblast elektronických komunikací, může mít, jako součást krizového řízení připraven projekt, kdy ISP budou povinni průběžně, či na výzvu filtrovat určité IP adresy. V době masivního napadení Internetu by byly řízeně dostupné jen vnitrostátní adresy a případně adresy okolního světa, které by byly určeny k předávání informací. Tento „White list“ by bylo nutné neustále udržovat aktuální na základě vznikajících nebo zanikajících informačních systémů v prostředí Internetu. Díky této metodě by se velice omezila možnost DDoS útoku na ohrožené servery bez zásahu vlastníka serveru. Ovšem cenou za takové řešení by byla dočasná nedostupnost a snížený komfort služeb poskytovaných prostřednictvím Internetu, oproti době mimo útok. K takovému kroku je nutná mj. změna příslušné národní legislativy, spočívající v uložení povinnosti monitoringu a nastavení flitrů provozu pro ISP,

dále v povinnosti pro regulátora tuto oblast nad rámec krizového řízení kontrolovat a plnění povinností vyžadovat. V neposlední řadě by bylo nutné řešit i otázku souvisejících nákladů.

White list by ovšem mohl vzniknout i na základě dobrovolnosti, resp. komerčních dohod mezi ISP a jeho klienty s chráněnými zájmy - službami. Jednalo by se o z pohledu práva dobrovolné zavedení restrikcí nežádoucího provozu, v návaznosti na podmínky vyplývající z národních a mezinárodních propojovacích smluv a smluv o přístupu k sítím elektronických komunikací a přiřazeným prostředkům.

Poškozený by se následně při nedostupnosti služby z důvodu nezajištění přiměřené bezpečnosti mohl dožadovat nápravy přímo u ISP (jakkoliv se ISP obecně v jejich všeobecných podmínkách nyní předem vyviňují z nedostupnosti služby cizím zaviněním), jež by tak byl nucen na základě smluvního závazku nebo zákonné povinnosti konat a předcházet takovým nežádoucím stavům, např. navrhovaným monitorováním a filtrováním provozu.

Obchodní model naprosté regulace vs. model dobrovolnosti (smluvního vztahu ISP/uživatel), lze pro danou situaci kombinovat i regulací částečnou. Regulován by příslušným způsobem byl pouze povinný obsah smluv o propojení a o připojení, kdy by ISP měl povinnost zavést monitor a filtr, současně s právem nežádoucí provoz přerušit.

Ale již v současné době je možno uvažovat také o uplatnění náhrady vzniklé škody stranou poškozenou (spotřebitelem/uživatelem) přímo na ISP. Využívání tohoto právního prostředku, resp. navazujících soudních rozhodnutí (precedentů) by mohlo být spouštěcím impulsem a přispět k systematickému a preventivnímu řešení situace, ze strany samotných ISP. Uživatel služby nemůže totiž situaci příliš ovlivnit a dle mého názoru není ani možné po něm spravedlivě požadovat zajištění takové ochrany vlastními prostředky. Zde je patrná jistá analogie s užíváním služeb elektronického bankovnictví, kdy povinnost zajistit bezpečnost v této rovině je jednoznačně přenášena na poskytovatele služeb – banky, čemuž v prostředí ČR svědčí rozhodnutí finančního arbitra.

Pokud navrhovaná řešení shrneme – bezpečnost internetu je záležitostí všech zúčastněných a je žádoucím „do hry“ vtáhnout zvláště poskytovatele služeb elektronických komunikací, ať již formou úplné, či částečné regulace anebo formou zvláštní bezpečnostní služby poskytované ISP za úplatu (garance dostupnosti). Tlak ovšem musí primárně vzejít ze strany poškozených nebo ohrožených uživatelů, kterými jsou stát, právnické i fyzické osoby.

Poznámka na závěr. Existuje celá řada aktivit mezinárodních organizací a států, spojených s kritickými infrastrukturami. V Evropě se jedná zejména o ITU, G8, IOCE/HTC, OECD, GTSC, GRSC, IEFT, ETSI. V Kanadě vytvořil ministerský předseda Úřad pro ochranu kritických infrastruktur spadající pod obecnou pravomoc ministra národní obrany. Ve Spojených státech je vytvořen Prezidentské rady pro ochranu kritických infrastruktur. Problematika je pochopitelně řešena i na úrovni vojenské (NATO a další).

C. Kvantový šumátor ve Společné laboratoři optiky UP a Fyzikálního ústavu AV ČR

RNDr. Jaroslav Hrubý, CSc., Fyzikální ústav v.v.i. AV ČR,
(hruby@fzu.cz)

Úvod

Ve Společné laboratoři optiky University Palackého v Olomouci a Fyzikálního ústavu v.v.i. Akademie věd ČR v Praze (dále jen SLOUP) byl vyvinut unikátní kvantový generátor náhodných čísel, který představuje špičku mezi hardwarovými generátory ve světě.
Tyto hardwarové fyzikální generátory náhodných čísel mohou být založeny na nejrůznějších fyzikálních procesech.
Jde přitom o to, aby samotný proces generování byl náhodný, a to ve smyslu nepředpověditelnosti výsledku jeho individuální realizace a vzájemné nekorelovanosti takovýchto individuálních realizací. Tato náhodnost může být:

- praktická, kdy systém je sice po teoretické stránce považován za deterministický, ale je popsán mnoha (často neúplně známými) parametry a obvykle není přesně znám jeho počáteční stav (nebo je technicky obtížné jej připravit opakovaně ve stejném počátečním stavu, příkladem takového generátoru náhodných čísel je třeba ruleta), dalším příkladem může posloužit tzv. deterministický chaos, který je generovaný nelineárním disipativním dynamickým systémem, někdy se hovoří také o kvasináhodném procesu,
- fundamentální, kdy náhodnost je zahrnuta přímo ve fyzikální podstatě jevu a jev je jako náhodný popsán i fyzikálními zákony.

Skutečná fundamentální náhodnost je garantována v kvantové fyzice. Právě v oblasti kvantové fyziky existuje celá řada jevů, které jsou náhodné ze své samotné podstaty. Zákony kvantové fyziky popisují chování souborů kvantových objektů, nejsou ale, vyjma speciálních případů, schopny předpovědět s určitostí chování individuálního kvantového objektu; předpovídají pouze pravděpodobnosti, s jakými nastane ten či onen konkrétní jev.
Důvodem přitom není, jak dnes dotvrzuje velké množství experimentálních dat, momentální neznalost jakýchsi „skrytých“ parametrů, ale jde o skutečně fundamentální vlastnost mikrosvěta, kterou nelze nijak obejít!
To poskytuje velmi dobrý prostor pro konstrukci generátoru náhodných čísel, splňujícího nejpřísnější kritéria vyžadovaná právě např. kryptologickými aplikacemi.

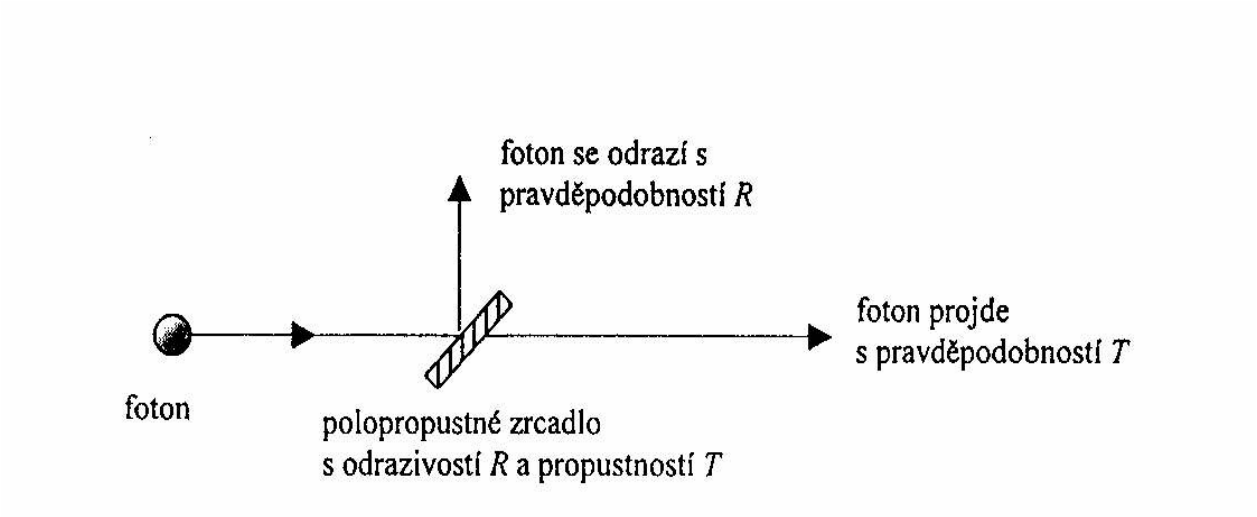
Vybereme-li nějaký elementární kvantový proces, který jsme schopni dobře teoreticky analyzovat, tj. určit pravděpodobnosti všech jeho možných výsledků, a jsme-li schopni takový proces opakovaně za dobře definovaných podmínek realizovat, můžeme jej použít jako základ pro generaci náhodných čísel.

Zvolený fyzikální proces ve SLOUP

Dělení světla na děliči svazku

Jedním z elementárních kvantových procesů je dopad světelného kvanta – fotonu na tzv. dělič svazku. Jedná se o zařízení, které se v klasické optice používá k rozdělení jednoho svazku světla na svazky dva. Může jít např. o tzv. polopropustné zrcadlo, existuje však i řada jiných konkrétních realizací tohoto prvku. Zajímavé pro nás je, že snižujeme-li intenzitu

světla, začne se projevovat jeho kvantový charakter. Světelná energie se totiž šíří v malých nedělitelných dávkách – fotonech. Dopadne-li jediný foton na dělič svazku, nemůže se rozpůlit; může prostě jen „zvolit“ jednu ze dvou možných cest. Foton ale není kulečníková koule, to, kterou cestou se vydá, je náhodný jev v nejryzejším smyslu.



Takový proces poskytuje několik výhod:

1. jde o jednoduchý, dobře teoreticky popsatelný proces, který poskytuje dvě hodnoty možných výsledků při dopadu jednoho světelného kvanta na dělič svazku,
2. jde o proces dobře experimentálně realizovatelný (dílčí problémy s jeho realizací jsou popsány dále) a kontrolovatelný,
3. výsledek procesu je snadno detekovatelný a dobře převoditelný do elektronické formy k další zpracování,
4. technologie k praktické realizaci je dostupná na komerční úrovni.

Přes jednoduchost zvoleného procesu vyžaduje jeho laboratorní realizace s ohledem na předpokládané aplikace řešení několika dílčích problémů. Ty budou popsány v následujících odstavcích. Do hry v celém experimentálním řetězci vstupuje mnoho dalších náhodných procesů, jejichž vlastnosti nejsou přesně známy. Jejich vliv by tedy měl být eliminován nebo aspoň omezen na minimum, aby výsledky generátoru vycházely z jediného, dobře kontrolovaného a z fyzikálního hlediska fundamentálního náhodného procesu.

Příprava počátečních stavů

Především v současné době není znám způsob, jak opakovaně a kontrolovatelně připravovat jednofotonové stavy světla. Poměrně snadno lze však vytvořit jejich napodobeninu v podobě silně zeslabených laserových pulsů, které vykazují poissonovskou statistiku v počtu fotonů obsažených v pulsu, tj. pravděpodobnost, že puls obsahuje *n* fotonů lze psát jako:

$$p(n) = \frac{\alpha^n}{n!} e^{-\alpha},$$

kde α je střední počet fotonů v pulsu. Tedy např. pro $\alpha = 0{,}1$ dostáváme pravděpodobnosti:

$$p(0) = 90{,}5\ \%,$$
$$p(1) = 9{,}0\ \%,$$
$$p(>2) = 0{,}5\ \%,$$

neboli devět z deseti pulsů neobsahuje žádný foton a přibližně každý dvacátý neprázdný puls obsahuje více než jeden foton. Případy, kdy nedojde k detekci na žádném z výstupů nebo kdy dojde k detekci na obou výstupech, nejsou pro generaci náhodných čísel použitelné.

Vzniká tedy otázka, **jaká intenzita (střední počet fotonů) vstupního stavu je optimální.** Pravděpodobnost, že detektor nezaregistruje žádný foton, je $p_0=e^{-\alpha/2}$ (je-li dělič vyvážený [*R=T],* pak na obou jeho výstupech je střední počet fotonů poloviční než byl na vstupu). Tedy pravděpodobnost, že nebude detekován foton ani na jednom výstupu $p_{00} = p_0^2 = e^{-\alpha}$, pravděpodobnost, že bude detekován foton na obou výstupech $p_{DD} = (1-p_0)^2 e^{-\alpha/2}$.

Pak pravděpodobnost, že puls neposkytne výsledek použitelný pro generaci náhodných čísel, $p_{00}+ p_{DD}$, nabývá minimální hodnoty pro střední počet fotonů vstupního pulsu $\alpha= 2 \ln 2 = 1{,}39$ fotonu na puls. V tom případě bude puls použitelný s pravděpodobností $1 - p_{00} - p_{DD} = 0{,}5$.

Dalším důležitým problémem je **otázka vzájemné nekorelovanosti individuálních realizací** tohoto jevu. Z hlediska fyzikálního popisu se předpokládá, že mezi následnými individuálními realizacemi je celý experimentální systém uveden do téhož počátečního stavu, který je zcela nezávislý na předchozích realizacích jevu. To lze velmi dobře předpokládat u samotného děliče svazku, který představuje klasické (makroskopické) zařízení, které vystupuje v celém procesu jen ve funkci parametru, předpokládá se, že interakce s fotonem dělič téměř neovlivňuje a změna jeho stavu je zanedbatelná. Pokud jde o vlastnosti zdroje fotonů, lze pro naši praktickou realizaci rovněž předpokládat, že jeho vlastnosti jsou na časových škálách generace fotonů (10^{-4}-10^{-15} s) konstantní. Máme na mysli zejména střední frekvenci fotonů a polarizaci. Na obou těchto veličinách totiž obecně závisí dělicí poměr děliče svazku a případné změny vlastností zdroje na těchto škálách by mohly vnést do generované náhodné sekvence nežádoucí korelace. V případě detektorů největší nebezpečí plyne z tzv. „afterpulsů“, tj. u detektoru, který zaznamenal detekci, se zvyšuje pravděpodobnost, že zaznamená „falešnou detekci“ (temný puls). Toto nebezpečí je minimalizováno na zanedbatelně malou úroveň pomocí detekční elektroniky.

Kontrola procesu dělení pulsu

Dalším faktorem, který je třeba experimentálně kontrolovat, je rovnovážnost generátoru, tj. zajištění toho, aby počet generovaných nul a jedniček byl s vysokou přesností stejný. Není totiž triviální zajistit, aby dělicí poměr děliče (spolu s detekční účinností detektorů) byly stabilně nastaveny na stejnou pravděpodobnost detekce na obou detektorech s přesností výrazně lepší než 1 %.

Jednou z možností jak tento nedostatek zmírnit je použít techniku tzv. **XORování**. Touto metodou vytvoříme jeden náhodný bit vždy ze dvou po sobě následujících úspěšných (detekce buď na detektoru A nebo na detektoru B) realizací experimentu podle následujícího klíče:

2. realizace	*1. realizace*	*výsledný bit*
A	A	0

B	A	1
A	B	1
B	B	0

Pak pravděpodobnosti generace bitů 0 a 1 jsou ($p_A = 1 - p_B$):

$$p_0 = p_A p_A + p_B p_B = 1 - 2 p_A (1- p_A),$$
$$p_1 = p_A p_B + p_B p_A = 2 p_A (1- p_A).$$

Pokud např. $|p_A - 1/2| = 1$ %, pak $|p_0 - 1/2| = 0{,}04$ %. Tohoto zlepšení se ale dosahuje na úkor snížení rychlosti generace na jednu polovinu.

Pro uvažované kryptologické aplikace by však ani takové zlepšení nemuselo být dostatečné. Proto využíváme následující **metodu vyvážení generátoru, pocházející od von Neumanna.** Opět je vytvořen jeden logický náhodný bit vždy ze dvou po sobě následujících úspěšných realizací experimentu. Dvojice AA a BB však jsou vyřazeny a dvojice AB a BA použity podle následujícího klíče.

2. realizace	*1. realizace*	*výsledný bit*
A	B	0
B	A	1

Při této metodě se sice rychlost generace náhodných bitů sníží v průměru na jednu čtvrtinu, ale platí $p_0 = p_1 = p_A p_B$ (pro libovolné $= p_A p_B$).

Aby se eliminoval vliv potenciálních dlouhodobých pomalých (např. teplotních) změn detekčních pravděpodobností p_A a p_B, započítávají se dvojice AB, resp. BA, pouze tehdy, leží-li odpovídající detekce uvnitř zvoleného časového intervalu.

Detekce

Detektory pro detekci jednotlivých fotonů nemají ideální (100%) detekční účinnost, navíc detekční účinnosti u dvou detektorů použitých na výstupech děliče svazku nemají v praktickém systému stejnou hodnotu. Pro tuto aplikaci lze však v konkrétním systému zahrnout hodnoty detekčních účinností do dělicího poměru, tj. vyvážit nerovnovážnost detekčních účinností nastavením dělicího poměru děliče svazku tak, aby pravděpodobnost detekce na obou detektorech dosahovala potřebné hodnoty (zpravidla požadujeme stejnou pravděpodobnost detekce na obou detektorech).

Detektory vykazují dva druhy „falešných detekcí“, tj. poskytují elektronický puls i v případě, že na ně nedopadl žádný foton měřeného signálu:

a) Temné county: jednak to mohou být termální děje v lavinové fotodiodě, jednak šumové fotony vstupující do zařízení z jiných zdrojů než signálový laser. Množství termálních countů se omezuje termoelektrickým chlazením a volbou dostatečně krátkého detekčního časového okna (námi používané detektory vykazují 30-100 temných countů za sekundu, což při detekčním okně 10 ns širokém dává pravděpodobnost zachycení temného countu $<10^{-6}$).
b) Afterpulsy: po dopadu pulsu na detektor a detekci fotonu se zvyšuje pravděpodobnost vyslání falešného pulsu v důsledku nedokonalého návratu detektoru do základního stavu. Toto nebezpečí se eliminuje dostatečně dlouhou prodlevou mezi po sobě následujícími detekcemi. (V našem případě je opakovací frekvence omezena na 100kHz jinými faktory, což činí výskyt afterpulsů zanedbatelně malým.)

Generace dat

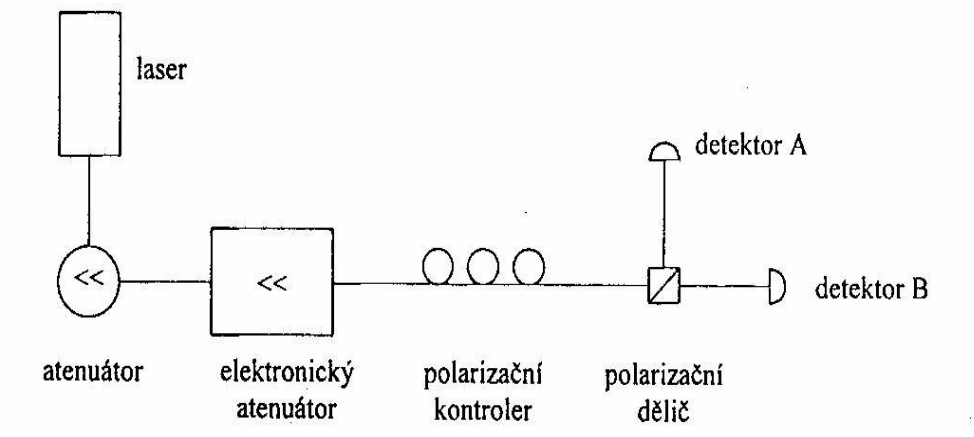
Technické možnosti, tj. maximální opakovací frekvence laserových pulsů, rychlost detekce (daná mrtvou dobou detektorů) a rychlost návazné detekční elektroniky, omezují maximální rychlost generace náhodných bitů. Největší omezení je na straně detektorů (doba nutná na uhašení lavinového procesu a vyčištění PN-přechodu) a především v detekční elektronice (zpracování obvody TAC a SCA a transfer dat do PC). Naše zařízení může pracovat s opakovací frekvencí laseru kolem 100 kHz. Pouze asi polovina pulsů bude správně detekována (nepoužijí se případy, kdy došlo k detekci na obou detektorech nebo na žádném z nich). Z úspěšných detekcí bude dál zužitkována asi čtvrtina (viz předchozí výklad). Lze tedy očekávat něco kolem 10 000 náhodných bitů za sekundu. Skutečné hodnoty v provedeném experimentu jsou 11 500 bitů za sekundu, tj. přibližně 5 megabyte za hodinu.

Vzhledem k tomu, že chyba odchylky průměru od ½, tedy veličiny $\left|\frac{1}{2} - \frac{\sum x}{n}\right|$, činí pro binomické rozdělení $\frac{1}{2\sqrt{n}}$, je pro potvrzení rovnováhy nul a jedniček s přesností např. 10^{-5} nutné vygenerovat nejméně 10^{10} bitů náhodných dat. To při dané rychlosti zařízení (v naší laboratorní realizaci) zabere asi 10 dní. Omezení rychlosti však není fundamentální, týká se dané laboratorní realizace a použitých komponent.

Experimentální realizace ve SLOUP

Experimentální uspořádání

Schéma optické části experimentálního uspořádání je načrtnuto na následujícím obrázku. Zdrojem pulsů je polovodičový laser pracující na vlnové délce 830 nm, který je schopen generovat pulsy 400 ps až 4 ns dlouhé s opakovací frekvencí 100 Hz až 1 MHz. Každý puls obsahuje řádově 10^8 fotonů. Pulsy jsou zeslabeny nejprve mechanickým atenuátorem a poté je střední počet fotonů nastaven elektronických atenuátorem tak, aby součet intenzit na obou detektorech odpovídal vstupní intenzitě před děličem svazku 1,38 fotonu na puls. Dělič svazku s měnitelným dělicím poměrem je zkonstruován pomocí dvojice prvků – polarizačního kontroléru a polarizačního děliče svazku. Nastavením polarizačního stavu na vstupu polarizačního děliče lze dosáhnout libovolného dělicího poměru. Výstupy děliče svazku jsou sledovány detektory založenými na lavinových fotodiodách s kvantovou účinností okolo 50% na 830 nm.



Signály z detektorů jsou zpracovány pomocí detekční elektroniky sestávající z převodníků čas- amplituda a z jednokanálových analyzátorů, jejichž výstupy jsou sledovány z řídícího PC, které rovněž zajišťuje řízení elektronického atenuátoru, spouštění laseru a synchronizaci celého zařízení.

Experimentální výsledky

Na zařízení zkonstruovaném podle výše popsaného schématu byla provedena generace náhodných posloupností bitů oběma způsoby popsanými v části 1.2, tj. metodou XORování i von neumannovskou metodou.

V případě generace pomocí XORování bylo dosaženo rychlosti generace 22,1 kbit/s. Dělicí poměr děliče svazku v průběhu měření kolísal v rozmezí 50,7:49,3 až 51,8:48,2 (typický průběh těchto změn lze vidět na následujícím obrázku) s průměrnou hodnotou 51,3:48,7. Metodou XORování by mělo dojít k vyvážení na hodnotu 50,03:49,97 (na vzorku 240 Mbit).

Von neumannovská metoda při podobném kolísání dělicího poměru teoreticky garantuje zcela vyvážený generátor.

Na vzorku dat získaných von Neumannovou metodou (výběr ze souborů Vn000-Vn073 na CD) byla zjištěna odchylka průměru od ½ o velikosti $4{,}8.10^{-5}$. Tato odchylka je menší než předpokládaná statistická fluktuace průměru ($8{,}6.10^{-5}$).

Závěr hodnocení dat z kvantového šumátoru

Zařízení ve SLOUP funguje stabilně a je schopno generovat kvalitní náhodná data vhodná pro kryptografické aplikace, a to nejen ve státní sféře (NBÚ, silová ministerstva apod.), ale i ve sféře komerční (banky apod.). Na zařízení se dařilo dobře kontrolovat všechny klíčové parametry a omezovat vnější rušivé vlivy. Výhodou zařízení je lehká ovladatelnost.
Posuzováno podle průběžně prováděných testů rovnováhy nul a jedniček, jeví generovaná data poměrně dobrou kvalitu (odchylky leží v rozsahu statistických chyb). Zařízení splňuje všechny dostupné kryptografické testy na generátory náhodných čísel.

Zařízení bylo testováno v rámci projektu registrační číslo **1ET300100403:**
APLIKACE KVANTOVÉ INFORMATIKY NA BEZPEČNOST PKI

Jsme přesvědčeni, že zařízení najde uplatnění v rámci ČR nejen ve státní a komerční sféře, ale může sloužit jako etalon pro srovnávání kvality náhodných dat vygenerovaných jinými hardwarovými generátory.

D. Mikulášská kryptobesídka 2008 / SantaCrypt 2008

http://mkb.buslab.org/

POZVÁNKA

Vážené kryptoložky a vážení kryptologové,

srdečně Vás zveme na 8. ročník českého a slovenského workshopu Mikulášská kryptobesídka, který se uskuteční ve dnech 4. a 5. prosince 2008 v hotelu Olympik v Praze.

Setkání pořádá TNS, a.s. (http://www.tns.cz/) a BUSLab (http://www.buslab.org/) za podpory ANECT a.s. (http://www.anect.cz/).

Na workshopu zazní mimo jiné zvané příspěvky významných zahraničních odborníků:

- Eli Biham (Technion, Haifa, Israel)
- Gilles Brassard (Universite de Montreal, Canada)
- Richard Clayton (University of Cambridge, UK)

Zájemci o krátké vystoupení v rámci Rump Session se mohou i nadále hlásit e-mailem na adrese matyas@fi.muni.cz .

Těšíme se na setkání s Vámi a připomínáme, že poslední **termín včasné registrace je 18. 11. 2008.**

Akce je otevřená každému, kdo se o tuto oblast zajímá!!!

Předběžný program workshopu přikládáme.

Za organizační a programový výbor
Vašek Matyáš a Zdeněk Říha

Program

4. prosince 2008 (čtvrtek) / December 4, 2008 (Thursday)

8:45 –	*Registrace / Registration*
9:30 – 9:40	*Zahájení workshopu / Workshop opening*
9:40 – 10:40	*Keynote* Eli Biham – On the (in)security of the ciphers and protocols of GSM
10:40 – 11:40	*Keynote* Richard Clayton – Can cryptography secure the Internet?

11:40 – 12:25	Piyi Yang – An ID-based threshold broadcast encryption scheme for key distribution in mobile ad hoc networks
12:30 – 13:30	*Oběd / Lunch*
13:30 – 14:30	*Keynote* Gilles Brassard – The origin of quantum cryptography
14:30 – 15:30	*Zvaný příspěvek / Invited talk* Jozef Gruska & Jan Bouda – New directions in quantum cryptography
15:30 – 16:00	*Přestávka na kávu a čaj / Coffee & tea break*
16:00 – 16:45	Jiří Vábek, Daniel Joščák – Complexity and Classification of New Collision Types in MD5
16:45 – 17:25	*Rump session*
17:30 –	*Večeře / Dinner*

Následují neformální diskuze v prostorách vyhrazených pouze pro účastníky kryptobesídky. / Followed by informal discussions in the hall available only to the workshop participants

5. prosince 2008 (pátek) / December 5, 2008 (Friday)

9:00 – 9:05	*Zahájení druhého dne workshopu / Opening of the second day of the workshop*
9:05 – 10:05	*Zvaný příspěvek / Invited talk* Zdeněk Říha – On security and crypto issues of e-passports.
10:05 – 10:35	*Přestávka na kávu a čaj / Coffee & tea break*
10:35 – 11:35	*Zvaný příspěvek / Invited talk* Martin Hlaváč & Tomáš Rosa – Towards disclosing the RSA private key of an e-passport.

KEYMAKER

11:35 – 11:55	Michal Rjaško – Properties of Cryptographic Hash Functions
11:55 – 12:15	Petr Veselý – Německá válečná šifra Lorenz a její prolomení
12:15 –	*Mikuláš – přináší Microsoft / Santa supported by Microsoft*

Závěr workshopu... / Workshop ends...

E. O čem jsme psali v listopadu 2000 – 2007

Crypto-World 11/2004

Crypto-World 11/2005

Crypto-World 11/2006

Crypto-World 11/2007

F. Závěrečné informace

1. Sešit

Crypto-World je oficiální informační sešit "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Obsahuje články podepsané autory. Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.
Adresa URL, na níž můžete najít tento sešit (zpravidla 3 týdny po jeho rozeslání) a předchozí sešity GCUCMP, denně aktualizované novinky z kryptologie a informační bezpečnosti, normy, standardy, stránky některých členů a další související materiály:
http://crypto-world.info

2. Registrace / zrušení registrace

Zájemci o e-zin se mohou zaregistrovat pomocí e-mailu na adrese pavel.vondruska@crypto-world.info (předmět: Crypto-World) nebo použít k odeslání žádosti o registraci elektronický formulář na http://crypto-world.info. Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu určenou k zasílání kódů ke stažení sešitu.
Ke zrušení registrace stačí zaslat krátkou zprávu na e-mail pavel.vondruska@crypto-world.info (předmět: ruším odběr Crypto-Worldu!) nebo opět použít formulář na http://crypto-world.info. Ve zprávě prosím uveďte jméno a příjmení a e-mail adresu, na kterou byly kódy zasílány.

3. Redakce

E-zin Crypto-World

Redakční práce:	Pavel Vondruška
Stálí přispěvatelé:	Pavel Vondruška
	Jaroslav Pinkava
Jazyková úprava:	Jakub Vrána
Přehled autorů:	http://crypto-world.info/obsah/autori.pdf
NEWS	Vlastimil Klíma
(výběr příspěvků,	Jaroslav Pinkava
komentáře a	Tomáš Rosa
vkládání na web)	Pavel Vondruška
Webmaster	Pavel Vondruška, jr.

4. Spojení (abecedně)

redakce e-zinu	ezin@crypto-world.info ,	http://crypto-world.info
Vlastimil Klíma	v.klima@volny.cz ,	http://cryptography.hyperlink.cz/
Jaroslav Pinkava	Jaroslav.Pinkava@zoner.cz ,	http://crypto-world.info/pinkava/
Tomáš Rosa	t_rosa@volny.cz ,	http://crypto.hyperlink.cz/
Pavel Vondruška	pavel.vondruska@crypto-world.info ,	http://crypto-world.info/vondruska/index.php
Pavel Vondruška,jr.	pavel@crypto-world.info ,	http://webdesign.crypto-world.info
Jakub Vrána	jakub@vrana.cz ,	http://www.vrana.cz/