

Ozvěny 29C3

29th Chaos Communication Congress

Pavel Růžička
ruza@ruza.eu

Brmlab, hackerspace Prague
<http://brmlab.cz>.

3.1.2012 / Brmlab, Lightning talks



WTF

1 O CCC

2 Talks

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
 - Hamburg, 1984-1993
 - Berlin, 1994
 - Hamburg, 1995-1997
 - Berlin, 1998-2011
 - Hamburg, 2012

<https://events.ccc.de/congress/>

Congress Center Hamburg



CCH -> CCC



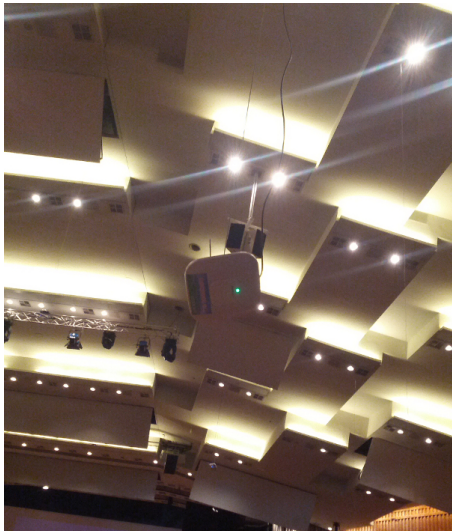
Congress Center Hamburg, Saal1



Congress Center Hamburg



access points



Jacob Appelbaum - Not my department

<http://events.ccc.de/congress/2012/Fahrplan/events/5385.en.html>

- NSA datacenter Utah



*National Security Administration building construction near
Bluffdale, Tuesday, March 20, 2012. (Ravell Call, Deseret News)*

Jesselyn Radack, Thomas Drake, William Binney

<http://events.ccc.de/congress/2012/Fahrplan/events/5338.en.html>

- Enemies of the State: What Happens When Telling the Truth about Secret US Government Power Becomes a Crime
- "I Am A Whistleblower"

Jesselyn Radack, Thomas Drake, William Binney

<http://events.ccc.de/congress/2012/Fahrplan/events/5338.en.html>

- Enemies of the State: What Happens When Telling the Truth about Secret US Government Power Becomes a Crime
- "I Am A Whistleblower"

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>



Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- **DSRC: Digital Short Range Communications (380m)**
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- **DSRC: Digital Short Range Communications (380m)**
- **The US Dept. of Transportation is considering mandating this for all new cars.**
- **Basic safety messages sent out every 10 seconds.**
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.

Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.



Christie Dudley - Privacy and the Car of the Future

<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.



Christie Dudley - Privacy and the Car of the Future

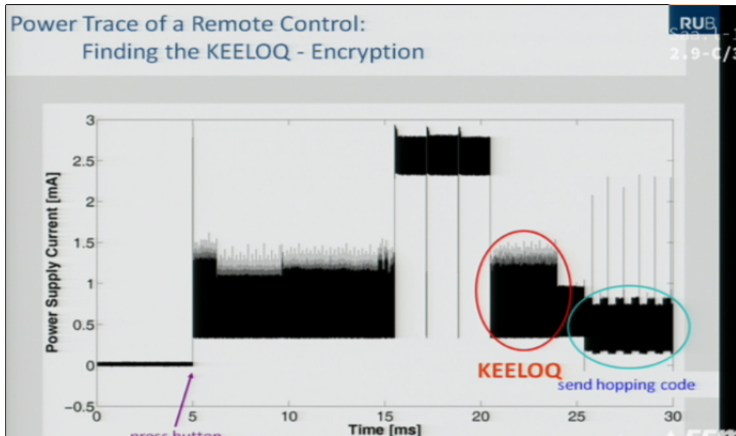
<http://events.ccc.de/congress/2012/Fahrplan/events/5095.en.html>

- DSRC: Digital Short Range Communications (380m)
- The US Dept. of Transportation is considering mandating this for all new cars.
- Basic safety messages sent out every 10 seconds.
- 5.9GHz reserved in US and Europe.
- Signaling standard: IEEE 802.11p
- All messages are cryptographically signed
- Signing certificates issued by central authority
- Privacy issues: Correlate location, speed to independent identification?
- All zero source address for vehicles. Unrouteable
- Any algorithm to make network routeable will make vehicles trackable.



Timo Kasper - Milking the Digital Cash Cow, 2008

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

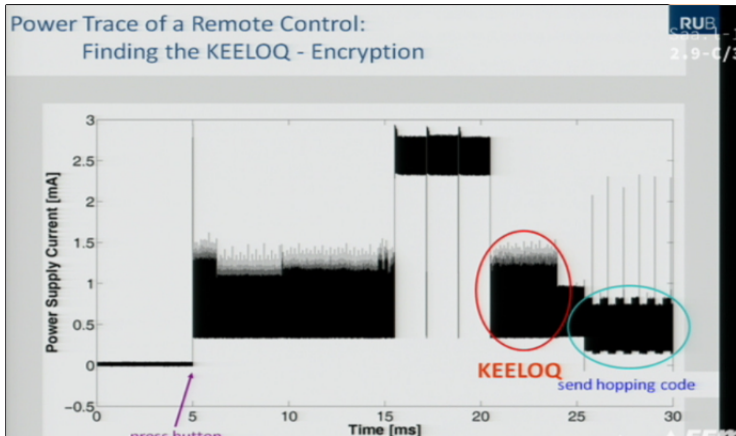


- side channel power analysis, (2008)

• $K_{remotecontrol} = f(serial, K_{Master})$

Timo Kasper - Milking the Digital Cash Cow, 2008

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>



- side channel power analysis, (2008)
- $k_{remotecontrol} = f(serial, k_{Master})$

Timo Kasper - Milking the Digital Cash Cow, 2012

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 applications/folder with 16 files max each
- 14 keys per app, 1 master key

Timo Kasper - Milking the Digital Cash Cow, 2012

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 applications/folder with 16 files max each
- 14 keys per app, 1 master key

Timo Kasper - Milking the Digital Cash Cow, 2012

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 applications/folder with 16 files max each
- 14 keys per app, 1 master key

Timo Kasper - Milking the Digital Cash Cow, 2012

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 applications/folder with 16 files max each
- 14 keys per app, 1 master key

Timo Kasper - Milking the Digital Cash Cow, 2012

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 applications/folder with 16 files max each
- 14 keys per app, 1 master key

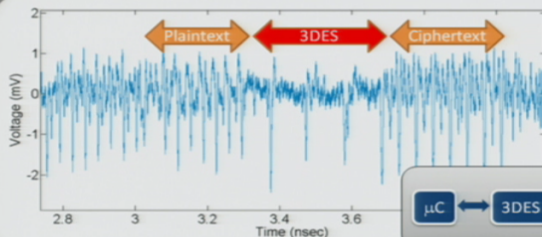
Timo Kasper - Milking the Digital Cash Cow

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- after demodulation a low pass filtering
- equipment <2000€

With known secret key:

- power analysis reveals processing of plain- and ciphertext
- locate 3DES computation



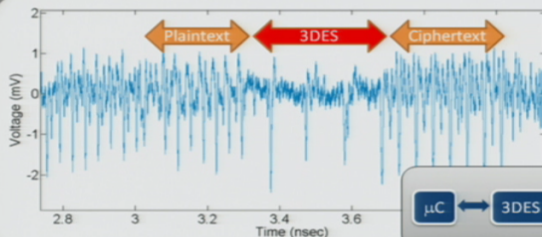
Timo Kasper - Milking the Digital Cash Cow

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- after demodulation a low pass filtering
- equipment <2000€

With known secret key:

- power analysis reveals processing of plain- and ciphertext
- locate 3DES computation



Timo Kasper - Milking the Digital Cash Cow, 2008

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- master key extracted (identical for all Opencards)
- all application keys extracted



Timo Kasper - Milking the Digital Cash Cow, 2008

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- master key extracted (identical for all Opencards)
- all application keys extracted



Timo Kasper - Milking the Digital Cash Cow

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

DESFire MF3ICD40 discontinued and replaced by
DESFire EV1 (released 2009)




Timo Kasper - Milking the Digital Cash Cow

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

- Chameleon, can emulate UID

Chameleon:
A Versatile Emulator for Contactless Smartcards



- Mifare Classic: **Crypto1** stream cipher
- Mifare DESFire *MF3ICD40*: **(3)DES**
- Mifare DESFire EV1: **AES-128, (3)DES**

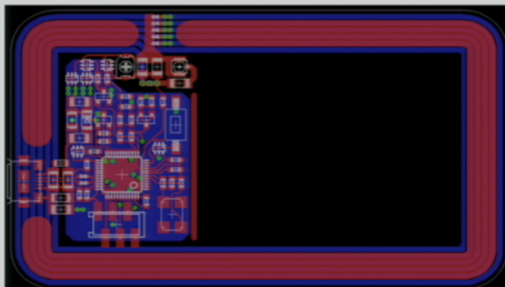
<http://sourceforge.net/projects/reader14443/>

Timo Kasper - Milking the Digital Cash Cow

<http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html>

Chameleon:

New Mini Version in 2013



open source project: <http://sourceforge.net/projects/chameleon1443/>

James Forshaw - ESXi Beast

<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- Vmware vSphere client, Vmware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

James Forshaw - ESXi Beast

<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- VMware vSphere client, VMware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

James Forshaw - ESXi Beast

<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- Vmware vSphere client, Vmware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

James Forshaw - ESXi Beast

<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- Vmware vSphere client, Vmware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

James Forshaw - ESXi Beast

<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- Vmware vSphere client, Vmware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

James Forshaw - ESXi Beast

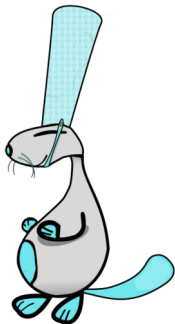
<http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html>

- Vmware vSphere client, Vmware Auth Daemon over tcp/443
- datastore browser, NFC protocol tcp/902 communication unencrypted
- CANAPE - protocol analyzer, Win based, network protocol analysis tool, interception proxy
- TCP and net graph
- interception proxy, password bruteforce, fuzzin'
- traffic injection, forged response

Frédéric Guihéry, Georges Bossert - The future of protocol reversing and simulation applied on ZeroAccess botnet

<http://events.ccc.de/congress/2012/Fahrplan/events/5256.en.html>

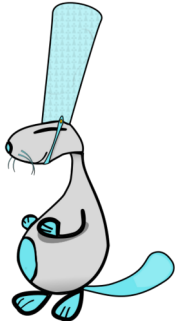
- message format, state machine
- Netzob



Frédéric Guihéry, Georges Bossert - The future of protocol reversing and simulation applied on ZeroAccess botnet

<http://events.ccc.de/congress/2012/Fahrplan/events/5256.en.html>

- message format, state machine
- Netzob



Pierre Jaury, Damien Cauquil

Small footprint inspection techniques for Android

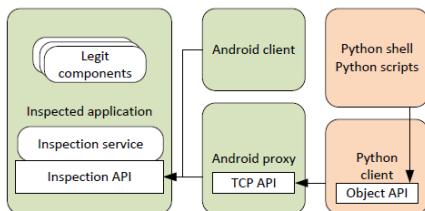
Fino

'cause we finally built some tool

Fino Low footprint inspection service

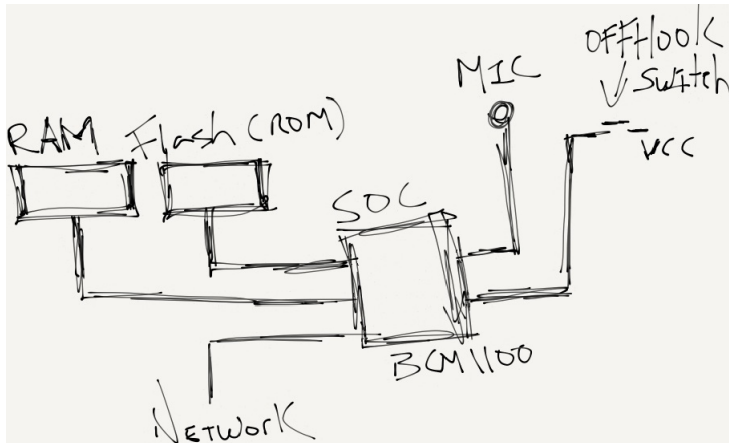
Gadget Android-side API proxy

Client Python object oriented API and interactive shell



Ang Cui, Michael Costello - Hacking Cisco Phones

<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>



Ang Cui, Michael Costello - Hacking Cisco Phones

<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>

0x000	0x001	0x002	0x003	0x004	0x005	0x006	0x007	0x008	0x009	0x00a	0x00b	0x00c	0x00d
0x00e	0x00f	0x010	0x011	0x012	0x013	0x014	0x015	0x016	0x017	0x018	0x019	0x01a	0x01b
0x01c	0x01d	0x01e	0x01f	0x020	0x021	0x022	0x023	0x024	0x025	0x026	0x027	0x028	0x029
0x02a	0x02b	0x02c	0x02d	0x02e	0x02f	0x030	0x031	0x032	0x033	0x034	0x035	0x036	0x037
0x038	0x039	0x03a	0x03b	0x03c	0x03d	0x03e	0x03f	0x040	0x041	0x042	0x043	0x044	0x045
0x046	0x047	0x048	0x049	0x04a	0x04b	0x04c	0x04d	0x04e	0x04f	0x050	0x051	0x052	0x053
0x054	0x055	0x056	0x057	0x058	0x059	0x05a	0x05b	0x05c	0x05d	0x05e	0x05f	0x060	0x061
0x062	0x063	0x064	0x065	0x066	0x067	0x068	0x069	0x06a	0x06b	0x06c	0x06d	0x06e	0x06f
0x070	0x071	0x072	0x073	0x074	0x075	0x076	0x077	0x078	0x079	0x07a	0x07b	0x07c	0x07d
0x07e	0x07f	0x080	0x081	0x082	0x083	0x084	0x085	0x086	0x087	0x088	0x089	0x08a	0x08b
0x08c	0x08d	0x08e	0x08f	0x090	0x091	0x092	0x093	0x094	0x095	0x096	0x097	0x098	0x099
0x09a	0x09b	0x09c	0x09d	0x09e	0x09f	0x0a0	0x0a1	0x0a2	0x0a3	0x0a4	0x0a5	0x0a6	0x0a7
0x0a8	0x0a9	0x0aa	0x0ab	0x0ac	0x0ad	0x0ae	0x0af	0x0b0	0x0b1	0x0b2	0x0b3	0x0b4	0x0b5
0x0b6	0x0b7	0x0b8	0x0b9	0x0ba	0x0bb	0x0bc	0x0bd	0x0be	0x0bf	0x0c0	0x0c1	0x0c2	0x0c3
0x0c4	0x0c5	0x0c6	0x0c7	0x0c8	0x0c9	0x0ca	0x0cb	0x0cc	0x0cd	0x0ce	0x0cf	0x0d0	0x0d1
0x0d2	0x0d3	0x0d4	0x0d5	0x0d6	0x0d7	0x0d8	0x0d9	0x0da	0x0db	0x0dc	0x0dd	0x0de	0x0df
0x0e0	0x0e1	0x0e2	0x0e3	0x0e4	0x0e5	0x0e6	0x0e7	0x0e8	0x0e9	0x0ea	0x0eb	0x0ec	0x0ed
0x0ee	0x0ef	0x0f0	0x0f1	0x0f2	0x0f3	0x0f4	0x0f5	0x0f6	0x0f7	0x0f8	0x0f9	0x0fa	0x0fb
0x0fc	0x0fd	0x0fe	0x0ff	0x100	0x101	0x102	0x103	0x104	0x105	0x106	0x107	0x108	0x109
0x10a	0x10b	0x10c	0x10d	0x10e	0x10f	0x110	0x111	0x112	0x113	0x114	0x115	0x116	0x117
0x118	0x119	0x11a	0x11b	0x11c	0x11d	0x11e	0x11f	0x120	0x121	0x122	0x123	0x124	0x125
0x126	0x127	0x128	0x129	0x12a	0x12b	0x12c	0x12d	0x12e	0x12f	0x130	0x131	0x132	0x133
0x134	0x135	0x136	0x137	0x138	0x139	0x13a	0x13b	0x13c	0x13d	0x13e	0x13f	0x140	0x141
0x142	0x143	0x144	0x145	0x146	0x147	0x148	0x149	0x14a	0x14b	0x14c	0x14d	0x14e	0x14f
0x150	0x151	0x152	0x153	0x154	0x155	0x156	0x157	0x158	0x159	0x15a	0x15b	0x15c	0x15d
0x15e	0x15f	0x160	0x161	0x162	0x163	0x164	0x165	0x166	0x167	0x168	0x169	0x16a	0x16b

- total syscall entries: 364
- total syscallz: 173
- total trivial crash: 60

Ang Cui, Michael Costello - Hacking Cisco Phones

<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>

0x000	0x001	0x002	0x003	0x004	0x005	0x006	0x007	0x008	0x009	0x00a	0x00b	0x00c	0x00d
0x00e	0x00f	0x010	0x011	0x012	0x013	0x014	0x015	0x016	0x017	0x018	0x019	0x01a	0x01b
0x01c	0x01d	0x01e	0x01f	0x020	0x021	0x022	0x023	0x024	0x025	0x026	0x027	0x028	0x029
0x02a	0x02b	0x02c	0x02d	0x02e	0x02f	0x030	0x031	0x032	0x033	0x034	0x035	0x036	0x037
0x038	0x039	0x03a	0x03b	0x03c	0x03d	0x03e	0x03f	0x040	0x041	0x042	0x043	0x044	0x045
0x046	0x047	0x048	0x049	0x04a	0x04b	0x04c	0x04d	0x04e	0x04f	0x050	0x051	0x052	0x053
0x054	0x055	0x056	0x057	0x058	0x059	0x05a	0x05b	0x05c	0x05d	0x05e	0x05f	0x060	0x061
0x062	0x063	0x064	0x065	0x066	0x067	0x068	0x069	0x06a	0x06b	0x06c	0x06d	0x06e	0x06f
0x070	0x071	0x072	0x073	0x074	0x075	0x076	0x077	0x078	0x079	0x07a	0x07b	0x07c	0x07d
0x07e	0x07f	0x080	0x081	0x082	0x083	0x084	0x085	0x086	0x087	0x088	0x089	0x08a	0x08b
0x08c	0x08d	0x08e	0x08f	0x090	0x091	0x092	0x093	0x094	0x095	0x096	0x097	0x098	0x099
0x09a	0x09b	0x09c	0x09d	0x09e	0x09f	0x0a0	0x0a1	0x0a2	0x0a3	0x0a4	0x0a5	0x0a6	0x0a7
0x0a8	0x0a9	0x0aa	0x0ab	0x0ac	0x0ad	0x0ae	0x0af	0x0b0	0x0b1	0x0b2	0x0b3	0x0b4	0x0b5
0x0b6	0x0b7	0x0b8	0x0b9	0x0ba	0x0bb	0x0bc	0x0bd	0x0be	0x0bf	0x0c0	0x0c1	0x0c2	0x0c3
0x0c4	0x0c5	0x0c6	0x0c7	0x0c8	0x0c9	0x0ca	0x0cb	0x0cc	0x0cd	0x0ce	0x0cf	0x0d0	0x0d1
0x0d2	0x0d3	0x0d4	0x0d5	0x0d6	0x0d7	0x0d8	0x0d9	0x0da	0x0db	0x0dc	0x0dd	0x0de	0x0df
0x0e0	0x0e1	0x0e2	0x0e3	0x0e4	0x0e5	0x0e6	0x0e7	0x0e8	0x0e9	0x0ea	0x0eb	0x0ec	0x0ed
0x0ee	0x0ef	0x0f0	0x0f1	0x0f2	0x0f3	0x0f4	0x0f5	0x0f6	0x0f7	0x0f8	0x0f9	0x0fa	0x0fb
0x0fc	0x0fd	0x0fe	0x0ff	0x100	0x101	0x102	0x103	0x104	0x105	0x106	0x107	0x108	0x109
0x10a	0x10b	0x10c	0x10d	0x10e	0x10f	0x110	0x111	0x112	0x113	0x114	0x115	0x116	0x117
0x118	0x119	0x11a	0x11b	0x11c	0x11d	0x11e	0x11f	0x120	0x121	0x122	0x123	0x124	0x125
0x126	0x127	0x128	0x129	0x12a	0x12b	0x12c	0x12d	0x12e	0x12f	0x130	0x131	0x132	0x133
0x134	0x135	0x136	0x137	0x138	0x139	0x13a	0x13b	0x13c	0x13d	0x13e	0x13f	0x140	0x141
0x142	0x143	0x144	0x145	0x146	0x147	0x148	0x149	0x14a	0x14b	0x14c	0x14d	0x14e	0x14f
0x150	0x151	0x152	0x153	0x154	0x155	0x156	0x157	0x158	0x159	0x15a	0x15b	0x15c	0x15d
0x15e	0x15f	0x160	0x161	0x162	0x163	0x164	0x165	0x166	0x167	0x168	0x169	0x16a	0x16b

- total syscall entries: 364
- total syscallz: 173
- total trivial crash: 60

Ang Cui, Michael Costello - Hacking Cisco Phones

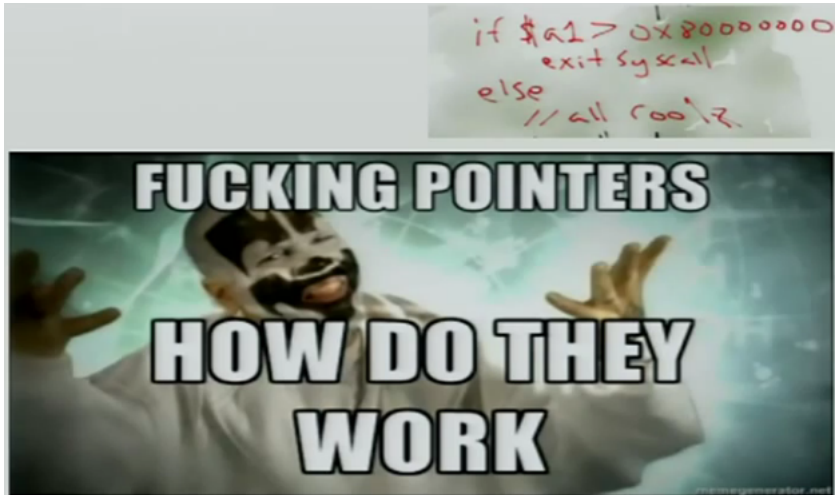
<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>

0x000	0x001	0x002	0x003	0x004	0x005	0x006	0x007	0x008	0x009	0x00a	0x00b	0x00c	0x00d
0x00e	0x00f	0x010	0x011	0x012	0x013	0x014	0x015	0x016	0x017	0x018	0x019	0x01a	0x01b
0x01c	0x01d	0x01e	0x01f	0x020	0x021	0x022	0x023	0x024	0x025	0x026	0x027	0x028	0x029
0x02a	0x02b	0x02c	0x02d	0x02e	0x02f	0x030	0x031	0x032	0x033	0x034	0x035	0x036	0x037
0x038	0x039	0x03a	0x03b	0x03c	0x03d	0x03e	0x03f	0x040	0x041	0x042	0x043	0x044	0x045
0x046	0x047	0x048	0x049	0x04a	0x04b	0x04c	0x04d	0x04e	0x04f	0x050	0x051	0x052	0x053
0x054	0x055	0x056	0x057	0x058	0x059	0x05a	0x05b	0x05c	0x05d	0x05e	0x05f	0x060	0x061
0x062	0x063	0x064	0x065	0x066	0x067	0x068	0x069	0x06a	0x06b	0x06c	0x06d	0x06e	0x06f
0x070	0x071	0x072	0x073	0x074	0x075	0x076	0x077	0x078	0x079	0x07a	0x07b	0x07c	0x07d
0x07e	0x07f	0x080	0x081	0x082	0x083	0x084	0x085	0x086	0x087	0x088	0x089	0x08a	0x08b
0x08c	0x08d	0x08e	0x08f	0x090	0x091	0x092	0x093	0x094	0x095	0x096	0x097	0x098	0x099
0x09a	0x09b	0x09c	0x09d	0x09e	0x09f	0x0a0	0x0a1	0x0a2	0x0a3	0x0a4	0x0a5	0x0a6	0x0a7
0x0a8	0x0a9	0x0aa	0x0ab	0x0ac	0x0ad	0x0ae	0x0af	0x0b0	0x0b1	0x0b2	0x0b3	0x0b4	0x0b5
0x0b6	0x0b7	0x0b8	0x0b9	0x0ba	0x0bb	0x0bc	0x0bd	0x0be	0x0bf	0x0c0	0x0c1	0x0c2	0x0c3
0x0c4	0x0c5	0x0c6	0x0c7	0x0c8	0x0c9	0x0ca	0x0cb	0x0cc	0x0cd	0x0ce	0x0cf	0x0d0	0x0d1
0x0d2	0x0d3	0x0d4	0x0d5	0x0d6	0x0d7	0x0d8	0x0d9	0x0da	0x0db	0x0dc	0x0dd	0x0de	0x0df
0x0e0	0x0e1	0x0e2	0x0e3	0x0e4	0x0e5	0x0e6	0x0e7	0x0e8	0x0e9	0x0ea	0x0eb	0x0ec	0x0ed
0x0ee	0x0ef	0x0f0	0x0f1	0x0f2	0x0f3	0x0f4	0x0f5	0x0f6	0x0f7	0x0f8	0x0f9	0x0fa	0x0fb
0x0fc	0x0fd	0x0fe	0x0ff	0x100	0x101	0x102	0x103	0x104	0x105	0x106	0x107	0x108	0x109
0x10a	0x10b	0x10c	0x10d	0x10e	0x10f	0x110	0x111	0x112	0x113	0x114	0x115	0x116	0x117
0x118	0x119	0x11a	0x11b	0x11c	0x11d	0x11e	0x11f	0x120	0x121	0x122	0x123	0x124	0x125
0x126	0x127	0x128	0x129	0x12a	0x12b	0x12c	0x12d	0x12e	0x12f	0x130	0x131	0x132	0x133
0x134	0x135	0x136	0x137	0x138	0x139	0x13a	0x13b	0x13c	0x13d	0x13e	0x13f	0x140	0x141
0x142	0x143	0x144	0x145	0x146	0x147	0x148	0x149	0x14a	0x14b	0x14c	0x14d	0x14e	0x14f
0x150	0x151	0x152	0x153	0x154	0x155	0x156	0x157	0x158	0x159	0x15a	0x15b	0x15c	0x15d
0x15e	0x15f	0x160	0x161	0x162	0x163	0x164	0x165	0x166	0x167	0x168	0x169	0x16a	0x16b

- total syscall entries: 364
- total syscallz: 173
- total trivial crash: 60

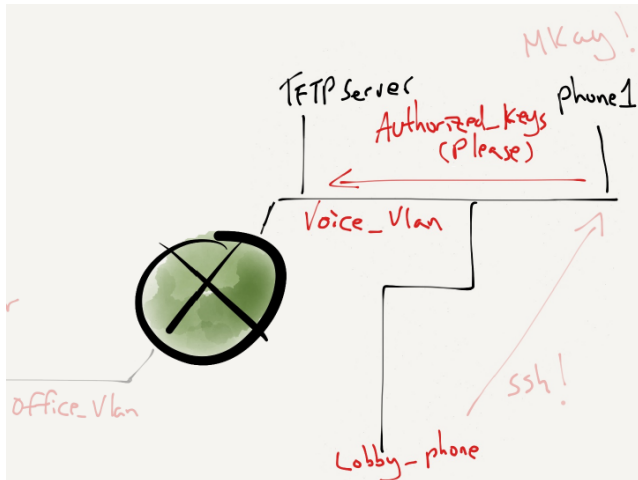
Ang Cui, Michael Costello - Hacking Cisco Phones

<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>



Ang Cui, Michael Costello - Hacking Cisco Phones

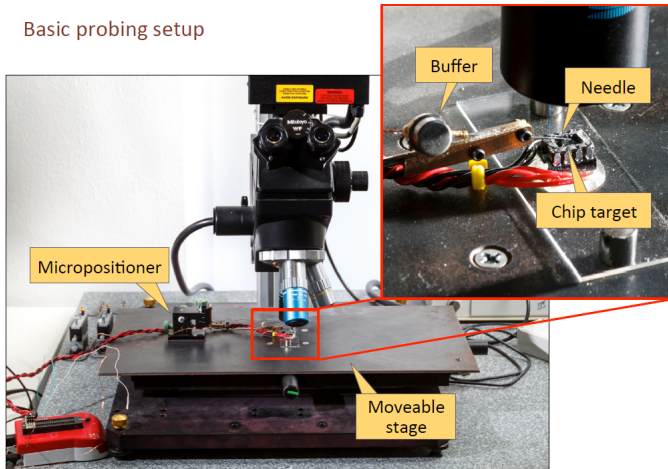
<http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html>



dexter, Karsten Nohl - Low-Cost Chip Microprobing

<http://events.ccc.de/congress/2012/Fahrplan/events/5124.en.html>

Basic probing setup



dexter, Karsten Nohl - Low-Cost Chip Microprobing

<http://events.ccc.de/congress/2012/Fahrplan/events/5124.en.html>

- cca 2000 €old optical microscope, 300 €micropositioner,
...
- probe distance limited to 2mm

dexter, Karsten Nohl - Low-Cost Chip Microprobing

<http://events.ccc.de/congress/2012/Fahrplan/events/5124.en.html>

- cca 2000 €old optical microscope, 300 €micropositioner,
...
- probe distance limited to 2mm

Travis Goodspeed - Writing a Thumbdrive from Scratch

<http://events.ccc.de/congress/2012/Fahrplan/events/5327.en.html>

- Read It Twice by Collin Mulliner (jailbreak Samsung tv), TOCTTOU (time of check to time of use) attack
- two versions of the same file read. big file read in between to flush cache
- the grugq, Defeating Forensic Analysis on Unix ,Phrack 59-6
- USB standard, SCSI standard

Travis Goodspeed - Writing a Thumbdrive from Scratch

<http://events.ccc.de/congress/2012/Fahrplan/events/5327.en.html>

- Read It Twice by Collin Mulliner (jailbreak Samsung tv), TOCTTOU (time of check to time of use) attack
- two versions of the same file read. big file read in between to flush cache
- the grugq, Defeating Forensic Analysis on Unix ,Phrack 59-6
- USB standard, SCSI standard

Travis Goodspeed - Writing a Thumbdrive from Scratch

<http://events.ccc.de/congress/2012/Fahrplan/events/5327.en.html>

- Read It Twice by Collin Mulliner (jailbreak Samsung tv), TOCTTOU (time of check to time of use) attack
- two versions of the same file read. big file read in between to flush cache
- the grugq, Defeating Forensic Analysis on Unix ,Phrack 59-6
- USB standard, SCSI standard

Travis Goodspeed - Writing a Thumbdrive from Scratch

<http://events.ccc.de/congress/2012/Fahrplan/events/5327.en.html>

- Read It Twice by Collin Mulliner (jailbreak Samsung tv), TOCTTOU (time of check to time of use) attack
- two versions of the same file read. big file read in between to flush cache
- the grugq, Defeating Forensic Analysis on Unix ,Phrack 59-6
- USB standard, SCSI standard

Carlos Garcia Prado - How I met your pointer

<http://events.ccc.de/congress/2012/Fahrplan/events/5219.en.html>

- Everybody loves chocolate
- Fuzzing is like violence: if it doesn't solve your problems, you are not using enough of it.
- need to follow protocol
<https://github.com/carlosgprado/Boyka>

Carlos Garcia Prado - How I met your pointer

<http://events.ccc.de/congress/2012/Fahrplan/events/5219.en.html>

- Everybody loves chocolate
- Fuzzing is like violence: if it doesn't solve your problems, you are not using enough of it.

- need to follow protocol

<https://github.com/carlosgprado/Boyka>

Carlos Garcia Prado - How I met your pointer

<http://events.ccc.de/congress/2012/Fahrplan/events/5219.en.html>

- Everybody loves chocolate
- Fuzzing is like violence: if it doesn't solve your problems, you are not using enough of it.
- need to follow protocol

<https://github.com/carlosgprado/Boyka>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Jacob Appelbaum, Roger Dingledine - The Tor sw ecosystem

<http://events.ccc.de/congress/2012/Fahrplan/events/5306.en.html>

- Firefox fork patched till now (Tor browser)
- Chrome in future, + isolation, - MS crypto API certificate verification ignores proxy setting
- HTTPS everywhere
- Tor browser bundle includes NoScript
- TorBirdy - Thunderbird add-on
- OrBot
- The Amnesic Incognito Live System

<https://www.torproject.org/volunteer>

Carlos Garcia Prado - How I met your pointer

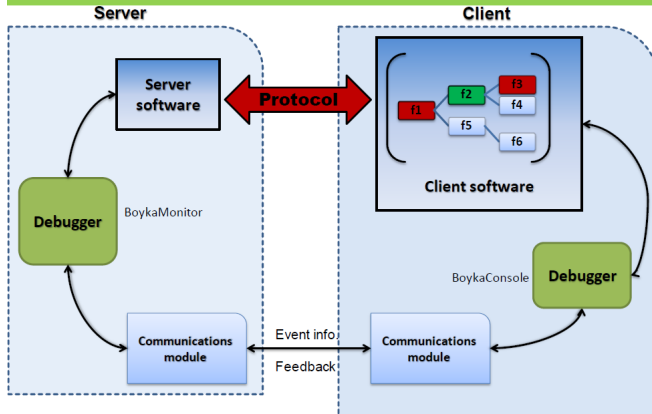
<http://events.ccc.de/congress/2012/Fahrplan/events/5219.en.html>



Carlos Garcia Prado - How I met your pointer

<http://events.ccc.de/congress/2012/Fahrplan/events/5219.en.html>

OVERVIEW (FROM A MILLION MILES AWAY)



Nico Golde - Let Me Answer That for You

<http://events.ccc.de/congress/2012/Fahrplan/events/5216.en.html>

- Home Location Register/Visitor Location Register, paging channel, Location Area Code
- race condition not limited to one BTS
- OsmocomBB layer23 too slow, layer1 is ok
- selective jamming
- fake responses, victim never receive sms/voice

Nico Golde - Let Me Answer That for You

<http://events.ccc.de/congress/2012/Fahrplan/events/5216.en.html>

- Home Location Register/Visitor Location Register, paging channel, Location Area Code
- race condition not limited to one BTS
- OsmocomBB layer23 too slow, layer1 is ok
- selective jamming
- fake responses, victim never receive sms/voice

Nico Golde - Let Me Answer That for You

<http://events.ccc.de/congress/2012/Fahrplan/events/5216.en.html>

- Home Location Register/Visitor Location Register, paging channel, Location Area Code
- race condition not limited to one BTS
- OsmocomBB layer23 too slow, layer1 is ok
- selective jamming
- fake responses, victim never receive sms/voice

Nico Golde - Let Me Answer That for You

<http://events.ccc.de/congress/2012/Fahrplan/events/5216.en.html>

- Home Location Register/Visitor Location Register, paging channel, Location Area Code
- race condition not limited to one BTS
- OsmocomBB layer23 too slow, layer1 is ok
- selective jamming
- fake responses, victim never receive sms/voice

Nico Golde - Let Me Answer That for You

<http://events.ccc.de/congress/2012/Fahrplan/events/5216.en.html>

- Home Location Register/Visitor Location Register, paging channel, Location Area Code
- race condition not limited to one BTS
- OsmocomBB layer23 too slow, layer1 is ok
- selective jamming
- fake responses, victim never receive sms/voice

Sylvain Munaut - Further hacks on the Calypso platform

<http://events.ccc.de/congress/2012/Fahrplan/events/5226.en.html>

- Motorola C123 can act as BTS with OsmocomBB

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

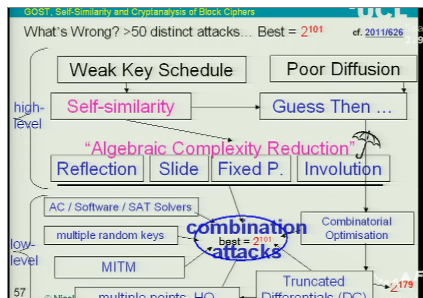
djb, Nadia Heninger, Tanja Lange - Facthacks

<http://events.ccc.de/congress/2012/Fahrplan/events/5275.en.html>

- RSA
- bad random-number generators (embedded devices)
- generate both primes from a single search (shared modulus)
- sometimes users choose special primes to try to make RSA run faster
- sometimes users leak secret bits through side channels
- sometimes the attacker has a botnet, or a 65-megawatt data center in Utah or Tianjin
- <http://factorable.net>

Dr Nicolas T. Courtois - Security Evaluation of Russian GOST Cipher

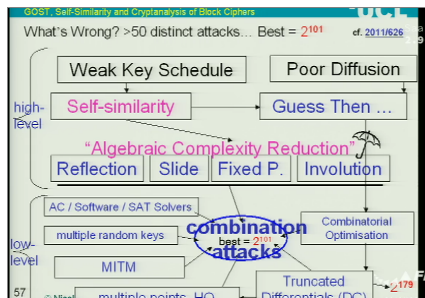
<http://events.ccc.de/congress/2012/Fahrplan/events/5225.en.html>



- GOST cipher is the official encryption standard of the Russian federation
- special versions for the most important Russian banks
- ☹ video not available at all mirrors

Dr Nicolas T. Courtois - Security Evaluation of Russian GOST Cipher

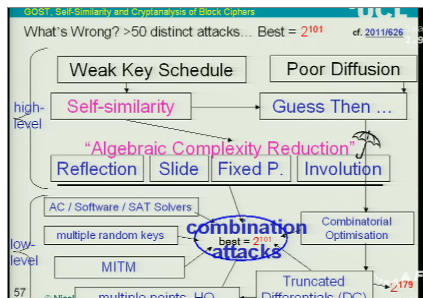
<http://events.ccc.de/congress/2012/Fahrplan/events/5225.en.html>



- GOST cipher is the official encryption standard of the Russian federation
- special versions for the most important Russian banks
- ☹ video not available at all mirrors

Dr Nicolas T. Courtois - Security Evaluation of Russian GOST Cipher

<http://events.ccc.de/congress/2012/Fahrplan/events/5225.en.html>



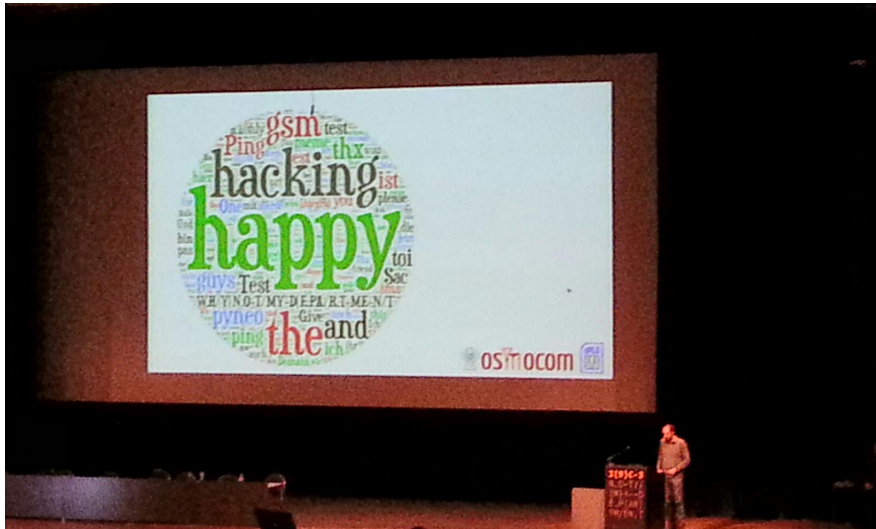
- GOST cipher is the official encryption standard of the Russian federation
- special versions for the most important Russian banks
- ☹ video not available at all mirrors

Andrei Soldatov - Russia's Surveillance State

<http://events.ccc.de/congress/2012/Fahrplan/events/5402.en.html>

how the government forces ALL local ISPs to buy and implement nation-wide surveillance mechanisms

Happy hacking & C U @ 30c3?



OHM 2013

Observe, hack, make

