Crypto-World

Informační sešit GCUCMP
ISSN 1801-2140

Ročník 7, číslo 10/2005 **15. říjen 2005**

10/2005

Připravil: Mgr. Pavel Vondruška
Sešit je přednostně distribuován registrovaným čtenářům.
Starší sešity jsou dostupné na adrese
http://crypto-world.info
(1001 registrovaných odběratelů !)

Obsah : str.

Příloha : Další informace k článku V.Klímy - Bude kryptoanalýza v Česku trestána vězením? - zřejmě už ne! - prilohy.zip (53 kB)
(Obsahuje: Žádost a podpisy odborníků, Návrh Šámal, Návrh Smejkal, Návrh VK_IURE, překlad části úmluvy, průvodní dopis vk_iure, link psp, stenozáznam jednání PSP, tisk zpráva ČTK)

A. Soutěž v luštění 2005 - přehled úkolů I. a II. kola!

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

Přesně o půlnoci z 19.10 na 20.10 odstartovala tradiční soutěž v luštění jednoduchých šifrových úloh zveřejněním deseti úkolů prvního kola. Příjemným překvapením byl letošní zájem a připravenost soutěžících. V současné době je přihlášeno přes 130 řešitelů a všechny úlohy prvého kola vyřešila více jak čtvrtina účastníků.

Limit patnácti bodů, který je potřebný pro zařazení do slosování o ceny (http://soutez2005.crypto-world.info/index.php?crypto=ceny) splnilo již 41 řešitelů (údaj platný v okamžiku psaní tohoto příspěvku). Nejdříve ze všech vyřešil úkoly prvého kola luštitel pod pseudonymem Stanislaw, který to dokázal hned první noc …. (cca 4-5 hodin luštění). Úkoly druhého kola se ukázaly být pro řešitele složitějším oříškem. Nejodolnější se ukázaly úkoly sedm, osm a devět. Tedy úlohy na šifrové systémy, které v předchozích ročnících zařazeny nebyly. Všechny úkoly druhého kola jako první vyřešil soutěžící pod pseudonymem vn (11.10 - ve 20:42).

Vzhledem k vyšší obtížnosti některých úkolů jsem se rozhodl, že budu průběžně zveřejňovat nápovědy a indicie, které vám pomohou najít řešení těchto úloh, nebo se pomocí nich alespoň ujistíte, že postupujete správně. Rady soutěžícím najdete v NEWS http://crypto-world.info/news/index.php . Informaci o zveřejnění nápovědy najdete také na stránce soutěže v sekci *aktuality*.

Prvé kolo byly šifry/nešifry (pracovně tak nazývám šifrové systémy, které nebyly v praxi nikdy použity), ve druhém kole jsou úlohy na klasické šifrové systémy, jejichž rozluštění vám pomůže zvládnout i vyluštění úloh třetího kola, které bude věnováno šifrám prvé a druhé světové války.

Doplňující informace *pro zvídavé*: chcete-li vědět, v jakém pořadí jste Vy nebo vaši soupeři řešili jednotlivé úlohy, nebo které úlohy konkrétnímu řešiteli ještě chybí, můžete to jednoduše zjistit takto:

- na stránce soutěže http://soutez2005.crypto-world.info/ zvolte v horním menu sekci *zebricek*
- vyhledejte uživatele, o kterém chcete získat informaci
- podržte myš na jeho jménu
- cca za jednu vteřinu se v informačním okně objeví pořadí úloh, ve kterém je zvolený uživatel řešil
- snadno si z této informace odvodíte, které úkoly ještě řešitel nerozluštil

Průběžná statistika soutěže (14. 10. 2005, 20:00)

Celkem soutěžících:	**134**
Počet soutěžících, kteří vyřešili alespoň 1 úlohu:	114
Počet soutěžících, kteří splnili podmínku k zařazení do slosování o ceny:	**41**
Nejvyšší počet dosažených bodů:	44
Celkem již publikovaných úloh:	19
Maximální počet bodů, které lze prozatím dosáhnout:	44

Aktuální statistika je k dispozici na stránce soutěže:
http://soutez2005.crypto-world.info/index.php?crypto=statistika

Přehled úkolů - I. kolo

Šifry/Nešifry

Na konci díla poznáme, čím jsme měli začít. (Blaise Pascal)

ÚLOHA I/1 - TRANSPOZICE Č. 1

BODY: 1

```
INEZAV ICIZETUOS EMANICAZ OKAJ YDZV EVRPJEN IMLEV UOHCUDONDEJ
UOHOLU IZUOLS K UMOT ETSYBA IS ILESUOKZO KAJ ES ENVARPS AVADAZ
EVOCILK OVOLS ICIJUZAKOD EZ ETSJ UHOLU ILISERYV ETJEVADAZ OTYT
YKDELSYV YDZV IMYKLEV YNEMSIP A ZEB REZEM ETSUKZ IS OT AN
OTMOT ELSEH INELOVYV
```

ÚLOHA I/2 - TRANSPOZICE Č. 2

BODY: 1

```
DUALH JOENT ASOII YTMAO TCYAE ZPEUE AUAOU AVRSN ZDJEI BOHRA
ITOEB ZEETM OCRKA AAELT SOAUE EEADO RVOEO UTNDZ MAPLE CAMVI
RIESL HVDAP OTDST ZMWHY IARNM LEINK IRZME TPESP NETRG BTEAI
EEYZK DKJDZ ZDREV ZNKIE PMESS CZPNR ATPEA OUHR
```

ÚLOHA I/3 - TRANSPOZICE Č. 3

BODY: 2

```
TEART IOZUU LJOEH TAEUN ZTVOA SMYMS OTZEN MATBE UXDTE SDEEN
LEAJT PPROV TEIRZ OEZTD REOLC IHNUA PDRVI EPPOO MLION VAILN
OYNAS PKAYK SSYES NTAEL MIPCO HDALM EIPSL TOATZ UAAPL IESJE
EPZRD VENPI RCEAC SETJA ENNAR SOUZD DAIML IVSET PAIDS RTUEH
KALCI ACSPT RSOYL SNTUE TMIST EONTA OZSYL VOAVP ORTOO LTNIU
ZTCIH TAERX ATKUT
```

ÚLOHA I/4 - STEGANOGRAFIE Č. 1

BODY: 1

```
KYQTT QATQE IQTJZ GQOEQ UZJQL HOXOQ OOZQH EXVDQ AYBQJ NYDEQ
EGQFQ NILNQ AWDYC QTXKO QZZTQ VVAAQ KLSQL BNQAE NQMOI QAKQC
WQEWB NQTYQ EPQXZ QTDLQ VHYQO XPRQT VSNLQ ELCQV CQWQR BQKSQ
EWBTU QNSQE MQPYF KPQOT QDCQO HQBWQ EVHQJ EORJQ EOURM QOBCP
QBIAQ AICQL DJQEG QNGTJ QPMEZ JQIFU KJQSH HQMGB AQERQ NEJQY
SJUFQ KIXPR QTPRQ EEIQJ QRLWC AQARN BQNCQ EYEYM QSUYT QOHQQ
UOROQ VXQID QSYAC BQIHD DQSBQ OZREQ TNMTQ EMQVV PEQRB QEBLM
HQNEN QYCJQ MUDNM QTWQW NQESE QXVZZ FQTKM QEVAN QMEBK CQRSY
QENDQ SAKTE QIWMR LQTEQ ESQLA QEECQ NMDYT QAMUE QPPQI UPRAQ
SLTFQ IARQK AQLCF QAFBF AQMCQ ALZQC MFZNQ SADQY ZGQSJ ETQTK
QEOQK QMCVW QJYRQ ESRGQ PTEQK QROQE NNQDM OQSHI FNQTK QATQV
```

```
LTQES ULQNN ZGQTO QANMQ KFRQA JDXBQ BIQYB ZVRQB JYQYW RVQLH
SKLQL FQECQ HKUQC UBDYQ ERYQL BQUPQ SYUIB QTEAT QIUNS HQTKQ
FOQEN QLBRQ NDQYS TQNAH DQERX QQBRY QOAWQ SHQNB QAFTT LQDMQ
NRQEB DHIQB WDHQY BEANQ LQ?XW
```

ÚLOHA I/5 - STEGANOGRAFIE Č. 2
BODY: 2

Potkan arest pan potrat spojit puska hryzavy vysledek tatinek kdekoli lama pepsin udrzba udiv aspirin svoloc Dominik lzice kunkat Ital buldok uroda panenka postava taktovka dloubat koudel moucha talar zbozny bahnice utulek mzdovy Kanadan ucebni listovi akacie vylodit stepni vyjmout posluha klokani louh lehky balit presun radnice exaktni usni hlasovy rypavy mnik laskani vymrely hledat bandita pratele hanba svisly pokojska kroutit uplata opic povalec sin skadlit topit mroz kostra celni slepit rada zinek briza limitni vymotat otisk myslet osteni kreol ohar malirka hvezda banker chatrat Petr Evropan jsem ustat stitek sopka mnozina dozadu lzi krcni dziny kovani hykat mrazivy vyzadat ledovec dneska krmitko kosikar nulovy klopny kovarna kdezto srdnaty emulace kokain cpavek fazole odvaha otyly utratit uderit dostih udel kanon zdimat kujny brevno pocasi zprahly zvyseny Popelec kotelna hrom Oswald zbourat ubrat nalehat dodavka

ÚLOHA I/6 - JEDNODUCHÁ ZÁMĚNA Č. 1
BODY: 1

-/-./-.-//.../..-./-./...-/---/-..//.../../.-../.-./-..//.../.-/-./..-//.-/./.-/..//.--./.-./---/...-/..-././--//-.../--.-/.-
././.../../-//---././/-/---//..../..-./-./-.../.-/.//.-/-./.--./---/-.../../..-/-.//-.-//.-/-./.../..-././..-/-../---./../.-.-/..//-
../..-./---/..--/.//..-/-../-.-/-./..--//-.../--.-/.-././.../././-/..//---././/..--/.-./.-.-/-./..-/..-././.-/..///

(Pozor –
vzhledem k problémům při zalomení stránky, jsem v tomto přehledu zaměnil pořadí výpisu zadání úloh č. I/7 a č.I/8)

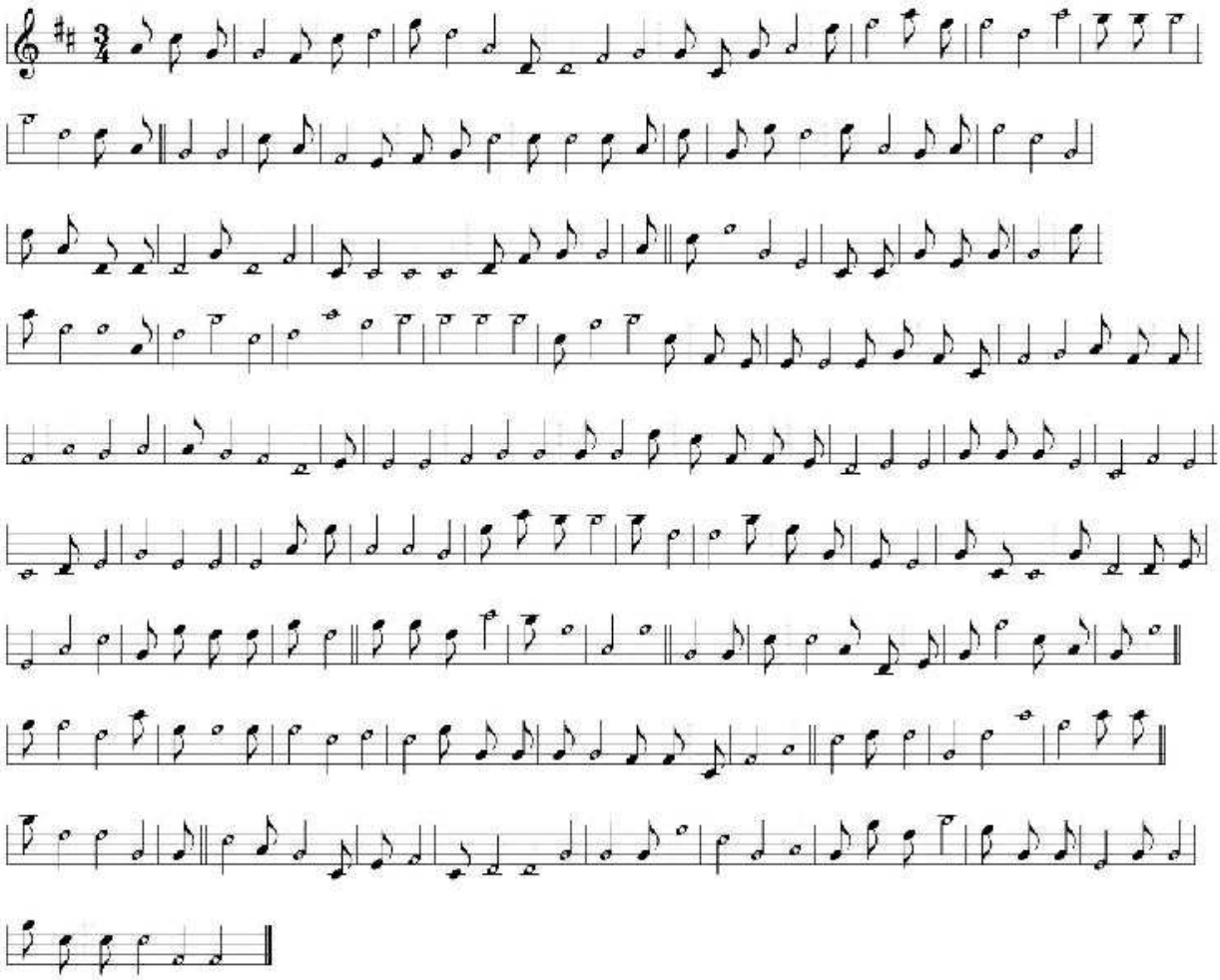
ÚLOHA I/8 - JEDNODUCHÁ ZÁMĚNA Č. 3 + STEGANOGRAFIE
BODY: 2

703 : 764 x 9659 x 9302 - 269 - 1548 + 0971 x 424 : 9 x 0 + 886 + 22 : 5906 + 539 : 6358 - 27 - 185 x 133 - 4227 + 81 : 6122 x 46 : 79 + 917 x 050 : 064 x 6 + 133 : 2687 : 541 x 605 x 3 x 27 + 185 x 8575 + 2 + 866 + 9 + 2 - 8313 - 0 x 340 + 10 + 25 : 229 + 0102 : 359 - 8226 - 49 x 369 - 971 : 328 - 375 x 4483 x 49 x 10 x 02 : 5 + 6 - 76 + 3 : 353 - 907 + 694 : 65 - 9 x 6 : 15 + 84 + 606 + 9 x 911 x 7038 x 81 x 256 : 745 x 7633 - 83 - 1 + 4 - 1016 x 103 + 5097 - 668 : 481 - 126 : 2 : 49 : 0324 + 02 - 1779 - 6 x 5698 + 06 + 480 : 4342 + 60 + 9050 x 2 x 7782 x 21 + 942 - 0 x 6915 + 9 : 4 - 2646 x 6 - 484 x 8304 - 199 : 55 : 25 + 1 + 8 : 19 + 83 + 3 + 68 - 703 : 87 =

Nápověda: zveřejněna v NEWS 30.9.2005
(http://crypto-world.info/news/index.php?prispevek=2017)
Tentokráte je nápověda velmi jednoduchá - rada, kterou naleznete v otevřeném textu úlohy číslo šest platí i pro úlohu číslo sedm!
Ještě nic ?

ÚLOHA I/7 - JEDNODUCHÁ ZÁMĚNA Č. 2 + STEGANOGRAFIE

BODY: 2



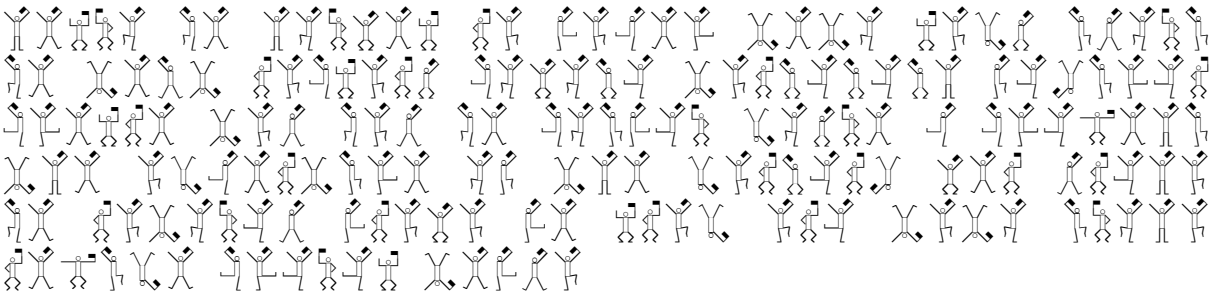
Nápověda: zveřejněna v NEWS 28.9.2005
(http://crypto-world.info/news/index.php?prispevek=2003)
Ode dneška si můžete stáhnout hudební part úlohy číslo sedm v lepší kvalitě.
(http://soutez2005.crypto-world.info/images/noty.jpg)
A teď ta nápověda, nepředbíhejte, vyluštěte si nejprve úlohu číslo šest ...

ÚLOHA I/9 - JEDNODUCHÁ ZÁMĚNA Č. 4
BODY: 3

Nápověda: zveřejněna v NEWS 27.9.2005
(http://crypto-world.info/news/index.php?prispevek=1995)
I was born on August the 29th, 1971. This means that I was born four months after Igor Stravinsky died, but one month before Jimi Hendrix died. This also means I share a birthday with Michael Jackson (joy) and with Richard Gere (double joy), and my birthday falls on the Feast Day of the Beheading of St John the Baptist (hold me back, I can hardly contain myself.)

jIbogh qaSDI' DIS 1971, jar 8, jaj 29. vaj jIbogh qaSpu'DI' Igor Stravinsky Hegh loS jar, 'a qaSpa' Jimi Hendrix Hegh nungbogh wa' jar'e'. vaj qoS rap wIghaj je jIH, Michael Jackson je (Quchqu'lu'), Richard Gere je (Quchqu'lu'bej); 'ej quq qoSwIj'e', yo'a'neS quv nach teqlu' 'e' lopmeH jaj je (HIqop; jISeH'eghchoHlaHbe' jay'.)

ÚLOHA I/10 - JEDNODUCHÁ ZÁMĚNA Č. 5
BODY: 2



Nápověda: zveřejněna v NEWS 29.9.2005
(http://crypto-world.info/news/index.php?prispevek=2010)
Mezi mé záliby patří samozřejmě kryptografie, ale rád čtu i o různých záhadách a přímo miluji detektivky (chytré). Naposledy jsem si přečetl výbornou sbírku detektivních povídek od Arthura Conana Doyleho - The Return of Sherlock Holmes. Mimochodem nevíte náhodou, zda kniha vyšla i v češtině?

Přehled úkolů - II. kolo

Klasické šifrové systémy

Je-li správná odpověď, kdopak se stará o to, je-li otázka špatná? (Norton Juster)

ÚLOHA II/1 - JEDNODUCHÁ ZÁMĚNA Č. 6

BODY: 2

```
U E L E N   L E S T J   R Y D R U   R D P U E   D L R C Z   E U L R F
I P J E J   E C Z U L   Z Y D H U   P J R I P   W E L Z W   R C Z E I
R Y K E G   U P F Z D   E F P J R   O H Y V Y   D R O H E   A Z C V F
I D E G P   J V F I T   E D G T P   C R P U L   E J C R C   R J V L P
X Z H J R   T R T P P   X R I H T   P J R W R   J V J R W   R U L P J
R W R C E   X Z W Z W   U L P Y D   L R T G H   A R U L P   T E C R X
P A Z C E   G W U L Z   Y D H U C   Z Y P X R   C R X P A   Z C R O H
P U E D L   Z C R X P   U L R F I   P J E J E   W E L Z W   R C Z C R
X P A R I   P Y P H F   E Y D U P   Y D H U C   E Y D L P   A C R X P
A E G V G   P K Z A Z   C V U L P   Y D L R T   R G J F R   D C R U P
F Z D E F   P J R I P   U L P N L   E O H J V   D J P L R   C V C R X
P U L Z W   U H Y P X   R C V G Y   U E F I E   C Z D L R   Y D C R I
P F Z C H   C R P U L   E J C R C   R I P U L   Z Y D H U   H G U P F
Z D E F P   J R O H Y   V Y D R O   H E U P Y   G P W R C   Z E W C R
H W Z D Z   W E W C E   O H J U P   F Z D E F   P J R O Y   V Y D R O
H E C E C   P Y Z F Z   Z C S P L   O E F Z U   P T K R U   E L E N L
E S H T J   R Y D R F   D V L Z C   R X P D L   R Y D C R   I P F Z C
H U P L H   Y P J E C   Z D E A R   O Y D J Z   T P U L E   J P J E C
V F I W U   L E J U P   T K R U E   L E N L E   S H Y D P   U E T R Y
E D Y R T   O P T Y D   A R T C E   U Z Y O X   E F C R X   P U L R F
I P J E J   E U P F Z   D E F P J   R I R Y K   P U L Z Y   D H U P J
V G P T U   P Y D H U   C R X P U   P T P X C   E T E D E   U P O P F
Z C Z F I   W K W R W   Z Y G E D   U L Z Y D   H U G U P   F Z D E F
P J R I P   Y V Y D R   O H C R X   P A R I P   F E Y D Z   X H T R U
P D L R Y   D E C P T   C R D Z O   Y J P X P   T V E W C   E A R T R
C L P G U   L P U E T   C H D Z O   J R F Z C   R X P W E   G E W R O
F Z C C P   Y D Z P T   C R D Z O   Y J P X P   T V E W C   E D L Z K
R D E U L   P U E T C   H D Z O J   R F Z C R   X P W E G   E W R O F
Z C C P Y   D Z X H T   R U E F I   E D R K U   P D L R Y   D E C Y U
E F I E K   Z F Z C H   J R T R C   V J P T Y   D E J F Z   A R T C E
A E G P F   K R C P L   N E C Z W   P J E C R   Y G H U Z   C V C R X
P W Z Y G   E K Z D E   G P J V O   F Z C R O   U L P Y R   X R C R X
P U L P A   Z C R I P   W C E F C   V U L P Y   U R F I A   E G P T H
G E W H J   R T D R U   L J R Y K   P J P D P   I P D P D   R Q D H X
(1020)
```

ÚLOHA II/2 - JEDNODUCHÁ ZÁMĚNA Č. 7

BODY: 3

```
L W T M D   M T U Z O   P Y A O F   O D T X W   Y A C U T   K Y M I G
V A L Z O   M U K O I   E C W Q V   D M Y H T   A L W O R   P V W Y Q
V H O F O   P M T D T   U F O A O   M D O M U   M I W T U   O M M W T
M A C W T   A M A C W   P O H K Y   W D T P Y   U P T G V   W O P C U
T D M T U   Q O E Y P   Y W Q I P   C K Z O R   G O P T Z   I Q Y F C
L T M A C   Y C M Z C   P M T Q F   Y D M C A   C P Y A O   W Y R G O
W I A O D   P C R O R   C U K W C   P T M D T   M V C U T   E Y R C F
C H T Y E   Y G Y U G   C M O G C   M T U Q O   K Y B O P   T C M Y G
C H O W T   U K C H O   W T U K Y   A D C Q W   O D T T D   A Y V D Y
V Q W Y G   Y V R C K   C F V H O   K Y U Z C   T W O R G   T R O Z C
E W C A O   A Y Q C G   R T Q V Q   F I A Z C   F P T Y W   B C P I E
```

```
Y H C Z I   E Y F O R   W O P T R   O A E C W   Q V H O D   E T Y P E
Y G C K C   G V H O H   T P O H Z   O E D T E   W T M O Z   Q I P O R
C U K I U   O P I M O   S M V D E   T Y P C Q   Y F W O X   Z O Q M Y
W D E C U   O L D E C   U O J K O   O Z D D E   C U O T T   T D E C U
O T A D E   C U O T T   D E C U O   W T P B D   M O Z Z V   P B D E C
U O D D E   C U O U D   E C U O C   D E C U O   E Z V B L   Y C W F D
E C U O H   E D E C U   O F I D E   C U O N D   D E C U O   K Z D E C
U O C O D   E C U O P   J D E C U   O U V D E   C U O T Q   D E C U O
X S D E C   U O L W D   E C U O M   O P M Y Q   W C M O D   T D U K Y
A O H M O   R T D Q C   P I Y M O   A W O P I   M O S M L   V F O D O
A C G K Y   F T M F V   Q C R H O   R C F C P   T P C R A   V K Z C A
P T K Y G   O D M C D   Z Y A O P   D Q O W O   E V L Z T   Q I X X X
(690)
```

ÚLOHA II/3 - JEDNODUCHÁ ZÁMĚNA Č. 8

BODY: 3

```
A W A F S   Q O M H C   O J Z C R   M A J H C   R D I R M   G J R M P
C R M G R   C G A M J   M D C D I   R W H I B   P I C Y J   F I F Z C
S C G F J   H C Y M Q   I C D J H   M X C D I   F M J P C   I Q A B L
M Z W J R   M P D I C   P F J M S   M J P B Z   F K C L M   A J H M Y
C J H Q D   M A F B P   I C G J D   C Z C H B   P I C G O   C X C O B
D I R B J   R M P C R   B R C G A   B O M K C   A J P I C   R B Z B X
I C Y W K   C O M I A   M G P M L   X A F H W   Y B D C G   M A M G O
C J P I B   P M U F M   A F L M A   F B A B J   B O M A F   M A C R W
L X Y S I   B A F P B   A H C R Z   F M P B O   F M Z B H   C B G L X
M K F L H   W L X S C   G C R W L   X Z B P C   H J F R W   Y F B O B
Z C Y F R   C P W K F   Z F C A C   R Z Q O F   R C G A B   J B O C P
H Z B R C   Y R W J M   A M G K F   M I M F L   F R F Z A   M X C C S
W R B P M   Z J P R B   A M O C J   P B P H C   K D C P I   B R F A D
I B L C Q   Y F M A R   Y S I C G   B I J H C   K D I F M   K W J Z M
S C K S B   I O C R B   A F K K F   M J P D I   F A F M J   Z B Y B R
B Y A M D   C Z F P F   L H M Y K   M A W D C   L B J R C   G A W J B
I C Y D B   O Z B D C   Z F P F L   H C J D C   Z C L M A   J H B J P
I Q H P Q   I B J P B   I M G M Q   I C D W K   C A B I L   X F B A M
K M L H M   G I F J M   I B H Q J   H C Q X C   I J H C B   I Q J H C
J B I C Y   D B O Z F   P B H F J   P C B H C   C J K B A   J H B I F
J B C H P   C S I C R   B I M R C   Z Q L F B   R I Q J H   Q D C D I
R W H I B   P R X F J   P C I F F   D I M J B   O F Z B J   C L F B Z
F J P F L   H M D I M   O J P B R   W O C D I   B V M A M   K M L H C
B A B J P   Q D A F L   H M J P B   P W X B S   J S Q I J   H M G K C
A B I L X   F M Y B L   B Z F D I   M L X B O   Y B P H O   M K C H I
B P F L H   W K I M D   Q S Z F H   B A J H W   K J P B P   A W K N C
I K B K R   J P Q D Q   J B O C R   C G A W D   I M J Q A   Q Z P B Y
F J H C J   R M P C R   M G D C Z   F P F H W   M Q I C D   B J P I B
P F Z B J   R C G M X   M U M K C   A A M D C   J P B R M   A F M Q J
B J B J P   B Z F I C   Y X C O Q   G Q L C Q   X C J D C   O B I J H
C Q B N F   A B A L A   C Q R M Z   K C L C Q   O C J Z M   O H B K F
D I R M G   J R M P C   R M G R C   G A W S C   Z F C H I   M K F A M
X C B G A   M O C J P   B P C H D   C P I B R   F A B I C   Y J F B X
Z B L X I   F D H C R   B M D F O   M K F B M   K B A L F   D B L F B
Y F M A Y   B L B Z F   D I B L C   R B P P B   K H O M D   I M O P W
K K B Z F   K C A C D   C Z F S B   K Q Y F B   L C J H C   I C Y F J
H B Z F B   G R C Z M   S A M D I   B R C R C   G A Q N F   A B A L C
R B Z F M   Q I C D J   H M R Z B   O W Y I C   Y J F B X   Z W L X D
C Y F L F   M H P Z B   L F Z F J   P B Z M R   F B L D B   D F M I C
R W L X D   M A B Y F   L C R F M   O Z C H F   A N Z B L   F X X X X
(1200)
```

ÚLOHA II/4 - JEDNODUCHÁ TRANSPOZICE (ÚPLNÁ TABULKA)
BODY: 3

```
L O A L P   U Z V C Y   Z M S C E   N P A M E   L A C K A   I O K L Z
E D M O V   L A K X K   D Z V R A   V C H L C   T U S R O   I E R G I
Y U S K A   U A A L H   C K S M N   Z A X A P   D E E R A   O E R Y I
I A N A A   K I N Y N   O S V N T   E A E D T   E P O I Z   E X G D Y
J V K O E   D I I K O   A A K H P   A O R T J   S I V R Z   K T Y Y D
M P D P N   K E R M E   O S V R A   N T Y V L   D A A A K   P A E E O
T Y C I Y   E B P O A   O Y R I A   N U L N K   E N L R A   L Z J L U
A A O A H   Z O D Z E   E S M R V   M N I T J   O N E X R   U L V C D
N N R E K   Z M Z E T   L C V S B   I P T Z S   E C E S I   A D S M Z
U Z A J I   V I C E J   V U Z C T   R E S E U   A T R R E   S V O E C
S P D A O   A N C D T   E X O A H   R N E L V   E O R N Y   O H Z N H
S N P N I   A N Z R R   I K U L A   Z T U V O   X E H Y I   U U L J P
T C E L Z   G I I A O   E E K O E   K E N E L   Y V D E Y   A A V Y K
K C O R U   G A E O K   U O V K L   T B T E D   K T T S P   G A J M A
J T R H M   O J R X A   U P E R U   H R S A T   R O T A K   L I P U O
D S M E E   T L I R I   S K E E P   E E X N U   B N L O E   I L K I R
E A U P J   L T R L M   H V A V E   N A B Y A   V D D Z A   H Z T R N
K O H A E   E T A P T   A R E A P   O S T O E   E N C S A   E A L U O
L S I D T   X A K K O   T R I U U   T Y E N I   D L Z R P   U N B R U
M R O Z I   A O I C E   S B A T X   I K E J I   N E O D M   H O I M O
R N N N U   I D U A T   N I E E O   K J T E O   R E J X U   K A E I P
K Y N L S   P D P U A   I T T E O   A V V O D   U A S D V   I R E A Z
K U X S Y   A E O L E   E L P A E   V T U D M   C O E K A   Z T I L D
Z L I O I   E E E O E   T X (702)
```

ÚLOHA II/5 - TRANSPOZICE (FLEISSNEROVA MŘÍŽKA)
BODY: 2

```
I O T H S   N Y A K T   S K E T D   A R O L K   Y P C A O   U A H K Y
S T B M C   A H B Y L   I O U S T   V L T A K   A L U A S   Z A X K I
X P C L   (64)
```

ÚLOHA II/6 - PERIODICKÉ HESLO (SYSTÉM VIGENÉRE)
BODY: 3

```
Q P E E G   R P O R M   K A F I N   I V I W E   O E U A M   A X P O E
Y N C C M   O N Z V U   T A D E P   Z J B G H   D U Q E K   Y X I E R
R D S O F   V X N H T   L N Q D T   L D Z Y E   O M V K H   Q G R E P
G I P Z P   L G V B S   K S O A M   P E A Y R   T M B I L   T D R N U
O W I E U   E N E R I   M R L P K   P Q K T T   N Y K E L   U X N D K
P N G Z T   L C I T T   B T X R Q   E N E N V   B K V X L   B W W D H
D K P N G   Z T L P S   O E N R X   H R D O E   X I M A D   V X A F I
F E O E S   R C T T V   R T P R C   Z V I F M   E A F M E   A K P L V
P Q K O O   M R E P M   K A O Q L   N U B X I   Q Z P L K   B X L V O
F P K V R   A U Q L D   L Q A N D   Z C H Q D   T L G Z P   V C Z B A
Q X J O R   M K A F M   Y A N M M   O W M D I   E L X V H   X D E V K
M Y U M N   E V B K I   E C W S K   L H B U I   G E F W F   Z W V L T
M B X R H   A P H T U   T C K X F   T T X X L   D W A A V   Z H V D P
A R Q B H   J H H T N   Q C G A G   I U I X C   W E U I N   H N W D A
O R T H Q   K A A U E   V T G Z N   K W I C E   R W L T X   T Y E R W
W K R T Z   U D W C O   Y S F S K   T N R X W   F M Q L X   L H Q A R
```

```
Q V X J E   C W A U I   F O C V P   J O M N S   S I D N C   X K O W M
Z F G V S   I Y E F C   J I K K R   Z L P T D   G I P E Y   S V M B N
H Q Y A X   Z A O Y E   Y A X I K   I D R E A   B I A R Q   S G A N I
K O C W L   H N G N S   W Y A N C   R B H X O   E E T G U   Y Q E D L
G L H V D   P O R V Q   O Y S V Z   T K C W E   U Z P D G   V R P U S
E I Q L D   R B X P M   W A X V H   V Y I O C   D R L H W   U R W L T
X T F J K   K B R X H   P A T U T   D B L T T   N M K V V   E V B A T
K O C L Z   D P M I R   R X T J C   S R M N S   W I X H M   R D X L M
W H X M L   E E U F Q   S T H R E   O R T T N   Q I A O F   X H R L P
O R W P T   M D R D T   G Q G O Y   E G A T Q   T N W E K   A J Z G O
Y E W A W   B H K Q E   V U T A D   Y Y C M E   B M D K W   I C Y O M
E B B X G   E F M G C   R R P J F   Z B V H R   P J N M I   E G S V O
P K X K Y   I E N C X   T K E C K   B A D T L   M I D T G   K T S R H
C A B Q M   P U I O P   Q S E A G   E Y O W A   H V H X D   K Q C H F
H R K I X   C G A M M   S U L I D   O U I D E   P Q O L R   D E E P I
S E Y S A   E T I V E   D N D T G   A H U F E   D N G X K   I S V L V
G V B N D   H P S K N   K A F M A   O U T X D   Q M F L Q   P R D U Y
S E J W D   O O E XX (1000)
```

ÚLOHA II/7 – ABSOLUTNĚ BEZPEČNÝ SYSTÉM Č. 1

BODY: 4

```
52998 31345 92108 48323 22633 91170 47386 48236 05764 81593 01912 19141
96452 77781 97358 51093 89097 10082 33995 02628 71415 61570 80157 01388
92742 37855 72309 12553 98600 67207 00778 03116 75946 22778 63885 46198
90431 29483 45041 07566 44169 04382 94477 90755 06856 88748 87817 68940
70762 06898 95711 79392 94777 30795 32851 67392 01146 00513 22428 17633
15912 99700 29357 01170 98233 48526 36953 21326 87360 77697 87947 28770
96168 14503 89762 60651 80640 87833 88826 18331 90134 30901 57804 43981
35677 01103 85013 45897 86267 07467 75817 11990 77499 62195 86806 14180
81973 55780 59058 19182 40392 81584 15981 73349 88387 39364 60832 41045
76647 14194 90784 00978 43081 82571 29505 71889 61628 57775 71972 03667
90343 67909 94247 50649 88404 47544 01557 76890 84792 98930 72888 40104
72045 86187 14947 44691 48514 58574 20966 80080 24048 24709 25807 32872
85738 71200 25707 06746 79035 89641 20079 02373 79189 20276 24312 79951
05697 92995 93933 07685 81007 13549 21785 06093 45981 39488 53 (832)
```

ÚLOHA II/8 – ABSOLUTNĚ BEZPEČNÝ SYSTÉM Č. 2

BODY: 4

```
41978 31659 98107 89732 08703 01593 30366 79944 92832 72293 77013 78720
14552 16591 04189 42099 91918 12674 42907 10103 77354 22201 77997 41603
82662 97846 85359 01278 92500 68326 98896 73731 71746 90194 56876 17198
75391 89260 56189 08460 41267 95196 94268 21567 82707 78024 99688 49932
81821 64205 85689 01917 85698 89716 23931 27985 01317 49610 35278 18343
93171 89306 21439 61151 84255 18323 28852 82112 81517 69386 88828 67576
96239 33819 01892 49649 11519 07936 82947 77523 96315 60005 48063 91993
34649 31018 79952 75287 87156 97857 89027 82885 71518 12399 95946 94783
09183 04275 46027 49173 54302 91675 00822 32939 85487 89250 66663 58963
88558 45696 92774 11185 48053 62698 01813 82193 46588 97882 82702 72951
86591 68783 04248 70148 85372 47743 94667 37278 90863 89421 65069 58390
99925 64782 31738 14973 31514 68969 23018 49692 27358 13014 39877 73072
88848 62600 17746 78232 60904 79042 39057 32459 87089 28780 34392 69971
13578 82499 99845 34187 08316 81943 24934 05299 45892 69987 40062 47270
60958 84299 35519 55112 57978 18195 26 (872)
```

Společná nápověda k úloze II/7 a II/8 zveřejněna v NEWS 9.10.2005 (http://crypto-world.info/news/index.php?prispevek=2057)

K vytvoření šifrového textu č.7 a č.8 byl použit tento postup:

- převod otevřeného textu do mezinárodní abecedy
- dekadické vyjádření ASCII znaků
- součet z heslem (bez přenosu)...

Příklad:

Otevřený text :	P	R	A	H	A
Převod na ASCII:	80	82	65	72	65
Heslo:	17	33	63	90	15
Součet:	97	15	28	62	70

Více o systému a o tom, kdy a za jakých okolností jej lze rozluštit viz článek Absolutně bezpečný systém v Crypto-Worldu 10/2001, str. 2-6 (http://crypto-world.info/casop3/crypto10_01.pdf)

ÚLOHA II/9 – ZLOMKOVÝ SYSTÉM EARLE CHASE

BODY: 3

```
LHMBW DQKIA JTR=J M!OGA FCCOO GABJA T!KIB PTRGG AJEFM LABRI MBKIF GAJEF
MLAA (64)
```

Nápověda: zveřejněna v NEWS 13.10.2005 (http://crypto-world.info/news/index.php?prispevek=2092)

Před jejím řešením si ještě jednou pozorně přečtěte vyluštěné otevřené texty úloh druhého kola ....

Přeji příjemnou zábavu při luštění těchto úkolů. Doporučuji si před tím, než se do jejich řešení pustíte, si pozorně přečíst popisy jednotlivých použitých systémů. Tyto popisy jsme v minulosti publikovali na stránkách našeho e-zinu.

B. Bude kryptoanalýza v Česku trestána vězením? - zřejmě už ne!

Vlastimil Klíma, nezávislý kryptolog, http://cryptography.hyperlink.cz

Prolog

Pokud s tím něco páni poslanci neudělají, tak až skončím přednášku o kryptoanalýze na MFF UK, půjdu se přihlásit na Policii, že jsem spáchal trestný čin. A ti, kdo provádí penetrační testy nebo administrátoři sítí, kteří testují slabá hesla, půjdou asi také.
To jsem napsal minule na adresu § 205 navrhovaného trestního zákoníku (dále jen **TZ**) a měl jsem, jak snadno Sedlák nahlédne z výňatku, pravdu:

> § 204: ... Kdo ... **neoprávněně získá přístup k počítačovému systému** ... bude potrestán odnětím svobody až na jeden rok...
> § 205: ... Kdo **neoprávněně ... zpřístupní... počítačové heslo**, pomocí nichž lze získat přístup k počítačového systému..., bude potrestán odnětím svobody až na jeden rok...

Pozn.: Sedlák = občan, nemající právní vzdělání, neseznámený s teorií právní vědy, může být zemědělcem, ale i doktorem jiných než právních věd i obojím, prostě člověk používající pouze svůj tzv. selský rozum :-).

Celý text stávajícího návrhu TZ:
Z ohledem na to, že se dále budeme bavit jen o odstavci (1), neuvádíme zde zbývající odstavce (2) a (3), které se nemění.

§ 205

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo neoprávněně vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k spáchání trestného činu neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),
b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačového systému nebo jeho části,
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2) ...(3)...

Požádal jsem proto rektora VŠFS, pana profesora Smejkala o zformulování pozměňovacího návrhu. Kolega Pavel Vondruška se stejným požadavkem kontaktoval odborníka na mezinárodní právo pana Loebla z CEAG. Nakonec se mi podařilo oba pány dát dohromady, aby netříštili úsilí, a čekal na pozměňovací návrh.

Pan Smejkal mi také potvrdil, že (po konzultaci s...raději nejmenovat...) by stávající znění TZ **umožnilo obvinit kryptoanalytiky a penetrační testery z trestné činnosti.** Tento názor potvrdili i jiní oslovení právníci. Podle nich by se beztrestnost musela komplikovaně dokazovat jinak, a prakticky i teoreticky by to byl holý nesmysl. Takže změna TR byla dle nás nutná.

Poznamenávám, že trestní zákoník v té době měl zaveden pouze princip tzv. formálního pojetí trestného činu, čili to, co splňovalo vyjmenované znaky v příslušném paragrafu trestního zákona, bylo trestné, bez ohledu na "společenskou nebezpečnost", která byla jako pojem vyloučena (Sedlák).

Abych docílil změny navrhovaného znění TR v Parlamentu, musela být moje žádost podpořena dostatečně pádným vzorkem nespokojených občanů. Takže jsem sepsal podle Sedláka "petici" (i když se to tak nesmí nazývat a je to oficiálně obyčejná "žádost") vědeckých pracovníků za změnu § 205 TZ. Tu jsem vytvořil a podpisy pod ní sbíral v době čekání na formulaci pozměňovacího návrhu, abych neztrácel drahocenný čas. Šlo opravdu o dny. Text petice jsem opět musel konzultovat s právníkem (pomohl pan Sekera z ČESKÉHO TELECOMU, děkuji touto cestou za promptní spolupráci), neboť šel poslancům, takže z právního hlediska tam nesměly být formální chyby. Pavel Vondruška zajistil rozeslání „petice“. Postupně pak docházely podpisy na podporu změny v TR. Díky všem podepsaným odborníkům! Bez vašich podpisů by to dále nešlo!

15. 9. jsem kontaktoval lidi, kteří mi nabídli pomoc na základě minulého článku v Crypto-Worldu (bez nich a bez Crypto-Worldu by to také nešlo). Požádal jsem je o kontaktování a informování „jejich“ poslanců s tím, že se připravuje petice i pozměňovací návrh.

Během toho všeho se mi ještě podařilo zajistit překlad pasáže Úmluvy rady Evropy. Do druhého dne to promptně provedl pan Ondřej Suchý z LOGIOSu (překlad bych zvládl sám, ale šlo o čas a hlavně právní slovíčkaření, čili přesnost nad přesnost). Překlad jsem poslal panu profesorovi Smejkalovi a v noci obdržel následující pozměňovací návrh (**označme ho jako tzv. Smejkalův návrh**).

Smejkalův návrh

§ 205

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, nebo
b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačového systému nebo jeho části,
vytvořené nebo přizpůsobené v úmyslu spáchat trestný čin neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2)... (3)....

Upozorňuji, že jsem zde udělal první chybu, že jsem si ho pozorně nepřečetl a přeposlal v této podobě dále. Šlo totiž o to stihnout v pátek rozeslat materiály poslancům, protože v pondělí poslanci nezasedali a v úterý nebo ve středu se to mělo projednávat.

Pozměňovací návrh byl zpracován a před jednáním PSP 20. 9. připraven!
Petice podepsána!
Dopis poslancům rozeslán e-mailem!
Byla slíbena podpora poslance Karla Vymětala. Další poslanci byli "rozpracováni"!

Upozorňuji, že mi to místy připomínalo a stále připomíná partyzánskou činnost, v několika případech jsem nevěděl o jakého poslance nebo poslankyni se jedná, měl jsem jen kontakt na prostředníka. Teprve později se jednotliví poslanci začali pídit po tom, jestli to bude předkládat ještě někdo jiný, takže jména oslovených postupně lezla na povrch.

Osobně jsem poslal e-mail také předsedkyni Ústavně právního výboru (dále ÚPV) paní Parkanové, neboť ÚPV měl TZ v kompetenci. Později jsem na Rootu napsal, že mě paní Parkanová velmi zklamala, neboť neodpovídala ani mě - jednajícímu za desítky vědeckých kapacit, ani jednomu akademickému pracovníkovi , který odpovídá za výuku (stále ještě ta partyzánská činnost, nevím, komu jsem slíbil, že nebudu mluvit o jeho kontaktech a komu ne, hrůza). To je nepochopitelné a neomluvitelné.

První zchlazení

-oOo-

Z emailu 19. 9. (pondělí) - kritický den (text dle originálu tj. bez háčků a čárek):
Na oplatku mam i pro Vas nejake informace primo z PS k nasi veci: Novela TZ by podle programu jednani schuze PS prisel na radu jiz zitra tj. 20.9.2005. Da se vsak predpokladat, ze tento bod bude z programu schuze stazen, protoze Ustavnepravni vybor (ÚPV, pozn. VK) na zadost ministerstva prerusilo projednavani pozmenovacich navrhu, protoze se vlada bude snazit tyto navrhy do novely zapracovat. A bez vyjadreni vyboru pak navrh bude pravdepodobne stazen. Zrejme bude tedy moznost, a pan poslanec (Karel Vymětal, KSČM, pozn. VK) uz na tom i pracuje, ze nas navrh bude predlozen k projednani jeste do Ustavnepravniho vyboru a s jeho dobrozdanim je schvaleni jeste jednodussi.

-oOo-

Projednávání TZ bylo staženo z programu PSP. Připomínkami se měl zabývat ÚPV. Kupodivu ideální situace, neboť pozměňovací návrh mohl být v klidu vyřízen na fóru právních odborníků. Tam pak chtěl přijít poslanec Vymětal a naše připomínky přednést. **Jeho návrh však nebyl projednáván, což pan poslanec označil za flagrantní porušení zákona přímo Ústavně právním výborem...**

Druhé zchlazení

To přišlo od kolegů z eBanky (panové Dr. Rosa a Ing. Komanický, díky moc), kteří mi napsali, že ten pozměňovací návrh, co jsem rozeslal, je špatně. Myslím, že v té době mi k tomu napsal připomínku i docent Tůma z MFF UK (také ohrožený na svobodě přednášením kryptoanalytické pavědy). Jak jednoduché! Když si přečtete pozměňovací návrh od pana Smejkala, tak tam stojí

Kdo ...přechovává... zařízení ... nebo postup...,vytvořené nebo přizpůsobené v úmyslu spáchat trestný čin ... bude potrestán...

Takže stačí mít na počítači virus…. Byl vyroben k páchání trestné činnosti a já ho přechovávám. Hned jsem kontaktoval pana rektora, protože jsem už věděl, že Sedlák nemusí

všechno vědět, a že to, co se mu zdá jako blbost, může být právně v pořádku. Pan Smejkal opravdu potvrdil, že jsou to inženýrské nesmysly.

Připadalo mi to ale tak jasné, že jsem raději dal na přítele Sedláka a nastalo kolo číslo dvě - hledání jiného pozměňovacího návrhu. (Pozor, tady si nedovozujte, že si myslím, že právníci jsou blbci - skutečně ani mezi řádky to tak nemyslím, oni mají svoji pravdu, uvidíte to ještě dále. Skutečně tím blbcem jsem byl já, že jsem rozeslal něco, s čím bych za normálních okolností, tj. po přečtení v klídku a s fajfkou v puse, nesouhlasil.)

Na světě bylo několik verzí, každou podporoval někdo jiný. Upozorňuji, že se nejednalo jen o "právníky", ale o vrcholové právníky (legislativní rada vlády, nejvyšší soud, ústav státu a práva, tehdy ještě nejširší státní zastupitelství, CEAG, autora návrhu trestního zákoníku doc. Šámala, ministerstvo spravedlnosti). To, co jeden navrhl, druhý označil za blbost (teď už ne mezi řádky).

Nebudu vás zatěžovat podrobnostmi, ale v posledním možném okamžiku jsem nakonec sednul s kamarádem Sedlákem a JUDr. Svatošovou z IURE a sepsal poslední návrh, který je tady (**označme ho pracovně jako návrh VK-IURE**):

Návrh VK-IURE

§ 205

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo neoprávněně vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává **v úmyslu spáchat trestný čin neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c)**
a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořen**é** nebo přizpůsoben**é** k spáchání trestného činu neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c),
b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačové**mu** systému nebo jeho části,
bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2)...(3)

Šli jsme nakonec cestou nejmenšího odporu, kdy jsme jednoduše těm činnostem předřadili podmínku úmyslu spáchat trestný čin.

Organizace IURE do kauzy vstoupila na základě kontaktu Ondřeje Mikleho (to je ten šikula, co zrealizoval ukázku využití kolize MD5, viz http://eprint.iacr.org/2004/356), který zase informoval o tomhle mém snažení IURE (http://www.iure.org/, omluvte, že to nemají ihned na webu, webař jim to dělá zdarma per partes) - neziskovou organizaci, občanské sdružení, co zdarma pomáhá lecjakým nešťastníkům.... a ta mi v pátek 7. 10. poslala návrh pozměňovacího návrhu plus kontakty na poslance a nabídku zaslání tiskové zprávy médiím.

IURE také dále opravila odůvodnění a dopis poslancům a text emailu a měli jsme to v neděli 9. 10. v kupě. V pondělí to dostali všichni zainteresovaní poslanci také fyzicky na papíře a do své schránky emailem (zařídila IURE a Ondra).

V pondělí 10. 11. následovaly telefonické kontakty s poslanci a jejich kancelářemi, protože všichni poslanci byli ve svých regionech. Měli jsme stále ještě zajištěnu podporu jen jednoho poslance. V úterý měla začít schůze PSP, na níž se už TZ měl skutečně projednávat a to ve druhém čtení. Takže zase poslední šance...

Během pondělí jsem kontaktoval řadu poslanců, jejich asistentů a poradců a jednoho poradce poslance, co dělá poradce druhému poslanci, který dělá poradce předsedovi poslaneckého klubu. Napřímo jsem jednal s poslancem Böhnischem, Koudelkou a v pozdější fázi Pospíšilem. Jinak všichni přímo nebo přes asistenty slíbili, že se tomu budou věnovat a ozvou se. Ozvali se Böhnisch (ČSSD), Pospíšil (ODS) a Vymětal (KSČM), přes asistenta Novotný (ODS) a přes IURE poslankyně Konečná (KSČM) - všichni s tím, že návrh podpoří resp. předloží.

Jednání ve sněmovně 11. 10.

V úterý začalo jednání PSP. Díky zprávě ČTK a médiím, které jsme s IURE obeslali, se ozvala televize NOVA a zpracovala během úterý příspěvek do hlavní zpravodajské relace.

Celý příspěvek si můžete přehrát z http://www.nova.cz/tvarchiv/video/?video=34842 nebo stáhnout http://crypto-world.info/casop7/tr_205_nova.asx (2,6 MB).

V příspěvku oslovili i ministerstvo spravedlnosti. Jeho mluvčí přiznal, že "ministerstvo si je vědomo možného špatného výkladu ... a je připraveno akceptovat změnu TZ". To bylo před projednáváním ve sněmovně, takže ministr spravedlnosti už byl připraven ke změně. Vyjímám jen pasáže, věnované nám, celý zápis
viz http://www.psp.cz/eknih/2002ps/stenprot/048schuz/s048061.htm a výňatky v přílohách tohoto článku (gramaticky neupravováno, stenografický záznam)

Odpoledne

Zřejmě po „televizním“ dotazu na ministerstvo spravedlnosti se odehrála scénka, kdy pan doc. Šámal, tvůrce návrhu TZ, hodinu řve na pana profesora rektora VŠFS Smejkala, co to navrhl za blbost v pozměňovacím návrhu. Netuší, že to není návrh jeho magnificence pana rektora, ale návrh můj a IURE.
Škoda, že jsem u toho nebyl :-)), protože jsem to stejně slíznul později od jeho magnificence a budu muset koupit láhev červeného na usmířenou.

PSP 11.10, 18 hodin

.....střih....
Bodem našeho jednání je bod číslo 15 a tím je Vládní návrh zákona - trestní zákoník....

Tento návrh zákona jsme projednávali ve druhém čtení na 45. schůzi, kdy jsme po obecné rozpravě návrh vrátili ústavně právnímu výboru k novému projednání. Ústavně právní výbor návrh zákona znovu projednal a jeho usnesení jsme obdrželi jako sněmovní tisk 744/2.

Místopředseda vlády a ministr spravedlnosti ČR Pavel Němec: ... tento návrh byl opětovně projednáván v ústavně právním výboru a doznal některých změn a doplnění....
Za prvé ústavně právní výbor reagoval na určité pochybnosti, které panovaly na plénu Poslanecké sněmovny ohledně navrhovaného formálního pojetí trestného činu. Právě proto, aby byly rozptýleny pochybnosti, které byly vznášeny i v prvém čtení v Poslanecké sněmovně, tak ústavně právní výbor se souhlasem předkladatele **doplnil toto formální pojetí o tzv. materiální korektiv** v podobě výkladového pravidla, které stanoví, jakým způsobem mají být vykládány znaky trestného činu. Tedy podle tohoto pravidla bude moci být jako trestný čin považován jen čin společensky škodlivý. Toto výkladové pravidlo má zajistit, aby nedocházelo na základě formálního pojetí k trestnímu stíhání v bagatelních případech.
.....

18.10 hodin

OBECNÁ ROZPRAVA

Poslanec Karel Vymětal: ..... se budu věnovat jen jedné odborné oblasti, která je obsažena v trestním zákoníku a kterou tady ve svém úvodním slově pan ministr spravedlnosti do značné míry zlehčoval. Ta se týká § 205. Je to mně velmi blízká problematika ochrany informačních systémů. Koneckonců sám jsem slaboproudý elektroinženýr, kdysi jsem i programoval.
Dámy a pánové, jestli vám něco říká obor kryptoanalýza nebo obor penetrační testování informačních systémů, dovolte, abych řekl několik slov o těchto oborech. Moderní kryptoanalýza je věda o hledání slabin a prolamování matematických metod informační bezpečnosti. Na druhé straně je její výsledky možné chápat a využívat jako návod na zneužití rozpoznaných slabin ke skutečné nezákonné činnosti. A mezi těmito dvěma póly je vel mi citlivá hranice. Trestní zákoník by měl být podle mého názoru upraven tak, aby nebyly vůbec žádné pochyby o tom, že je umožněna svoboda slova a svobodná výměna idejí v této vědě.

Penetrační testování je praktická činnost ob jednaná vlastníkem informačního systému k odhalení bezpečnostních slabin systému, kdy jsou dodavatelem prováděny takové činnosti, které se z technického hlediska neodlišují od nezákonných činností proti tomuto systému. I zde samozřejmě v této oblasti je velmi citlivá hranice mezi oprávněností a neoprávněností. Určitou formou penetračního testování je i odborná činnost administrátorů počítačových sítí, kteří používají nástroje k odhalování slabých hesel uživatelů, a to s cílem je vyloučit z použití, nikoli je zneužít. Dále je to činnost vývojářů, kteří tyto prostředky tvoří. Podobných činností je více a nelze je tady všechny vyjmenovat. I zde by trestní zákoník měl být upraven tak, aby nebyly žádné pochyby o tom, že tyto činnosti jsou oprávněné a zákonné.
Aby tato problematika byla přesně stanovena, byla 23. listopadu v roce 2001 v Budapešti přijata Úmluva Rady Evropy o počítačové kriminalitě č. 185, kterou je Česká republika vázána a v ní se v článku 6 nazvaném Zneužití zařízení v jeho odstavci 2 píše.. "Tento článek nesmí být vykládán takovým způsobem, který by zahrnul pod trestní odpovědnost takovou výrobu, prodej, zprostředkování, užití, dovoz, distribuci nebo jiné zpřístupňování nebo držení zmiňované v odstavci 1 tohoto článku, která nemá za účel spáchání přečinů uvedených v článcích 2 až 5 této úmluvy, jako např. pro oprávněné testování a ochranu počítačového systému. " Dámy a pánové, tolik mezinárodní úmluva, kterou je Česká republika vázána, jak jsem řekl.
A nyní, co se stalo. Vláda nám předložila v tisku 744 návrh trestního zákoníku a v jeho § 205 odst. 1 znění, ve kterém je uvedeno, že: Kdo neoprávněně vyrobí, uvede do oběhu, doveze, vyveze atd. včetně přechovává za b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačovému systému nebo jeho části, bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti. Konec citátu. **Ani**

slůvko o tom, že se tak musí stát s úmyslem spáchat trestný čin. A v tom je onen problém, kterým se dostal vládní návrh zákona do rozporu s citovanou úmluvou Rady Evropy, ale myslím si, že pro mnohé odborníky i se zdravým selským rozumem. (*vídíte, už je tady Sedlák, při prvním čtení jsem si ho nevšiml, ale jak je vidět, v Parlamentu někde sedí, pozn. VK*) **Pokud by totiž takové znění zákona bylo přijato, trestnou by se stala výuka kryptoanalýzy na vysokých školách nebo činnost administrátorů počítačových sítí, kteří se starají o jejich bezpečnost**. Oni totiž vědci, kryptoanalytici a bezpečnostní pracovníci se metodami práce a technickými prostředky ničím neliší od hackerů. Liší se pouze a jenom v cíli svého snažení - hackeři chtějí spáchat trestný čin a vědci se snaží trestnému činu zabránit.
Mezi odborníky na informační technologie je běžné, že se informace o zranitelnosti v počítačových systémech zveřejňují, o problémech se otevřeně diskutuje a různé demonstrační a testovací nástroje jsou volně dostupné. Pro tyto různé nástroje samozřejmě existuje dvojí využití - mohou být zneužity ale zrovna tak je může odborník používat k testování bezpečnosti systému, demonstraci zranitelnosti systému, ke studiu apod. Různě nebezpečné nástroje vytvářejí jak hackeři, tak i odborníci na bezpečnost, kteří tak právě tento nástroj analyzují, navrhují protiopatření, diskutují nad možnostmi řešení a nástroj lze i zveřejnit, aby se mohli bezpečnostní odborníci podle něj zařídit a chránit svěřené sítě.
Rozdíl mezi hackerem a přednášejícím kryptoanalýzu na Univerzitě Karlově je pouze a jenom v tom cíli. Oba dva mohou přechovávat, vytvářet a jinak pracovat se stejnými prostředky. Kryptoanalytik vyvíjí a používá tyto prostředky k odhalování slabin systému s cílem navrhnout protiopatření a zodolňovat je, hacker s cílem spáchat trestný čin. A protože rozdíl mezi nimi je jen a pouze, v jakém úmyslu tak činí, proto úmluva výslovně požaduje, aby podmínkou trestnosti byl protiprávní cíl.
Stejně tak je tomu u administrátorů počítačové sítě. Když podle nějaké nové kryptoanalytické metody vytvoří nebo použije program, který odhaluje slabá přihlašovací hesla, metodou práce se nijak neliší od hackera. Jeho úmyslem je zjistit, zda uživatelé nepoužívají slabá hesla a zabránit tomu, aby se systém nemohl stát předmětem útoku hackerů. Úmyslem hackera naopak je slabá hesla využít a do systému proniknout.

Oba dva opět použijí stejné prostředky a metody, ale liší se jedině a pouze právě úmyslem. Z toho, co jsem přednesl, je snad i laikovi jasné, že znění § 205 se musí změnit, a to tak, aby tyto činnosti byly trestné pouze tehdy, pokud jsou používány s úmyslem spáchat trestný čin neoprávněného přístupu k počítačovému systému a k použití a zneužití záznamů v něm atd. Pod protestem proti stávajícímu znění § 205, který mnozí z nás obdrželi, jsou desítky jmen významných vědeckých a bezpečnostních pracovníků. Mohu jmenovat doktora Klímu, docenta Matyáše, profesora Čapka z univerzity z Pardubic, doktora Matějku, vědeckého pracovníka Ústavu státu a práva Akademie věd a další a další, které bych tady mohl jmenovat dále.
Dámy a pánové, byl jsem si vědom těchto skutečností, a proto jsem předložil ústavně právnímu výboru 19. září letošního roku, i když jeho reprezentanti mě momentálně neposlouchají, **před jeho jednáním řešící pozměňovací návrh včetně odůvodnění, a to písemně obdrželi péčí paní poslankyně Rusové všichni členové tohoto výboru. Stala se neuvěřitelná věc. Ústavně právní výbor se rozhodl mým pozměňovacím návrhem se nezabývat, ač je to v rozporu s § 38 odst. 2 zákona o jednacím řádu Poslanecké sněmovny**, ve kterém se stanoví, že poslanci, kteří nejsou členy výboru, mají na schůzi výboru poradní hlas, mohou se k projednávané věci vyjádřit a podávat k ní návrhy, nemohou však hlasovat. Ano, nehlasoval jsem. Návrh jsem podal. Ústavně právní výbor se protiprávně rozhodl, že se tím návrhem zabývat nebude.

Je to opravdu neuvěřitelné, že ústavně právní výbor pokládaný za vysokou autoritu zákonnosti, elitu právníků a legislativců tak nepochopitelným způsobem sám poruší zákon. Dokonce na jednání padla otázka, jak jsem byl informován, zda si některý ze členů ÚPV můj pozměňovací návrh osvojí. Já bych rád tady plénu oznámil, že nepotřebuji, aby si mé návrhy někdo osvojoval, protože se cítím plnoprávným poslancem a žádného poručníka či zákonného zástupce nepotřebuji. Mně je upřímně líto našeho ÚPV a opravuji si svůj názor na jeho právní výlučnost a dokonalost. **Možná ale, že jednání ústavně právního výboru bylo ovlivněno názorem přítomného náměstka ministra spravedlnosti pana Romana Poláška, který údajně prohlásil, že s takovým pozměňovacím návrhem nebude nikdy souhlasit.** Ono to s tím zlehčováním asi, pane ministře, nebude tak jednoduché. Řekl bych, že, **když už odborné problematice pan náměstek nerozumí, tak snad by měl alespoň rozumět tomu, že stávající znění je v rozporu s mezinárodní úmluvou**, kterou je Česká republika vázána a která asi pro jistotu není zmíněna v důvodové zprávě, byť jich je tam uvedena velká spousta.

....střih....

Místopředseda vlády a ministr spravedlnosti ČR Pavel Němec: ..... V úvodním slovu jsem tady hovořil a pan zpravodaj Pospíšil o tom informoval také, že ústavně právní výbor přijal tzv. **materiální korektiv formálního pojetí trestného činu**, který mé tvrzení ještě zesiluje. Pokud bude trestní kodex přijat ve znění usnesení ústavně právního výboru, tak **podle tohoto výkladového pravidla lze za trestný čin považovat jen čin společensky škodlivý**. To všechno, co říká pan poslanec Vymětal, by byla pravda za předpokladu, že tvrdí, že badatelé a vědci dělají činnost společensky škodlivou. Jsem přesvědčen, že nedělají činnost společensky škodlivou, a tudíž ani nemohou být stíháni podle tohoto trestního kodexu.
Nicméně opakuji, že v zájmu toho, aby i badatelé a vědci měli klidné spaní, aby pan poslanec Vymětal byl spokojen, tak **jsme připravili pozměňovací návrh** (*no jo, ale pan doc. Šámal musel hodinu křičet..., pozn. VK*), který myslím si, že pan poslanec Vymětal má k dispozici. .....střih....(*poznámka: materiální korektiv formálního pojetí trestného činu byl ovšem přijat pouze na jednání ÚPV, a tak o něm pan poslanec nemohl vědět, ani občané pane ministře, ani náš Sedlák pane ministře..., pozn. VK*)

Poslanec Jiří Pospíšil: .... **materiální korektiv, který právě oddělí jednání, které má formální podobu skutkové podstaty trestného činu, ale chybí tam škodlivá stránka. Chybí tam ta společenská nebezpečnost nebo škodlivost**. .... Nikdy nebudeme schopni, a to je právě kouzlo práva, najít dokonalé, pregnantní, kazuistické vymezení všech možných alternativ, které mohou v lidském životě nastat. Vždycky je tu určitá generalizace, určitá obecnost, což je vůbec základní definice práva, a proto jsme vrátili materiální korektiv.

.....střih....

Poslanec Jiří Pospíšil: Dámy a pánové, jen na závěr obecné rozpravy chci říci, že byla na ústavně právním výboru uzavřena jakási gentlemanská dohoda, lze-li to takto říci, že **poté, co budou přečteny pozměňovací návrhy, se ústavně právní výbor sejde, sejde se se zástupci navrhovatele, a jednotlivé navržené pozměňovací návrhy prostuduje a nechá si od navrhovatelů a od jejich odborného zázemí sdělit, na kolik tyto návrhy jsou v souladu či v rozporu se systematikou celého kodexu.** .....střih....To tedy pouze na vysvětlenou, jaký tedy bude případný postup po skončení druhého čtení.

-o-o-o-

Tak tohle byla tzv. obecná rozprava, kdy se ještě nečtou konkrétní pozměňovací návrhy.

Mezitím běžela na NOVĚ ona reportáž v 19:30.

V 19:38 jsem od pana poslance Böhnische dostal návrh, který zřejmě odpoledne v reakci na dění kolem zpracoval autor TZ Doc. JUDr. Pavel Šámal, Ph.D. (**označme ho pracovně jako tzv. Šámalův návrh)** se žádostí o náš názor. Podívejme se na něj.

Šámalův návrh

§ 205

Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

(1) Kdo v úmyslu spáchat trestný čin porušování tajemství dopravovaných zpráv podle § 157 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořené nebo přizpůsobené k neoprávněnému přístupu do veřejné komunikační sítě, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačové**ho** systému nebo k jeho části,

bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
(2)..(3)

Končilo úterý, další den měla následovat podrobná rozprava, kde už se měl číst přímo pozměňovací návrh (bylo to nakonec odloženo na čtvrtek). Jenže jaký návrh? Náš původní nebo Šámalův? A kdo ho přednese?

Tak vznikl tento email

-oOo-

Od: v.klima@volny.cz
Předmět: Re: Odp: 16.bod programu , Novy TZ - problematicke ustanoveni § 205
Komu: "Robin Bohnisch" <bohnischr@psp.cz>
Datum: Úterý, 11. října 2005 - 21:14:02
Kopie: svatosova@iure.org

Pane poslance,
velice Vam dekuji za angazovani se v teto veci. Text jsem si prostudoval a prodiskutoval i pani JUDr. Svatosovou z IURE. Oba dva souhlasime s navrhem § 205, ktery doc. Samal uvedl jako posledni v textu , pouze je potreba opravit preklep v pismenu b) pocitacoveho-mu systému.

Vzniká ideální situace, kdy bude predkladatel souhlasit se svym pozmenenym navrhem. Muzete tlumocit i nase souhlasne stanovisko. Rozdil mezi nasim navrhem a navrhem doc. Samala nam nevadi.

Pokud se chcete domluvit na tomto pozmenovacim navrhu sireji, stacilo by se domluvit s

poslanci Vymetalem + Konecna(KSCM) a Novotnym(ODS), kteri budou podporovat nas navrh.

Jeste jednou dekuji a preji hodne zdaru zitra.
Vlastimil Klima

-oOo-

Čtvrtek, podrobná rozprava, třetí studená sprcha

Ve čtvrtek 13. 10. pokračovala podrobná rozprava v 9:00. Pustil jsem si ji živě a nestačil jsem zírat.

PSP:
Poslanec Karel Vymětal: Děkuji za slovo, dámy a pánové, vážená vládo, chtěl bych v úvodu ocenit sílu sdělovacích prostředků, protože k inkriminované věci - § 205 - se v úterý večer ve zprávách zapojila televize Nova a zdá se, že to bylo významným impulzem i k tomu, aby Ministerstvo spravedlnosti se zamyslelo nad problémem, o kterém jsem zde hovořil v obecné rozpravě.

A nyní k vlastnímu pozměňovacímu návrhu. Bude se týkat pouze § 205 odstavce 1. Chtěl bych říci v úvodu, že k debatě, která ještě byla vedena včera v obecné rozpravě, že se domnívám, že k tomu, aby někdo spáchal trestný čin, je u této věci nepodstatné, **zda vlastní ty prostředky oprávněně či neoprávněně**. Tam je podstatné **ten úmysl spáchání trestného činu**. Takže jsem přesvědčen o tom, že ta **neoprávněnost** v úvodu tohoto odstavce je nadbytečná a zbytečná.

....střih....

Dámy a pánové, navrhuji změnit znění § 205 odstavce 1 takto: 1) Kdo vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoliv jiný prostředek, včetně počítačového programu, nebo b) počítačové heslo, přístupový kód, postup nebo podobná data, pomocí nichž lze získat přístup k počítačovému systému nebo jeho části, a teď pokračuje text, který patří k oběma částem, vytvořené nebo přizpůsobené v úmyslu spáchat trestný čin neoprávněného přístupu k počítačovému systému a poškození a zneužití záznamu v počítačovém systému a na nosiči informací podle § 204 nebo trestného činu porušování tajemství dopravovaných zpráv podle § 157 odstavec 1 písm. b), c), bude potrestán odnětím svobody až na jeden rok, propadnutím věci nebo zákazem činnosti.
Děkuji vám za pozornost.

....střih....

Pokud se podíváte pozorně, není to návrh VK-IURE! Je to tzv. Smejkalův návrh. Pan rektor by teď mohl být spokojen.
Jenže mě polilo horko a studená vlna už potřetí. A tak se zapnutým videem z on-line jednání sněmovny jsem žhavil mobily. Nejdřív pana poslance Vymětala. Pak dalších a dalších. Pak SMS-ky. Pak poradci. No a mezitím vystoupil pan poslanec Böhnisch (ČSSD).

PSP

....střih....

Poslanec Robin Böhnisch: Dobrý den, dámy a pánové, rád bych se jen přihlásil k mému pozměňovacímu návrhu, který byl rozdán včera dopoledne na vaše lavice. Cítím potřebu

dodat, **že se týká již několikrát zmiňovaného § 205 navrhovaného trestního zákoníku, a zároveň bych rád dodal, že jde o text, který navrhl pan docent Šámal, hlavní autor tohoto kodexu, a tento text je kompromisem mezi současným zněním a mezi textem navrhovaným odborníky z oboru kryptoanalýzy, který tu do značné míry prezentoval pan kolega Vymětal. Ještě dodávám, že s tímto textem, který byl včera dodán, souhlasí-li i tito odborníci z oboru kryptoanalýzy a počítačových systémů.** Děkuji.

.

....střih....

Následuje můj telefonát s poslancem Vymětalem.
Nezkoumám, jak se ztratil návrh VK-IURE., ale raději jdu k věci. Pan poslanec si nechal vysvětlit rozdíl mezi tzv. Smejkalovým návrhem a VK-IURE a Šámalovým návrhem. Vše snadno a rychle pochopil a gentlemansky zareagoval!

.....střih....

Pan poslanec volá, že vše zařídil, že se domluvil se svým klubem a poslanci Pospíšilem a Böhnischem a ve třetím čtení stáhne svůj návrh, resp. podpoří návrh pana poslance Böhnische.

V zápětí nato dostávám email:
Od:"Robin Bohnisch" <bohnischr@psp.cz>
Předmět:Re: Odp: 16.bod programu , Novy TZ - problematicke ustanoveni § 205
Komu:v.klima @volny.cz
Datum:Čtvrtek, 13. října 2005 - 13:50:53

Dobry den,
s kolegou Vymetalem jsem uz mluvil a vyjasnili jsme si pozice. Nastesti jsem ho vcera neposlechl a predlozil ten Samaluv text. Ted je otazka, jestli zmenu celeho paragrafu 205 Snemovna podpori, anebo zustane v nezmenene podobe. Ale hadam, ze tento pozmenovaci navrh projde. Bylo mi cti spolupracovat, budeme spolecne ocekavat 3. cteni.
Zdravi
Robin Bohnisch

-oOo-

Třetí čtení nás čeká **za několik dní**, což bude záviset na rychlosti projednávání i jiných zákonů v PSP.

Další informace je v přílohách, zejména doporučuji přečíst dopis poslancům. Již přetahuji původní povolenou délku článku, ale nezmínil jsem tady spoustu věcí důležitých, jako je pomoc mnoha dalších zatím nejmenovaných lidí a např. to, že pan doc. Tůma kvůli tomu telefonoval a faxoval z Austrálie a ještě spoustu dalších zajímavostí. Až bude zákon přijat, změní se tam pár řádek, ale řeknu vám, že nás stály hodně času a úsilí. Děkuji VŠEM, koho jsem zde jmenoval i nejmenoval, ale podílel se na změně § 205 zákona.

Čtvrtek, 13. 10. 23:30
Vlastimil Klíma

C. Hardening GNU/Linux, část 2.
Časté problémy a chyby administrátorů

Josef Kadlec, student FJFI ČVUT Praha, (josef.kadlec@gmail.com)

Špatně nastavená PATH

Někteří uživatelé, v horším případě i superuživatelé, si zjednodušují práci tím, že si přidávají adresář "." do proměnné systémového prostředí $PATH. Výhody to má takové, že jim potom stačí psát pouze *mujprogram* místo *./mujprogram* či *sh mujprogram*.

Podívejme se, co se stane, když někdo vytvoří „zákeřný program“ s názvem běžně užívaného příkazu jako například *ls*, *who* nebo *ps*. Pokud je adresář "." v proměnné *$PATH* před adresářem, ve kterém se nachází program, jehož názvu chceme zneužít a uživatel napíše příkaz, jehož názvu zneužíváme - například *ls*, znamená to, že se spustí náš zákeřný program, který v případě spuštění uživatelem nebo superuživatelem může vést k přímé kompromitaci systému s nejvyššími právy a záleží jen na útočníkově fantazii, jak bude vypadat kód zákeřného programu - může posílat obsah souboru */etc/passwd* na určitou e-mailovou adresu nebo může například vytvořit setuid shell v adresáři */tmp* a umožnit sobě a ostatním uživatelům používaní shellu s právy superuživatele. Zákeřný kód může obsahovat pasáž, kde se vykoná původní záměr uživatele a ten nemusí vůbec nic poznat.

Je možno zneužít i situaci, kdy se "." nachází na konci proměnné *$PATH* a to například využitím názvu programu, který není v systému nainstalován a uživatel se ho pokouší spustit nebo využitím toho, že se uživatel někdy překlepne a napíše například místo příkazu *nice* příkaz *ncie*.

Obrana je jasná, nepoužívat adresář "." v proměnné *$PATH*. Superuživatel by měl také zajistit odstranění všech výskytů přidání tohoto adresáře do cesty především v souborech */etc/profile*, */etc/bashrc*a v domovských adresářích v souborech *.bashrc* a *.bash_profile*. Bezradný bude v hledání a odstraňování tohoto zavedení proměnné *$PATH* v binárních aplikacích.

Problém setuid a setgid programů

Setuid (programy, které mají v masce práv nastaven tzv. efektivní bit s) jsou programy, které po spuštění uživatelem běží s právy vlastníka (v případě setgid s právy skupiny, která se k souboru vztahuje). Takovéto programy mohou být zvláště nebezpečné, pokud je jejich vlastník superuživatel *root* (tzv. *root-setuid* nebo *root-setgid* programy) a navíc mohou být spouštěny kýmkoliv. Jedná se například o programy */usr/bin/at*, */usr/bin/passwd*, */bin/ping*, */bin/mount*, */bin/umount*, */usr/bin/chfn*, atd. Root-setuid programy (čili ty „nejnebezpečnější“) můžeme najít příkazem *find* například takto:

find / -perm -4000 -uid 0

Jak vidíme, mezi tyto programy patří soubory, které používáme velmi často. V těchto programech se v minulosti objevila spousta chyb, které často, i když v některých případech nepřímo, vedly k získání nejvyšších pravomocí. Příkladem může být chyba v programu */usr/bin/man*, která vedla k získání práv skupiny *man*. Tyto soubory bychom měli omezit tak, aby je mohla spouštět jen omezená část uživatelů. Toto můžeme realizovat dvěma způsoby. První je ten, že vytvoříme skupinu, která bude mít jediná přístup k danému setuid programu.

Druhům způsobem je použití programu *sudo* (http://www.courtesan.com/sudo), což je komplexnější řešení než první způsob. Konfigurace *suda* může být zprostředkována pomocí souboru */etc/sudoers*, který může vypadat například takto:

```
Host_Alias LOCAL = localhost
Cmnd_Alias MOUNT = /bin/mount /dev/hda1 /mnt/hda1
pepa   LOCAL=NOPASSWD:MOUNT
}
```

Tato konfigurace umožní uživateli *pepa*, který je přihlášen z localhostu připojení diskového oddílu */mnt/hda1* příkazem:

```
/bin/mount /dev/hda1 /mnt/hda1
```

a *sudo* nebude vyžadovat heslo. Pokud daný setuid (setgid) program nepotřebujeme, měli bychom ho odstranit. Pokud můžeme sejmout setuid bit, opět bychom tak měli učinit v rámci odstranění bezpečnostních rizik. Ale bohužel ve většině případů znamená tato akce nesprávnou funkčnost nebo úplnou nefunkčnost daného programu.

Omezení uživatelů pomocí kvót a limitů

Někteří uživatelé se domnívají, že jsou v systému sami a může dojít například k tomu, že uživatel využije celý procesorový čas stroje a tím znemožní práci ostatním uživatelům. Samozřejmě k tomu může dojít i nechtěně, jako se stalo například mně, když jsem na systému, kde kvóty a limity nebyly nastaveny, zaplnil celý diskový prostor v oddílu */home* v důsledku nesprávného běhu mého programu. Tak nebo tak je potřeba těmto situacím předcházet a uvalit na uživatele limity a kvóty.

Pokud chceme zamezit právě tomu, aby někdo zabral velkou část diskového prostoru, využijeme kvót. Abychom mohli kvóty používat, musíme v souboru */etc/fstab* přidat parametr *usrquota* či *grpquota* k oddílu, na kterém chceme kvóty používat. Dále na daném oddíle vytvoříme soubory *quota.user* a *quota.group* nejlépe s právy *600*. To, jestli je vše správně nastaveno, si můžeme ověřit příkazem:

```
quotacheck -avug
```

Samotné zapnutí kvót se provádí příkazem *quotation* bez parametrů. Přidání kvóty například pro uživatele *pepa* může vypadat takto:

```
edquota -u pepa
```

Tento příkaz spustí textový editor, který máte určený systémovou proměnnou *$EDITOR* (v mém případě je to důvěrně známý editor *vim*), ve kterém vidíte informace se současnými kvótami, které můžete editovat. Nastavit můžete překročitelný (soft) limit, při kterém bude uživatel jen upozorněn a nepřekročitelný (hard) limit, který překročen být nemůže. Hodnota nula znamená, že uživatel nemá nastavenou kvótu. Pokud bychom chtěli nastavit stejné kvóty jako má uživatel *pepa* například pro uživatele *karel*, provedli bychom to takto:

```
edquota -p pepa karel
```

Dále si představíme příkaz *ulimit*, který nám umožňuje omezit kromě velikosti datového segmentu například množství procesorového času, počet otevřených souborů, velikost souborů core, počet spuštěných procesů, atd. Omezení lze provést záznamem do souboru */etc/profile* a tím omezit všechny uživatele přihlašující se do systému. Další možností editování limitů je editace souboru */etc/security/limits.conf*, kde jsou informace seřazené ve formátu:

domain type item value

Domain je uživatelské jméno nebo název skupiny, který po znaku "@" nebo znaku "*" znamená všechny uživatele uvedené skupiny. *Type* může nabývat hodnot *soft* nebo *hard*, které jsou totožné s významem u kvót. *Item* označuje zdroj, který chcete omezit - například *cpu*, *nproc*, *maxlogins*, atd. *Value* je pak hodnota příslušného omezení.

Jak jsem již zmínil, omezení pro uživatele by mělo být co možná nejstriktnější. Abychom zbytečně neomezovali důvěryhodné uživatele, je možné vytvořit více skupin s různými omezeními. Jako systémoví správci tím předejdeme mnoha problémům.

Omezení práv superuživatele

S právy superuživatele bychom měli spouštět opravdu jen procesy, které to vyžadují. Co byste měli přímo zakázat, je např. používání programu *telnet* nebo FTP klienta z důvodu zamezení odchycení nezašifrovaného hesla superuživatele. Tento zákaz lze realizovat například přes TCP wrappers, ale to už bych příliš zasahoval do síťové vrstvy. Někdy je lepší vzdálené přihlašování superuživatele úplně zakázat. Takové SSH spojení se pak realizuje přes běžného uživatele připojením na daný systém, kde se privilegované operace provádí např. přes *su*.

Našli bychom i další příklady restrikce práv superuživatele. Některé nám nabízí projekt Bastille, o kterém se zmíním v následujícím pokračování tohoto seriálu. Existují také různé kernelové úpravy, kterými lze linuxový systém přeměnit tak, že práva uživatele *root* nebudou ta nejmocnější. Jedna z takových úprav se nazývá *Security-Enhanced Linux* (zkráceně SELinux) a domovská stránka projektu se nachází na URL http://www.nsa.gov/selinux/ .

Jistou restrikci práv superuživatele lze také provést pomocí souboru */etc/securetty*. Tento soubor umožňuje definovat, ze kterých TTY a VC (virtuální konsole) zařízení se může superuživatel přihlásit. Pokud nechcete, aby dané zařízení bylo funkční, zakomentujte příslušný řádek v tomto souboru. Program */bin/login* bude akceptovat pouze nezakomentované řádky a k němu příslušná zařízení.

Vypnutí a odstranění nepotřebných služeb a softwaru

Každá služba představuje jakési pomyslné dveře do systému, které může vetřelec využít k průniku. Je velmi pravděpodobné, že po instalaci vaší distribuce najdete služby, které potřebovat nebudete. Může se jednat například o web server, FTP server či drobné služby jako ECHO a chargen. Vidíme, že se jedná především o síťové služby. Pokud danou službu nepotřebujete, měli byste ji vypnout. Pokud víte, že službu nikdy potřebovat nebudete, můžete ji vymazat a tím znemožnit spuštění nepřítelem, který by si třeba chtěl takto zajistit přístup do systému. Seznam naslouchajících procesů můžeme vypsat příkazem *netstat* nejlépe takto:

netstat -atuvp

Další možností je použití příkazu *ps*, který může vypsat všechny běžící procesy, a následné důkladné prozkoumání každé z nich, zdali je potřebná, či nikoli.

To, jestli daná služba bude spuštěna, či nikoli, můžete ovládat pomocí spouštěcích skriptů (spouštěcí skripty unixového typu System V se nacházejí v adresáři */etc/rc.d/*) a další především nativnější služby se ovládají pomocí */etc/inetd.conf* (nebo */etc/xinetd.d/**). Vyšší bezpečnosti docílíme spuštěním minima služeb.

Mezi služby, které znamenají vysokou míru rizika, nedají se nijak účinně zabezpečit a na systému, který je označen jako bezpečný, by se rozhodně objevit neměly, patří např. *finger, telnet, R* služby, rsh, rcp, rexec, echo, chargen, talk, ntalk, ytalk, rwhod, rwalld, TFTP, X window, emulátory, apod.* Tyto programy již nejsou v současné době nutné a nebo našly své bezpečnější alternativy.

Udržování aktuálních verzí softwaru

Samozřejmě i v Linuxu se nacházejí chyby. Každou chvíli jsou nacházeny chyby v softwaru nebo samotných jádrech operačních systémů. Může se jednat o různě závažné chyby. Některé chyby mohou vést rovnou k získání nejvyšších oprávnění, jiné například k získání práv skupiny *man*. Dále bychom mohli rozdělit chyby na lokálně a vzdáleně zneužitelné. Lokálně zneužitelné chyby jsou chyby, kterých lze zneužít pouze v případě, pokud máme na daném systému uživatelské konto. Vzdáleně zneužitelné chyby pak může zneužít prakticky kdokoliv vzdáleně.

Minimem, které by každý linuxový administrátor měl splnit, je pravidelná instalace bezpečnostních záplat (angl. *patches*). V případě větších distribucí jsou tyto záplaty většinou pravidelně umisťovány na jejich stránkách. Pokud máte nějaký software, který přímo neposkytuje vaše distribuce, je potřeba sledovat domovské stránky daného softwaru. Spoustu informací o aktuálních problémech lze také nalézt ve specializovaných konferencích a poštovních konferencích (mailing listech). Jednou z nejznámějších konferencí, kde je probírána problematika bezpečnosti, je konference Bugtraq - archiv konference přístupný z webu na URL http://www.securityfocus.com/archive/1.

Po aplikování záplaty není většinou potřeba restartovat systém, kromě aplikace některých jaderných záplat.

Volba bezpečných hesel

Pokud budete vy a vaši uživatelé používat slabá systémová hesla, velmi usnadníte útočníkovi přístup do vašeho systému, protože je to jedna z věcí, kterou crackeři zkoušejí nejdříve. Pokud se bude jednat o slabé heslo ke kontu superuživatele, je situace alarmující. Heslo by měla znát opravdu jen osoba (může to být i více osob), která má oprávnění ho používat, a samozřejmě by nemělo být lehce uhodnutelné. Cracker může vaše heslo podrobit slovníkovému útoku nebo útoku hrubou silou, kde většinou záleží na délce a složitosti (paletě použitých znaků) hesla, jak bude odolné - čím delší a složitější, tím déle bude trvat crackerovi prolomení tohoto hesla. Existují i další specializované útoky.

Jedním ze způsobů, jak kontrolovat to, zdali si uživatel zvolil bezpečné heslo, je ten, že se vžijeme do role crackera a pokusíme se hesla uživatelů prolomit. K tomu můžeme použít

například program *John the Ripper* (http://www.openwall.com/john/). Samozřejmě záleží na výpočetním výkonu počítače, který by útočník použil, ale určitý obrázek o stavu hesel uživatelů na našem systému si můžeme udělat. Jen bych chtěl upozornit, že k tomuto kroku byste si měli vyžádat písemný souhlas vašich nadřízených, abyste se sami nedostali do problémů. Existují i moduly do programu *passwd*, které se snaží automaticky heslo uživatele prolomit.

Další možností je použít knihovnu *cracklib* z PAM (o PAM budu podrobněji mluvit později). Tato knihovna analyzuje hesla a snaží se je prolomit. Pokud chceme tuto možnost aktivovat, je potřeba do souboru */etc/pam.d/passwd* napsat:

```
passwd password requisite /usr/lib/security/pam_cracklib.so retry=3
passwd password required /usr/lib/security/pam_pwdb.so use_authtok
```

Pozn. pro uživatele Slackware Linuxu: je ještě potřeba nainstalovat příslušný slovník a zapsat do souboru */etc/login.defs*:

```
CRACKLIB_DICTPATH		/var/cache/ceacklib/cracklib_dict
```

Abychom zabránili nežádoucím důsledkům plynoucích z používání slabých hesel, je potřeba inkriminované jedince donutit k používání bezpečných hesel (nebo striktně slabá hesla nepovolovat) a také samotnému zacházení s tímto heslem, což by mělo být zmíněno v případné bezpečnostní politice dané sítě.

Příznaky připojování

Samotnému příkazu *mount* nebo v souboru */etc/fstab* můžeme definovat příznaky (angl. *flags*) pro zvýšení bezpečnosti. Prvním příznakem je *nodev*, který řekne jádru, aby nerozpoznávalo žádné soubory zařízení. Toto je užitečné především u jednotek CD či DVD-ROM nebo NFS. Dalším flagem je *noexec*, který zakáže na příslušném oddílu provádění spustitelných souborů, které vyvolává jádro. Příznak *nosuid* zapříčiní to, že nebudou akceptovány příznaky set-UID a set-GID. Příznakem *ro* se připojí daný oddíl pouze pro čtení.

Jak už jsem zmiňoval, adresář */boot* by měl mít přístupová práva jen pro čtení. Pokud máme tento adresář na zvláštním oddílu, což je relativně časté, můžeme elegantně využít příznak *ro* a docílit tak stejného efektu.

Problém adresáře /lost+found

Distribuce Red Hat, Fedora Core, Mandrake, Slackware a další vytvářejí v současných verzích adresář */lost+found* s přístupovými právy *755*. Do tohoto adresáře se ukládají případné ztracené soubory nalezené programem *fsck* po náhlém pádu systému. Souborový systém Ext2 totiž nemá žurnál, který této události dokáže předcházet. Problém je, že tomuto adresáři je povolen přístup pro všechny uživatele. Řešením je restrikce práv na mód *700* nebo používání žurnálovacích souborových systémů - například Ext3.

Bezpečné odstraňování souborů

Problém je v tom, že když v Linuxu (na souborovém systému Ext2 nebo Ext3) vymažete soubor, Linux pouze označí datové bloky, které soubor zabíral, jako volné, ale skutečný obsah

na disku stále je, dokud ho nepřepíše nějaký jiný. To si můžeme ověřit příkazem *grep*, který prohledává neformátované diskové zařízení a hledá v blocích vámi nadefinovaný text.

Jedním ze způsobů, jak odstranit obsah souborů, které jsme již smazali, je zaplnění volné kapacity disku. To lze provést například příkazem:

cat /dev/urandom >> velky_soubor

Tento příkaz začne plnit soubor *velky_soubor* náhodnými znaky ze zařízení */dev/urandom* a tím dojde postupně k zaplnění celého oddílu. Je třeba si dávat pozor na limity, kterými můžeme mít určenou maximální velikost souboru. Velikost souboru také určuje souborový systém Ext2 a to na hodnotu 2 GB, takže v případě oddílu, který je větší než 2 GB, je potřeba vytvořit souborů s náhodnými znaky více, než dojde k úplnému zaplnění kapacity oddílu. Toto je ovšem zejména účinné, pokud tento soubor vytváříme s právy superuživatele. Jen bych chtěl upozornit, že zaplněním celé diskové kapacity můžete ohrozit některé běžící procesy, a proto by toto mělo být vykonávané, pokud zrovna není nikdo přihlášen v systému.

Tento postup se však hodí spíše v situacích, kdy chce uživatel nebo administrátor preventivně přepsat bloky dat, které jsou označeny jako volné a tím zamezit zpětnému extrahovaní dat. Pro případy, kdy chcete bezpečně odstranit nějaké soubory, je výhodné použít některé z programů pro tento účel určené.

Jednou asi z nejznámějších je program Wipe (http://wipe.sourceforge.net). Tento program přepisuje mazané soubory bezvýznamnými daty a to opakovaně. Pokud bychom mazané soubory přepsali pouze jednou (např. binární nulou), byla by tu možnost je extrahovat pomocí metody MFM (Magnetic Force Microscopy). Takže se jedná opravdu o velmi spolehlivé likvidování dat, protože několik posledních vrstev bude tvořit jen bezcenná paměť.

Je zde možnost sáhnout po alternativách jako BCWipe
(http://www.jetico.com/index.htm#/linux/).

Vidíte, že aspektů, které je nutno hlídat, je opravdu dost. Možná vám některé přijdou banální a jasné, ale skutečně je každá ze zmíněných věcí pro každého z vás samozřejmostí? Některé problémy zanikají s postupným vývojem samotného operačního systému – např. snadnější nebo automatické aktualizace softwaru a instalovaní bezpečnostních patchů, a nebo nezmíněný problém zastíněných hesel, která jsou snad implicitně zapnuta ve všech současných verzích distribucí. Ale některé problémy asi jen tak nezaniknou a je potřeba je neustále ošetřovat a mít je na vědomí.

D. O čem byl CHES 2005 a FDTC 2005?

Jan Krhovják, Fakulta informatiky, MU, Brno
(xkrhovj@fi.muni.cz)

Tento článek stručně shrnuje několik hlavních témat (a do nich spadajících příspěvků) z workshopů Cryptographic Hardware and Embedded Systems (CHES) 2005 a Fault Diagnosis and Tolerance in Cryptography (FDTC) 2005, které proběhly na přelomu srpna a září ve skotském Edinburgu. Témata CHES pokrývají problematiku (bezpečného) hardware určeného pro kryptografické účely, jeho efektivitu, problémy spjaté s nedostatkem zdrojů, ale také útoky (nejen postranními kanály) na tento speciální hardware, či problémy související s aritmetikou používanou pro kryptografické operace. Témata FDTC pak pokrývají především útoky založené na chybové analýze a metody ochrany proti nim. Podrobné informace a kompletní příspěvky (v původním pořadí :-) lze nalézt ve sbornících [CHES05, FDTC05].

Speciální hardware

Tento blok byl věnován specializovaným hardwarovým zařízením, která souvisejí jak s kryptologií, tak také s kryptoanalýzou. První příspěvek pojednával o realizovatelném hardwarovém prosévacím zařízení SHARK, které by mělo být schopno uskutečnit prosévací část GNFS (General Number Field Sieve) pro 1024bitové číslo do jednoho roku. GNFS je (asymptoticky) nejlepší známý algoritmus pro faktorizaci velkých čísel s velkými faktory, který je složen z prosévací a maticové části (kde právě prosévací část je ta obtížnější). Cena takovéhoto zařízení je odhadnuta na méně než 200 milionů dolarů. Dále bylo popsáno hardwarové zařízení, které urychluje maticový krok GNFS pomocí řešení řídkých systémů lineárních rovnic. Jeho cena by měla být výrazně nižší než cena prosévacích zařízení. Na závěr byl představen návrh testovatelného (a bezstavového) generátoru skutečně náhodných bitů/sekvencí. Jako bezstavový je navržen jak digitalizovaný zdroj šumu, tak také digitální jednotka, která vygenerované bity zpracovává. Bezstavovosti je dosaženo pravidelným resetováním obou těchto hlavních částí generátoru (každé však v různých intervalech). Zváženy jsou také nejrůznější hypotetické možnosti útoků, jejich efektivní detekce a obrana proti nim.

Efektivní hardware

Tématem této části byly efektivní hardwarové implementace a hardwarové akcelerátory. Byly představeny dva návrhy implementací AES (jeden zaměřen na rychlost a druhý na úsporu plochy čipu a paměťovou nenáročnost) určené pro FPGA (Field Programmable Gate Array). Oba tyto návrhy ukázaly, kam až sahají hranice možností využití současné technologie FPGA pro implementaci AES. Dále byl popsán postup, jak implementovat co nejkompaktnější S-Box pro AES. Redukce velikosti S-boxu je oproti předcházející nejlepší kompaktní implementaci celých 20 %. To umožňuje jednak snazší implementaci AES do zařízení omezených plochou čipu (např. čipové karty), ale úspora místa může být u malých čipů také využita pro vytvoření více kopií S-boxu a tím i ke zvýšení stupně paralelismu při provádění *SubByte*. Pro jednoduché zvýšení paralelismu je sice potřeba pouze 16 kopií S-boxu pro jedno kolo, ale kdybychom chtěli (pro nezpětnovazební mody jako ECB a CTM) dosáhnout úplného pipeliningu, bylo by zapotřebí minimálně 160 kopií S-boxů (pro AES s délkou klíče 128 bitů a tedy s 10 koly). Další dva příspěvky se zabývaly urychlením některých specifických

algebraických operací (Tate pairing) nad konkrétními poli. Jejich hardwarová implementace je však náročná a lze zatím uskutečnit jen na zařízeních jako FPGA.

Nedostatek zdrojů

Tento blok byl věnován problematice omezených zdrojů (např. energie či paměť). Úvodní příspěvek pojednával o vytvoření energeticky nenáročných softwarových implementací algoritmů pro práci s modulární aritmetikou. Na základě podrobných analýz vybraných instrukcí RISCových procesorů (např. *load*, *store*, *add*, *mul*) byl vytvořen model pro srovnání spotřeby energie softwarových implementací těchto algoritmů. Dále byla popsána výkonná, avšak paměťově nenáročná metoda výpočtů skalárního násobku na Koblitzových křivkách. Úspora paměti je oproti doposud známým metodám v případě hardwarové implementace 85 % a v případě softwarové implementace 70 %. Na závěr pak byla představena kombinace hardwarové a softwarové implementace algoritmů pro práci s hypereliptickými křivkami (hardware obstarával výpočet inverze a násobků v binárních polích).

Hardwarové útoky a jejich prevence

V této části byl prezentován úspěšný DPA (Differential Power Analysis) útok na maskovanou hardwarovou implementaci AES. Útok je založen na energetickém modelu odvozeném ze simulací, které byly vytvořeny na základě velmi podrobných specifikací čipu (na úrovni jednotlivých hradel). Oproti běžným DPA útokům nevyužívá tento útok výstupních hodnot uložených v registrech, ale právě výstupních hodnot logických hradel. Naštěstí útočník v praxi většinou nemá přístup k podrobným specifikacím čipu, na jejichž základě by byl schopen vytvořit pro útok nezbytnou simulaci. Dále byl představen zcela nový typ logiky odolné proti DPA útokům – MDPL (Masking Dual-Rail Pre-charge Logic). Tato logika zajišťuje konstantní spotřebu energie tak, že používá pro přenášené signály zdvojené vodiče, z nichž jeden (v závislosti na přenášené logické hodnotě) je v každém hodinovém cyklu nabit a vzápětí vybit. Výhodou je, že MDLP lze implementovat pomocí běžně používané CMOS technologie, nicméně cenou, kterou zaplatíme za ochranu proti DPA, je zvětšená plocha čipu, zvýšená spotřeba energie a pouze poloviční rychlost. Na podobném principu pracuje i logika WDDL (Wave Dynamic Differential Logic), na jejímž základě byla vytvořena a prakticky testována hardwarová implementace AES. Oproti klasické implementaci AES pomocí CMOS technologie, u níž se pomocí DPA a 8 000 měření podařilo snadno získat 128bitový klíč, nebyl stejný útok na WDDL implementaci AES úspěšný ani s 1 500 000 měřeními (tj. v praxi by byl de facto neproveditelný). Byly navrženy také techniky vhodné pro technologii ASIC. V dalším příspěvku o maskování na úrovni hradel byl předveden nově vytvořený teoretický model spotřeby energie, který hrubě abstrahuje komplikovaný fyzikální proces rozptylování energie v aktivním CMOS obvodu. Poté byl prezentován popis několika pokusů o neinvazivní a semi-invazivní útoky, jejichž cílem bylo získání dat z vymazaných (nebo přepsaných) energeticky nezávislých paměťových modulů (jako např. UV EPROM, EEPROM či flash). Mnohé z útoků (především na nejnovější paměťové čipy) však byly neúspěšné. V dalším příspěvku byly popsány modely pro přímé vyhodnocování spotřeby energie v CMOS obvodu. Jejich pomocí lze simulovat odběrovou analýzu na mnoha existujících zařízeních.

Útoky postranními kanály

V tomto bloku byly představeny nové typy útoků postranními kanály. Prvním z nich je DPA útok na výpočet skalárního násobku bodu eliptické křivky. Tento útok je aplikovatelný bohužel právě na eliptické křivky, jejichž parametry jsou upraveny tak, aby umožnily snadnou implementaci do hardware s omezenými zdroji. Navíc překonává běžné anti-SPA a anti-DPA techniky obrany. Další DPA útok obchází ochranné náhodné maskování na čipové kartě tak, že využívá testovací kartu s ovlivněným RNG jako vzor k provedení útoku na kartu s perfektním RNG. Třetí DPA útok je zaměřen na blokové šifry (byl ověřen na hardwarové implementaci AES) a k zvýšení efektivity využívá speciálně navržený pravděpodobnostní model. Dalším typem útoku byla úspěšná EM analýza Rijndaelu a ECC implementovaných na PDA s podporou bezdrátového přenosu. Poté byly prezentovány bezpečnostní limity pro EM vyzařování (návrhy pro případný budoucí standard), jejichž dodržení by mělo zamezit únikům citlivých informací tímto postranním kanálem. A konečně, byla také navržena simulační metoda (založená na množství spotřebované energie a detailní znalosti čipu) pro zjišťování míry EM vyzařování v CMOS obvodech. Její praktická využitelnost je však především ve fázi návrhu čipu. Poslední dva příspěvky pak pojednávaly o DPA útocích vyšších řádů, kterým nelze zabránit ani často používanou ochranou maskováním.

Trusted computing

Jediný příspěvek v této části se zaměřil na problematiku bezpečné správy dat (což pokrývá životní cykly software, ale i hardware). Byly identifikovány hlavní nedostatky ve specifikaci TCG, které způsobují v současné době největší překážky pro nasazení TC ve velkém měřítku, a byla představena (a navržena ke standardizaci) také řešení těchto nedostatků.

Aritmetika pro kryptografii a kryptoanalýzu

Prví příspěvek tohoto bloku pojednával o nové rychlé metodě modulárního násobení. Ta umožňuje rozdělit celý proces násobení na dvě nezávislé části, které pak mohou být prováděny paralelně (čímž lze v multiprocesorovém prostředí teoreticky zdvojnásobit rychlost výpočtu). Dále bylo prezentováno několik dalších urychlení pro modulární násobení (která již nevyužívala paralelismu) a navržena byla také nová modifikace algoritmu pro urychlení modulární inverze. Změna při výpočtu inverze spočívá v nahrazení běžně používaného rozšířeného Euklidova algoritmu standardním (nerozšířeným) Euklidovým algoritmem. Tím je dosaženo dvojnásobného zrychlení. Nevýhodou této optimalizace je, že je určena výhradně pro implementace ECC do čipových karet navržených pro hardwarovou akceleraci RSA (kterých je ale na druhou stranu v současné době na trhu dostatečné množství). Prezentována byla i nová varianta „Giant-Step Baby-Step“ algoritmu, která ve speciálních případech umožňuje efektivnější výpočet diskrétního logaritmu. Na závěr byl pak představen mechanizmus umožňující analyzovat přínos randomizačních technik použitých k prevenci útoků postranními kanály.

Chybová analýza

Závěrečná část tohoto článku se zabývá útoky založenými na chybové analýze a metodami ochrany proti nim. Jako první byl prezentován návrh využití robustních nelineárních *(n, k)*-detekčních kódů, které jsou oproti lineárním kódům se stejným *n* a *k* schopny detekovat chyby mnohem rovnoměrněji (a zcela nezávisle na rozložení chyb). Tím je výrazně snížena pravděpodobnost, že útočník bude schopen nějakým způsobem vyvolat v systému nedetekovanou chybu. Dále byla popsána praktická realizace útoku na běžně dostupnou čipovou kartu Silvercard (založenou na čipu PIC16F877 firmy Microchip), kde byl pomocí výkyvu v přísunu energie redukován počet kol naivní implementace AES. Navržen byl také nový typ útoku na skalární násobení v ECC, který dokáže oproti předcházejícím útokům (ty vytvářely body ležící na kryptograficky slabé křivce a byly snadno detekovatelné) vytvořit bod neopouštějící původní křivku. Zajímavý přístup založený na redundantní aritmetice v konečných polích byl použit při tvorbě asymetrického kryptosystému odolného proti chybám. Dále byly prezentovány metody možného zabezpečení jak na CRT založené implementace RSA, tak i klasické implementace RSA. Navržena byla dokonce verze RSA využívající detekčních kódů a pozornosti neunikly ani kryptosystémy založené na párování, které doposud z pohledu chybové analýzy nikdo nestudoval. Několik zbývajících příspěvků se také zabývalo metodikou hodnocení útoků chybovou analýzou a jejich protiopatřeními (např. vzájemné porovnání existujících metod, vytvoření vhodného modelu útočníka apod.).

Reference

[CHES05] Proceedings of the 7th International Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2005, volume 3659 of Lecture Notes in Computer Science, Springer Verlag, 2005. ISBN 3-540-28474-5.

[FDTC05] Proceedings of the 2nd International Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC) 2005, Edinburgh, Scotland, 2005.

E. O čem jsme psali v říjnu 1999 – 2004

Crypto-World 10/1999

Crypto-World 10/2000

Crypto-World 10/2001

Crypto-World 10/2002

Crypto-World 10/2003

Crypto-World 10/2004

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@pvt.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/