Ozvěny 29C3

29th Chaos Communication Congress

Pavel Růžička
ruza@ruza.eu

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

3.1.2012 / Brmlab, Lightning talks

WTF

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
  - Hamburg, 1984-1998
  - Berlin, 1984
  - Hamburg, 1985-1997
  - Berlin, 1998-2011
  - Hamburg, 2012

`https://events.ccc.de/congress/`

Chaos Communication Congress

- organized by Chaos Computer Club since 1984
- venue
  - Hamburg, 1984-1998
  - Berlin, 1984
  - Hamburg, 1985-1997
  - 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/`

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

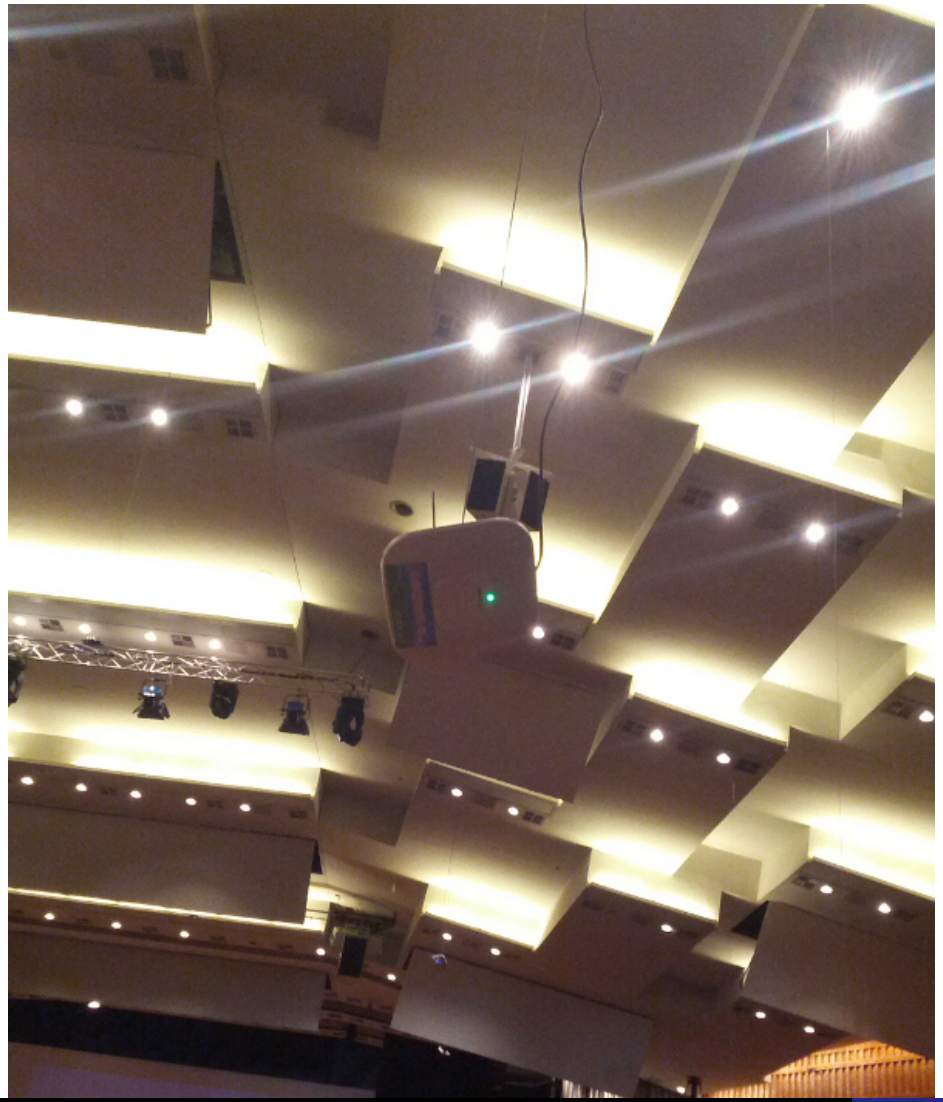
CCH -> CCC

brmlab hackerspace prague

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.

brmlab hackerspace prague

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.

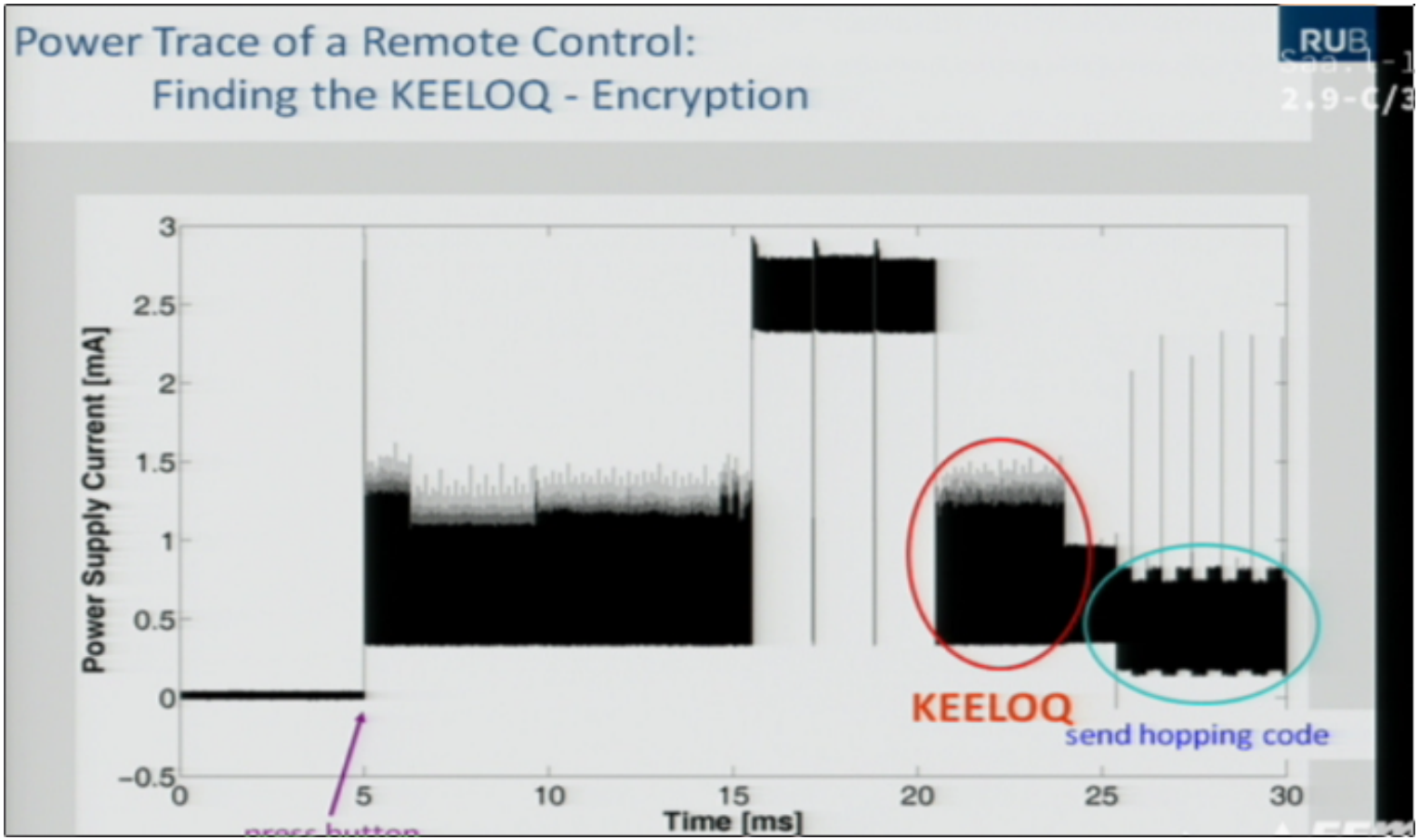
Christie Dudley - Privacy and the Car of the Future

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

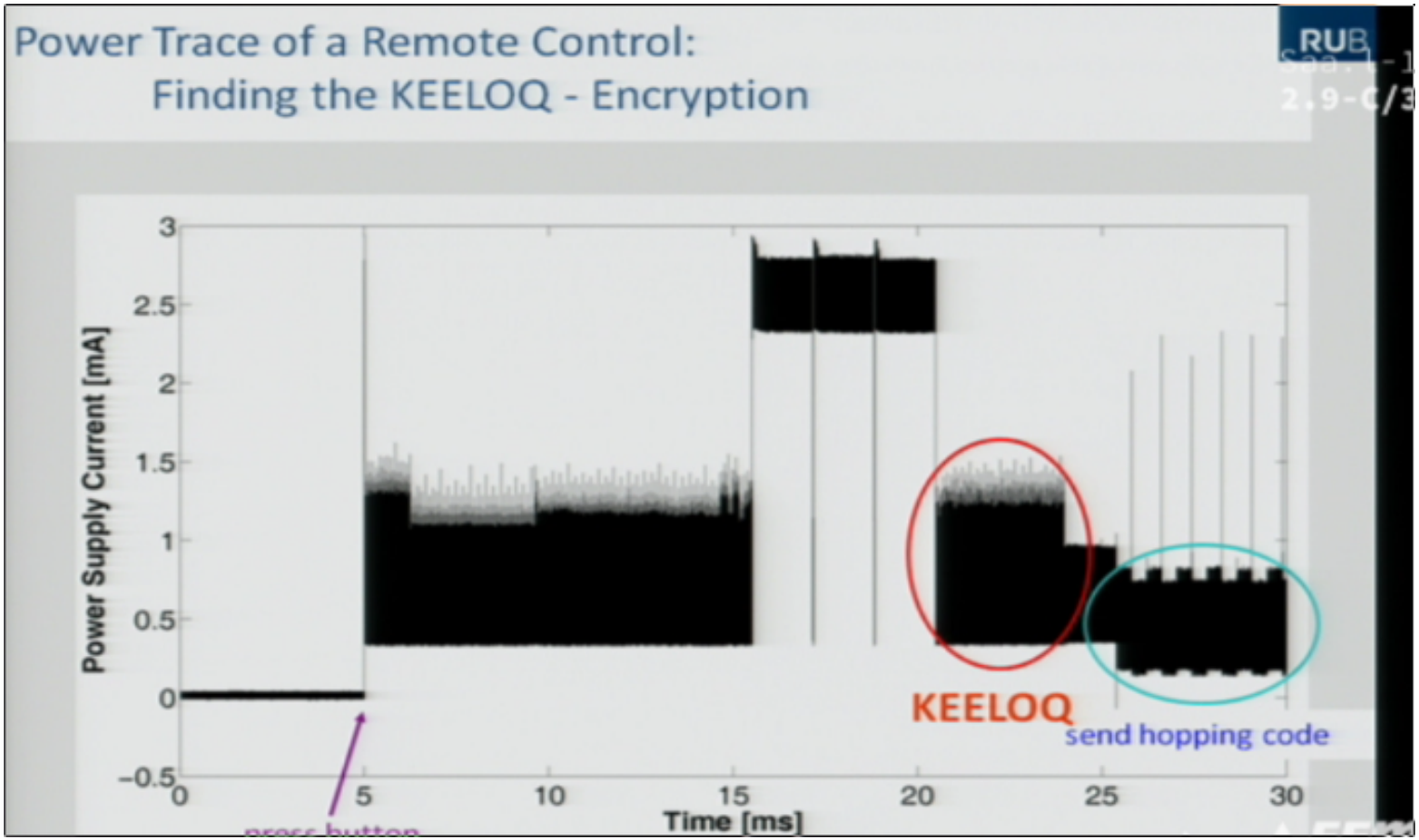
http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html



- 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)
- $k_{remotecontrol} = f(serial, k_{Master})$

brmlab hackerspace prague

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 aplications/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 aplications/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 aplications/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 aplications/folder with 16 files max each
- 14 keys per app, 1 master key

Timo Kasper - Milking the Digital Cash Cow, 2012

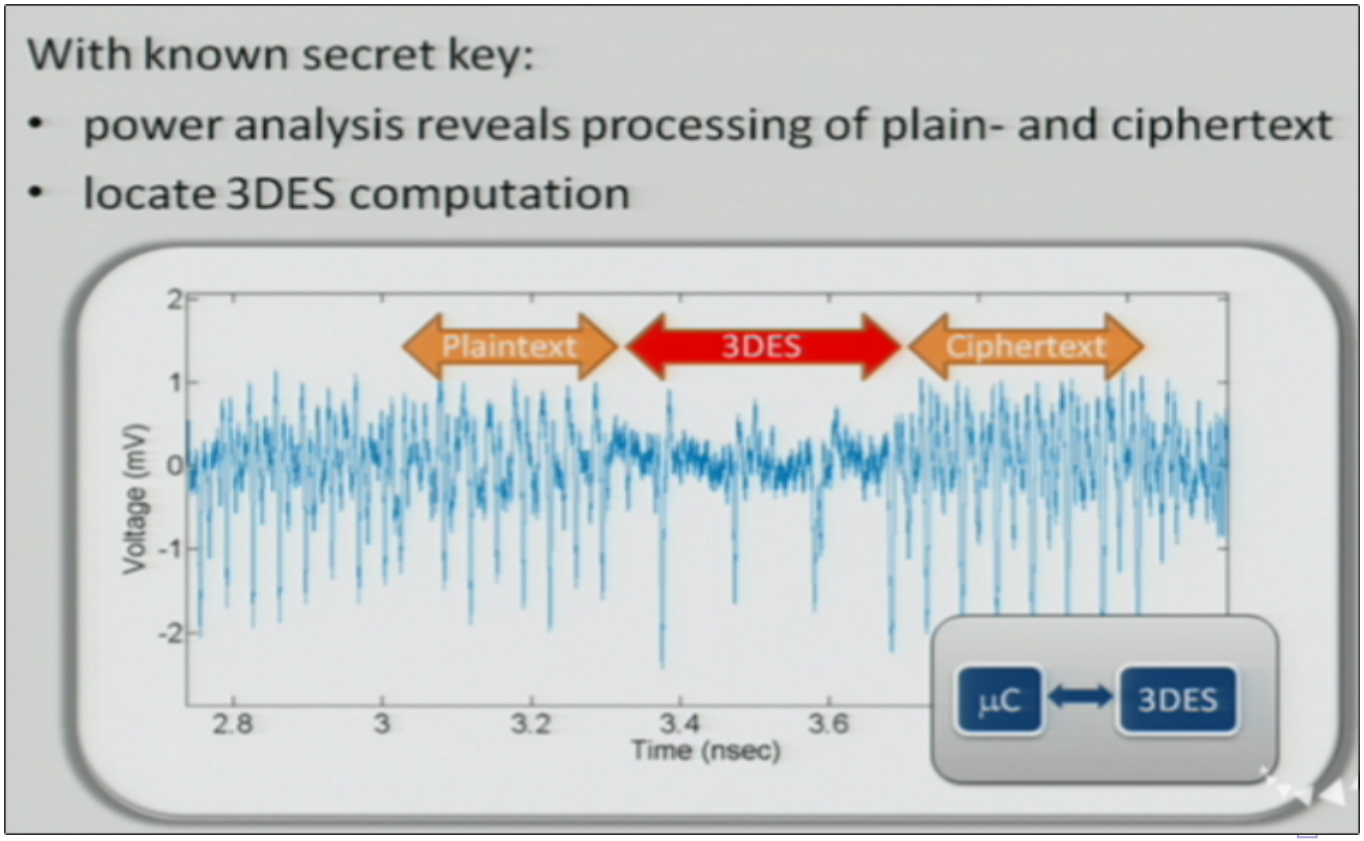
http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html

- Mifare DESFire MF3ICD40, contactless card
- 3DES for authentication and data encryption
- 4kB non-volatile memory
- 28 aplications/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

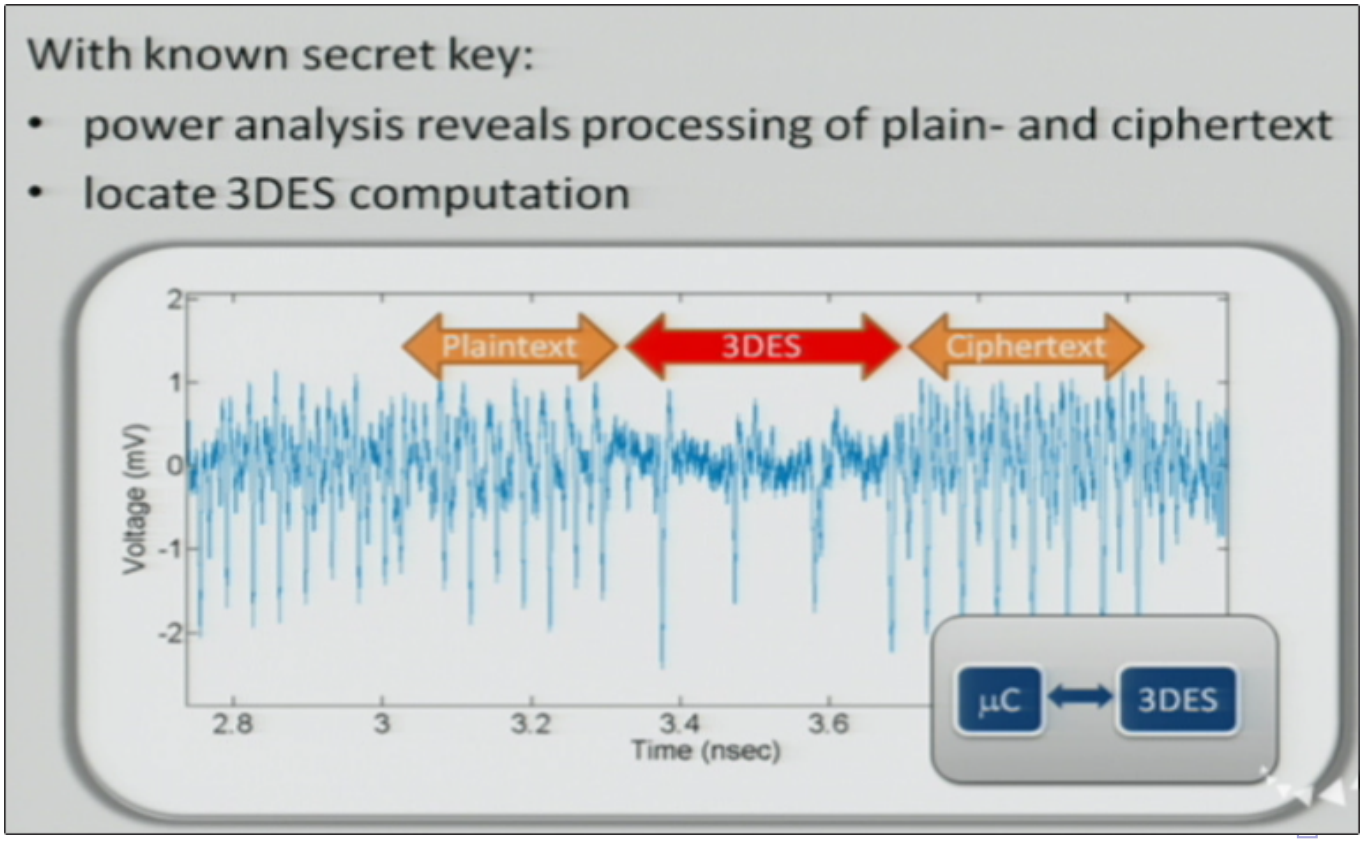
- after demodulation a low pass filtering
- equipment <2000€



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€



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

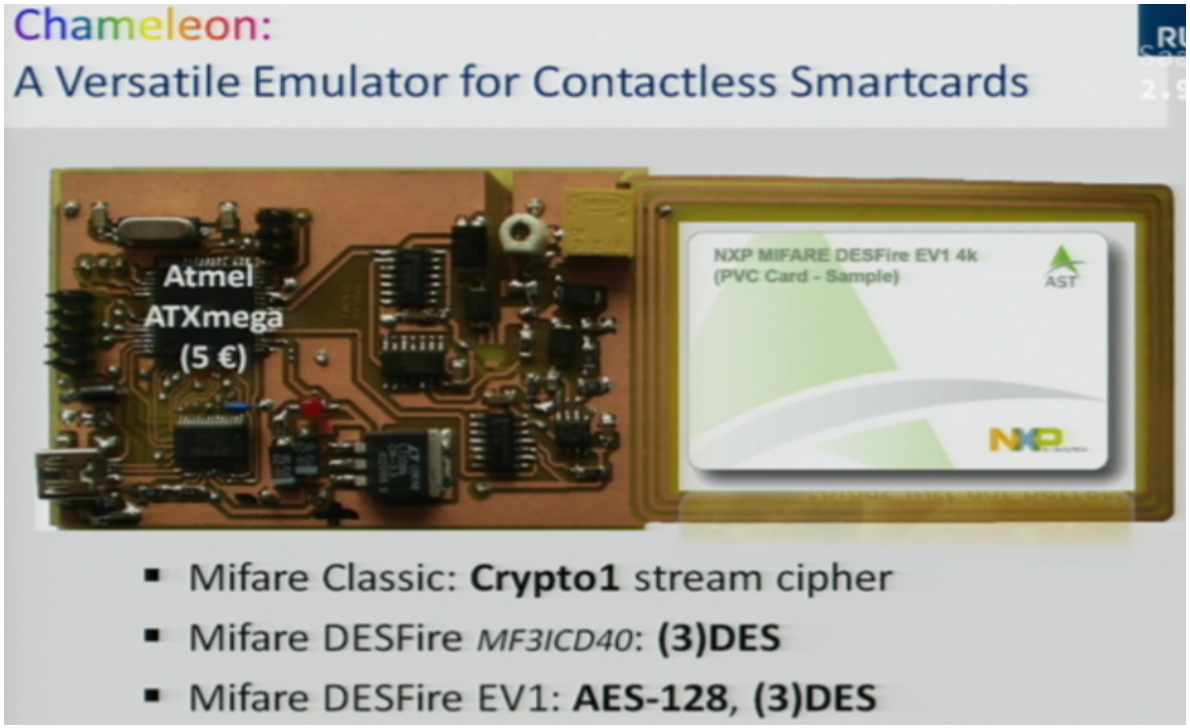
http://events.ccc.de/congress/2012/Fahrplan/events/5393.en.html

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

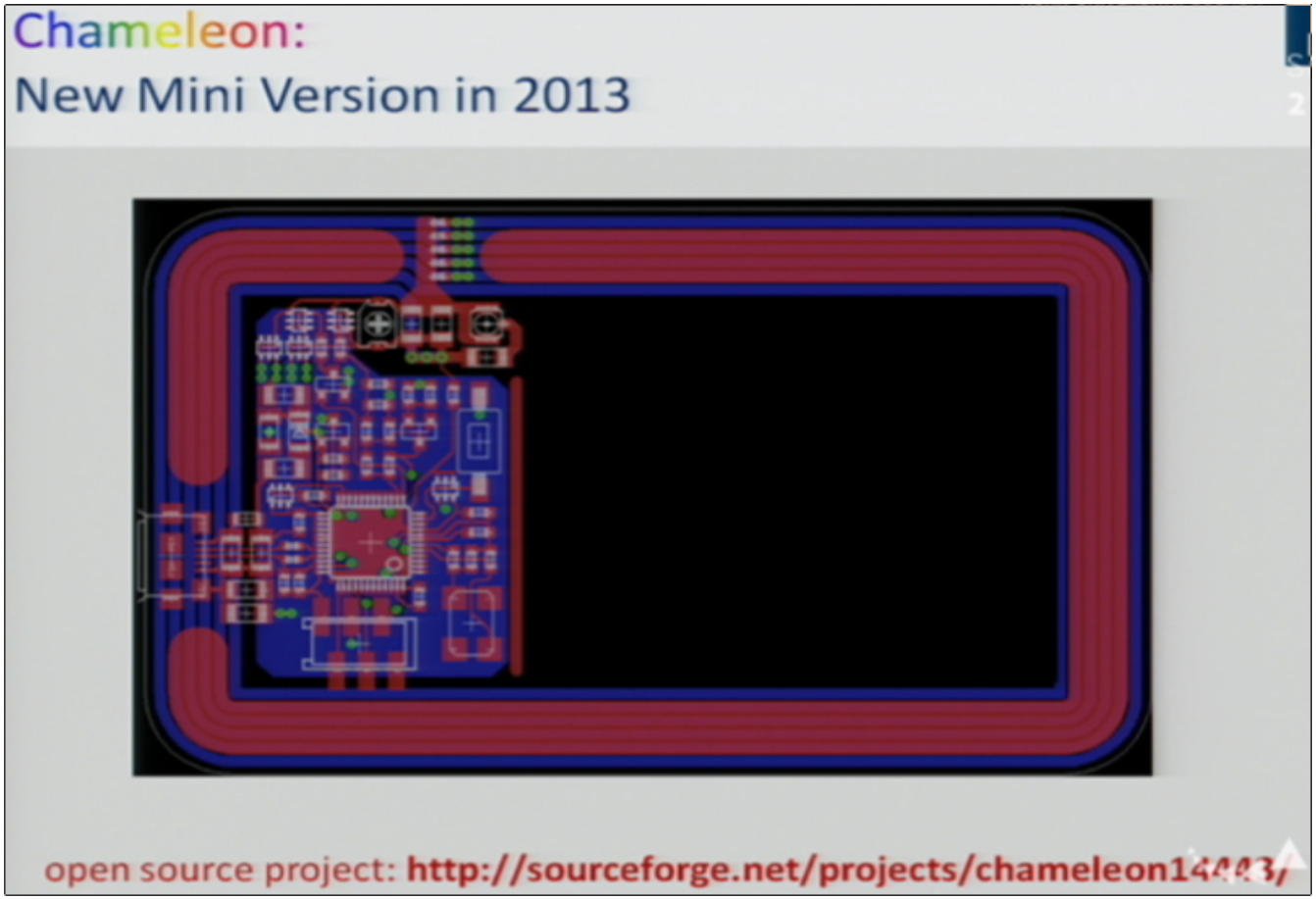


`http://sourceforge.net/projects/reader14443/`

brmlab hackerspace prague

Timo Kasper - Milking the Digital Cash Cow

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



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

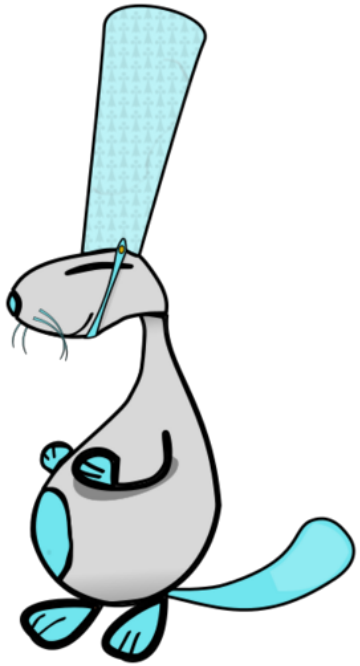
http://events.ccc.de/congress/2012/Fahrplan/events/5104.en.html

- 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

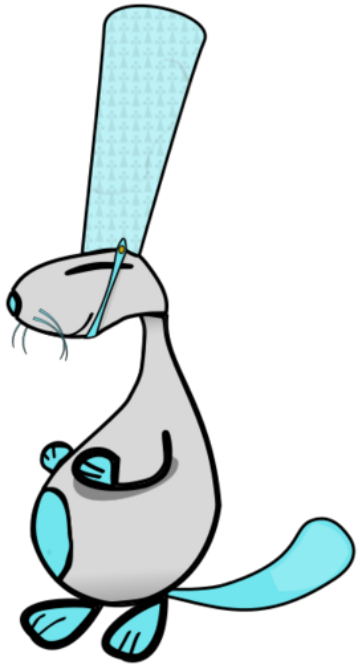
- message format, state machine
- Netzob



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



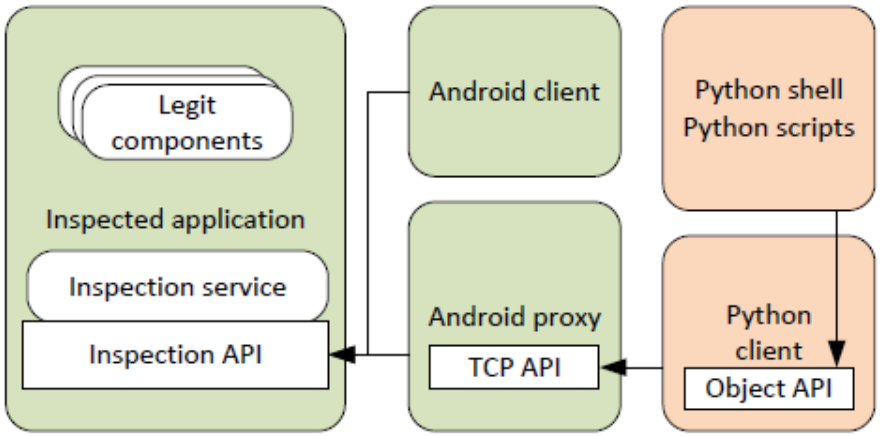
Pierre Jaury, Damien Cauquil
Small footprint inspection techniques for Android

Fino
'cause we finally built some tool

Fino Low footprint inspection service

Gadget Android-side API proxy

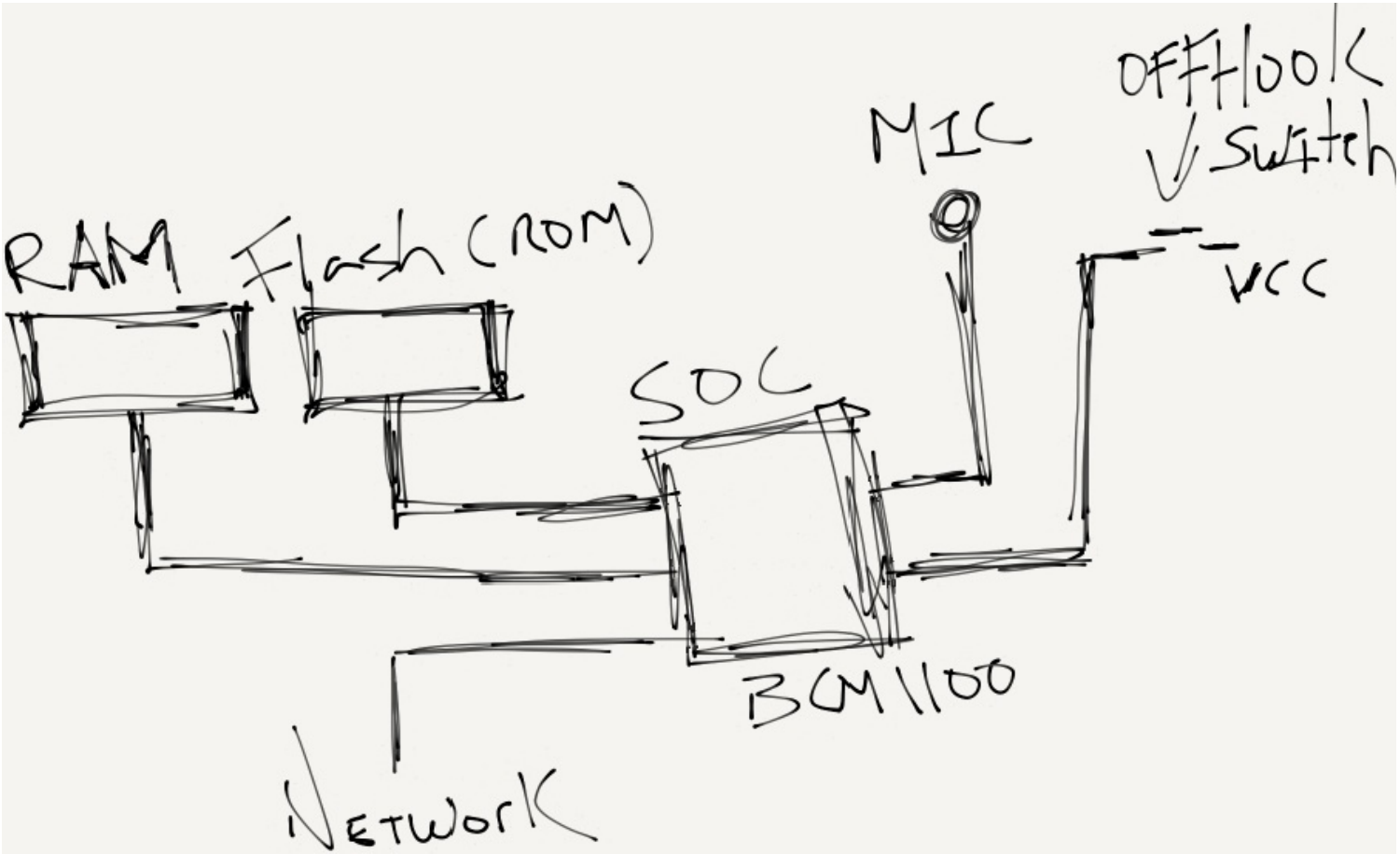
Client Python object oriented API and interactive shell



brmlab hackerspace prague

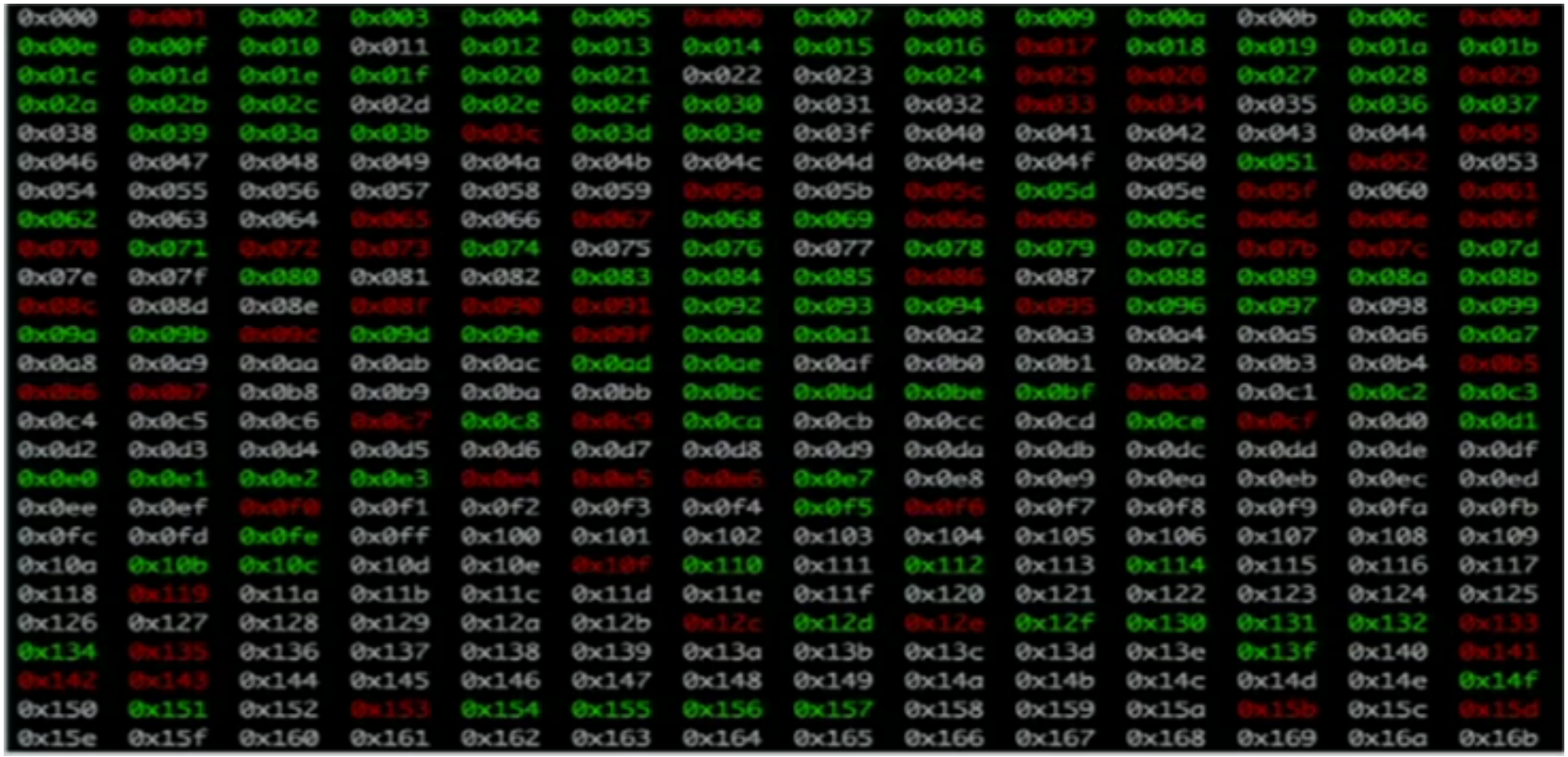
Ang Cui, Michael Costello - Hacking Cisco Phones

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



Ang Cui, Michael Costello - Hacking Cisco Phones

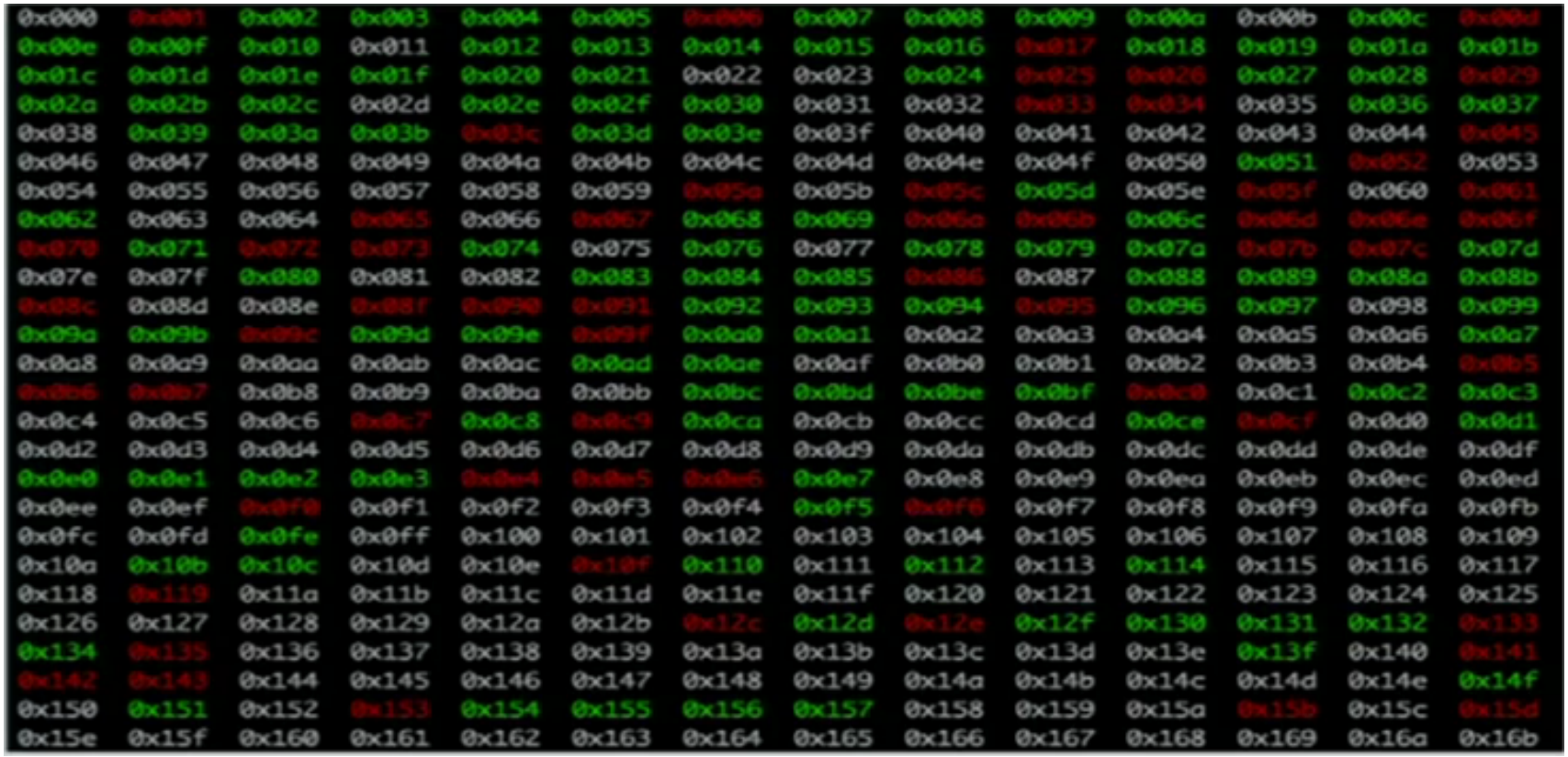
http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html



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

Ang Cui, Michael Costello - Hacking Cisco Phones

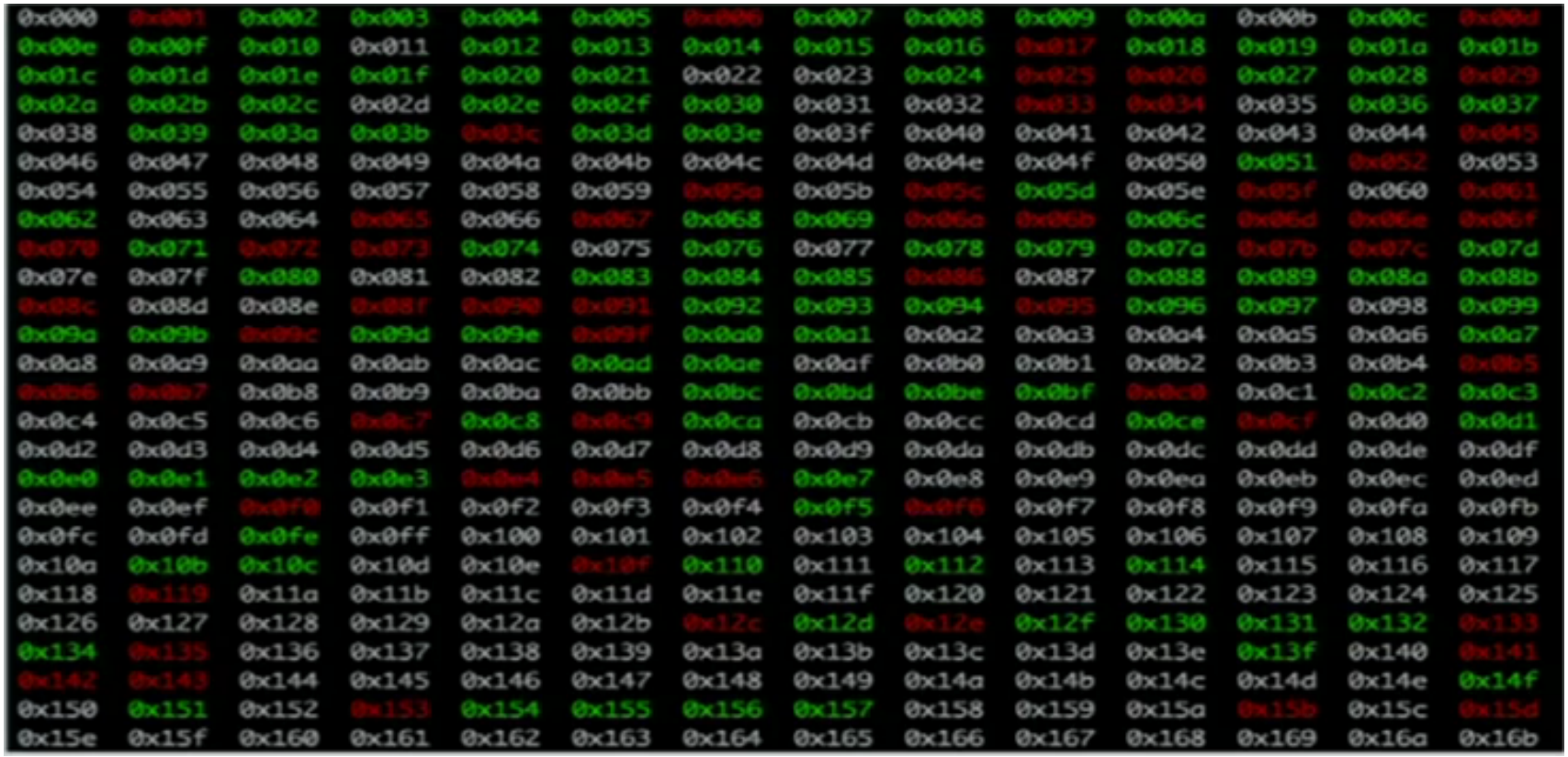
http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html



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

Ang Cui, Michael Costello - Hacking Cisco Phones

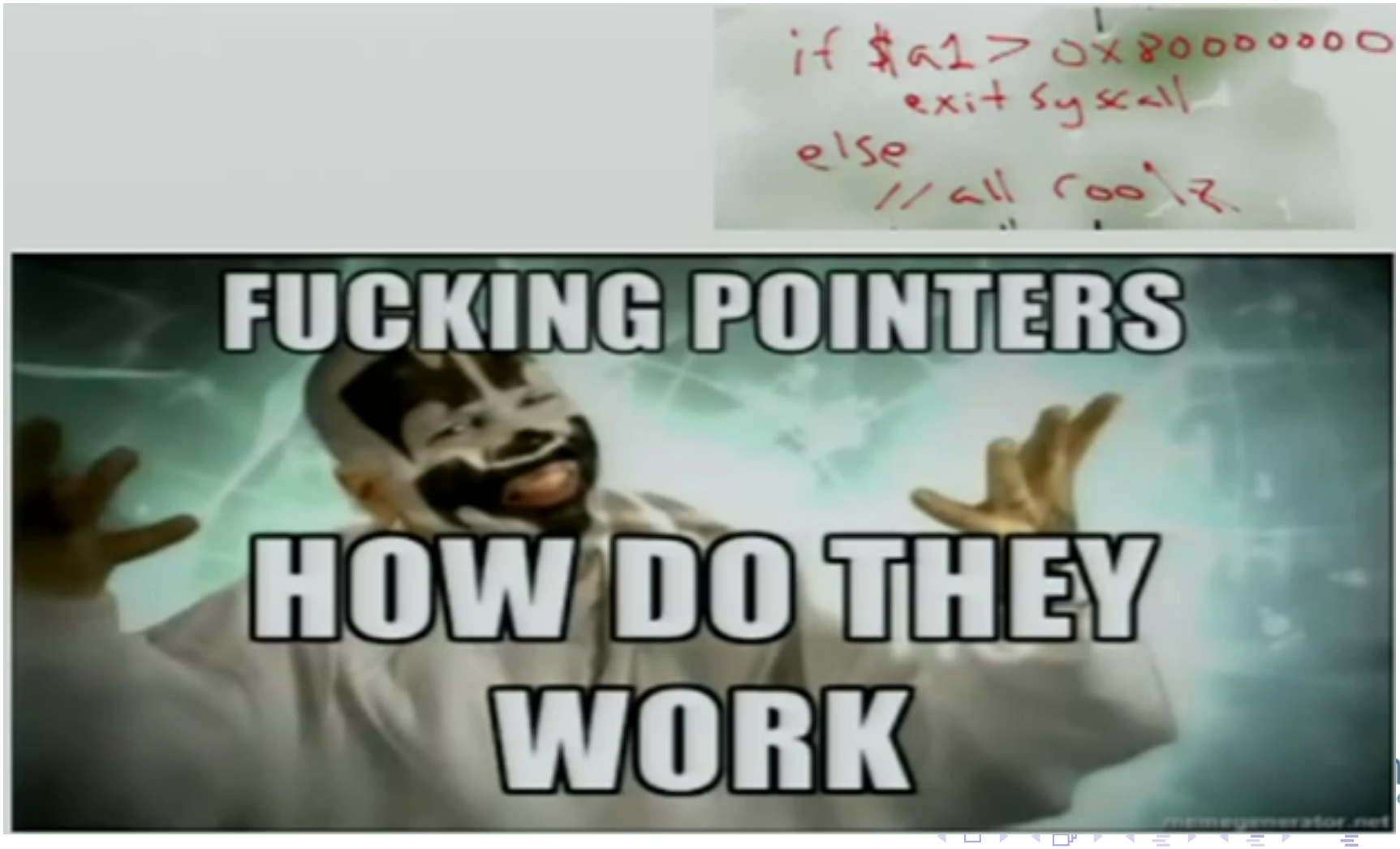
http://events.ccc.de/congress/2012/Fahrplan/events/5400.en.html



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

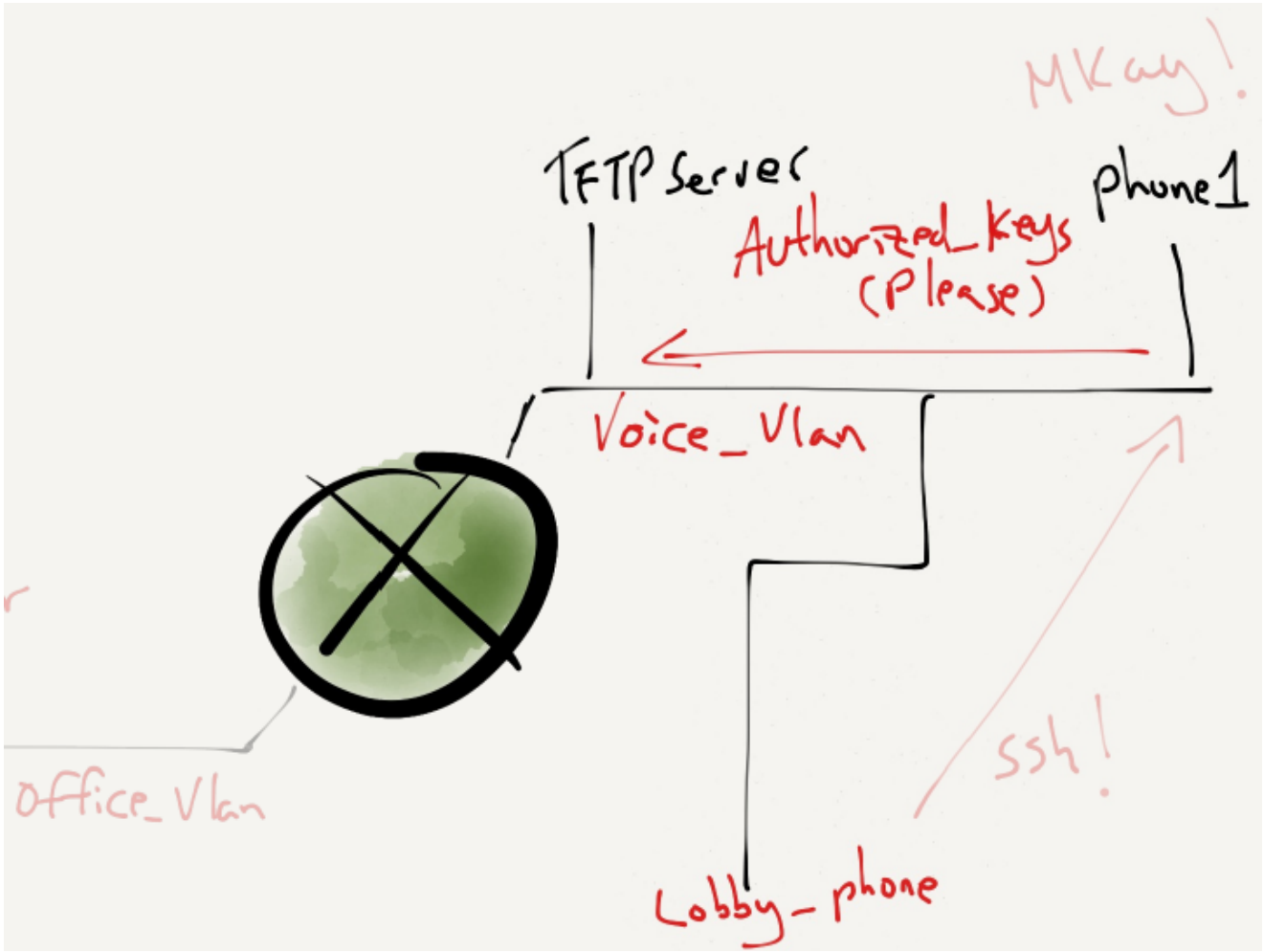
Ang Cui, Michael Costello - Hacking Cisco Phones

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



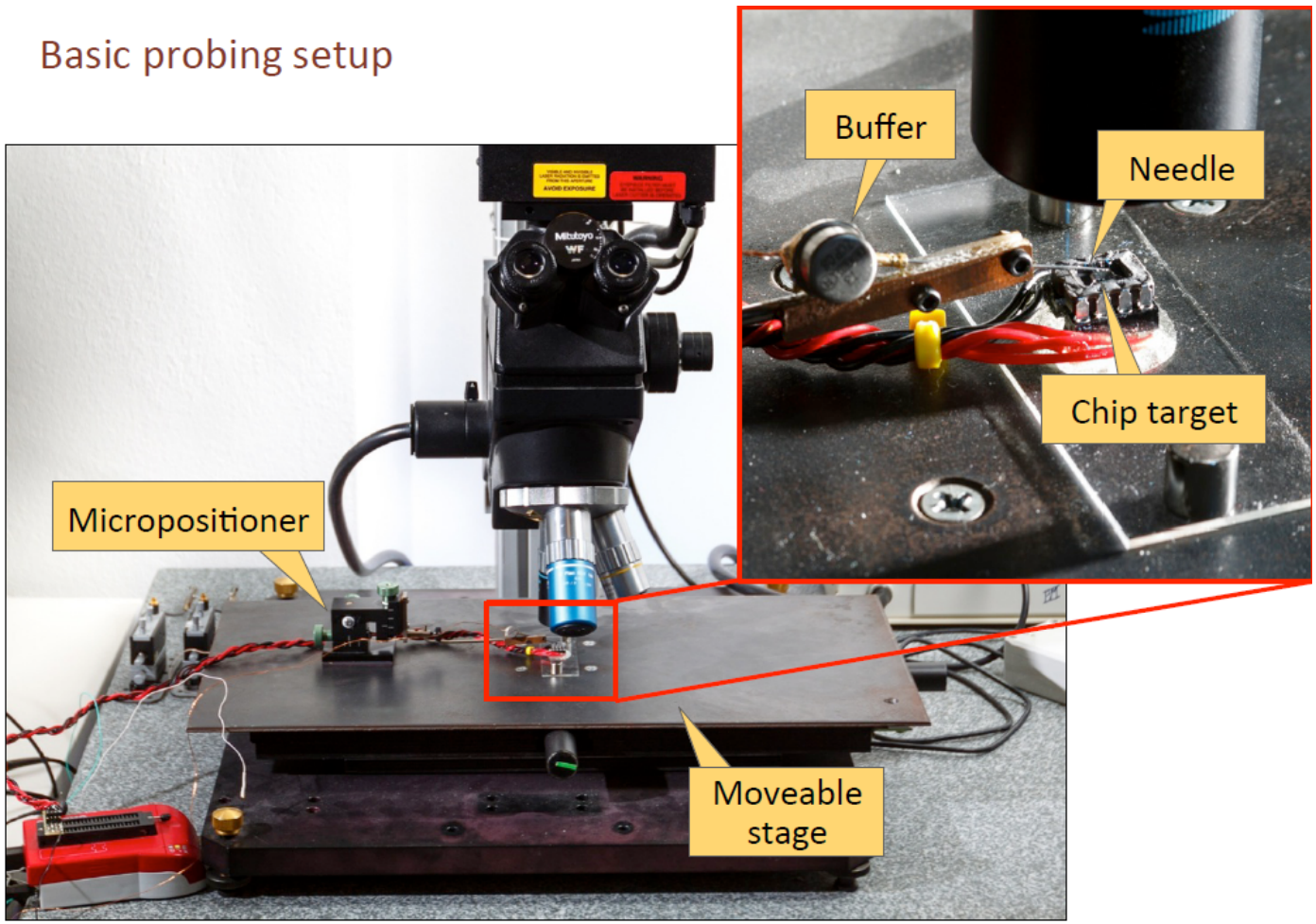
Ang Cui, Michael Costello - Hacking Cisco Phones

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



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`

brmlab hackerspace prague

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`

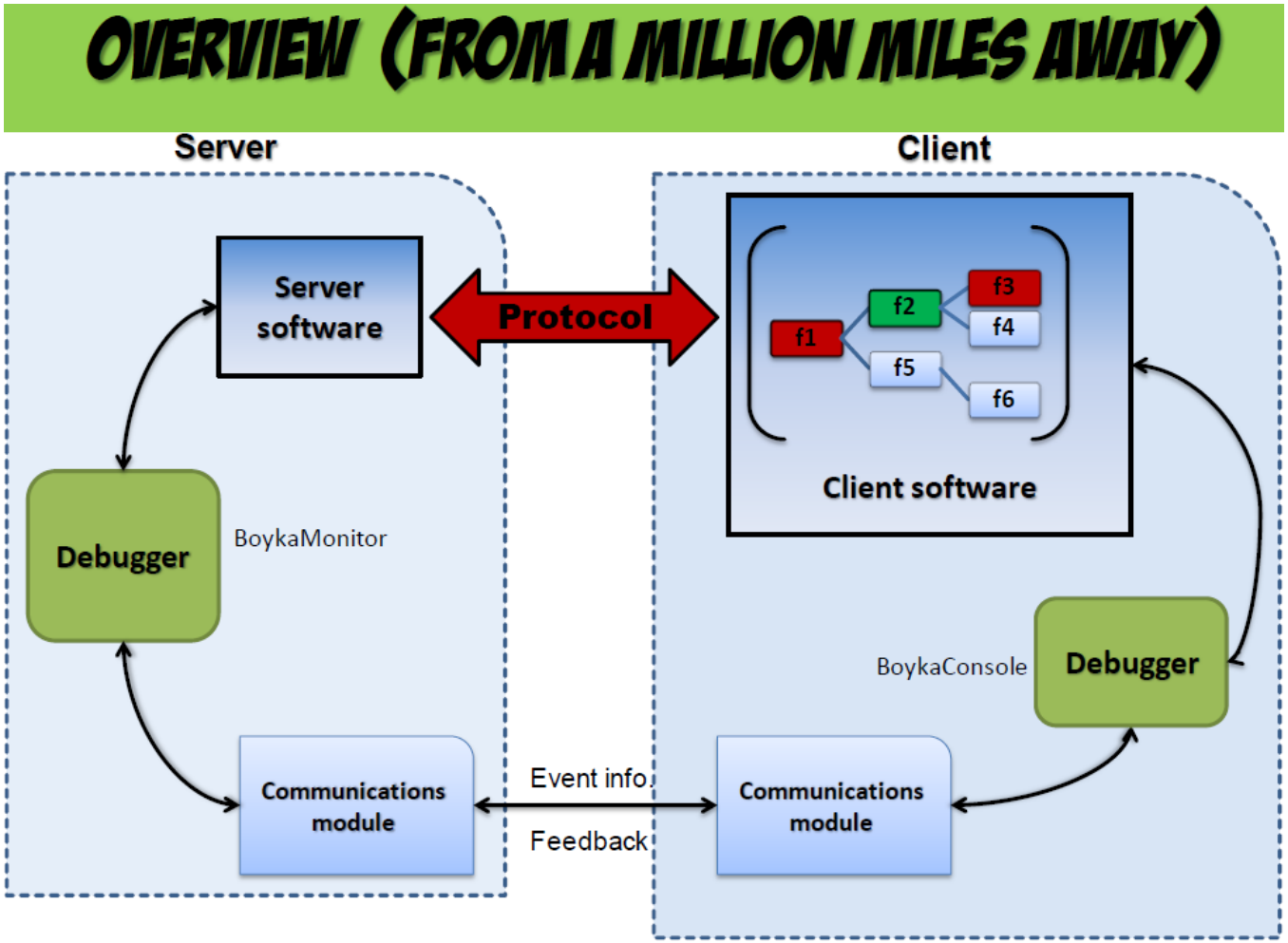
Carlos Garcia Prado - How I met your pointer

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

brmlab hackerspace prague

Carlos Garcia Prado - How I met your pointer

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



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 recieve 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 recieve 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 recieve 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 recieve 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 recieve 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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 (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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

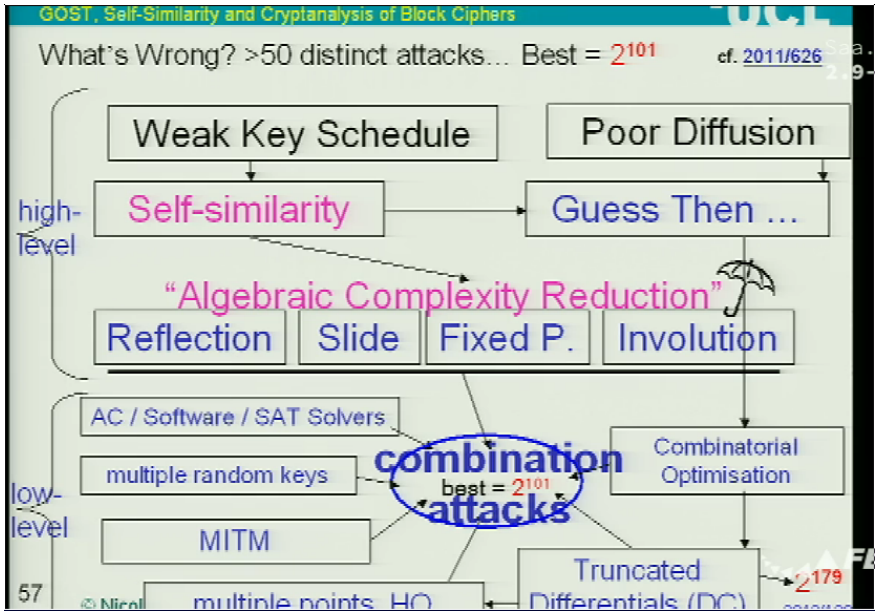
djb, Nadia Heninger, Tanja Lange - Facthacks

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

- RSA
- bad random-number generators (embeded deviced)
- generate both primes from a single search (shared modulos)
- 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

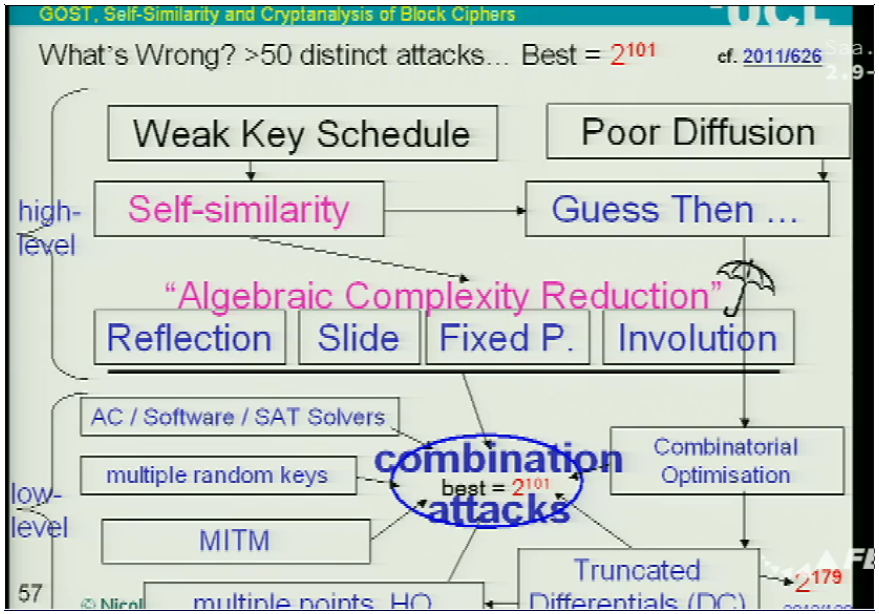
http://events.ccc.de/congress/2012/Fahrplan/events/5225.en.html



- 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

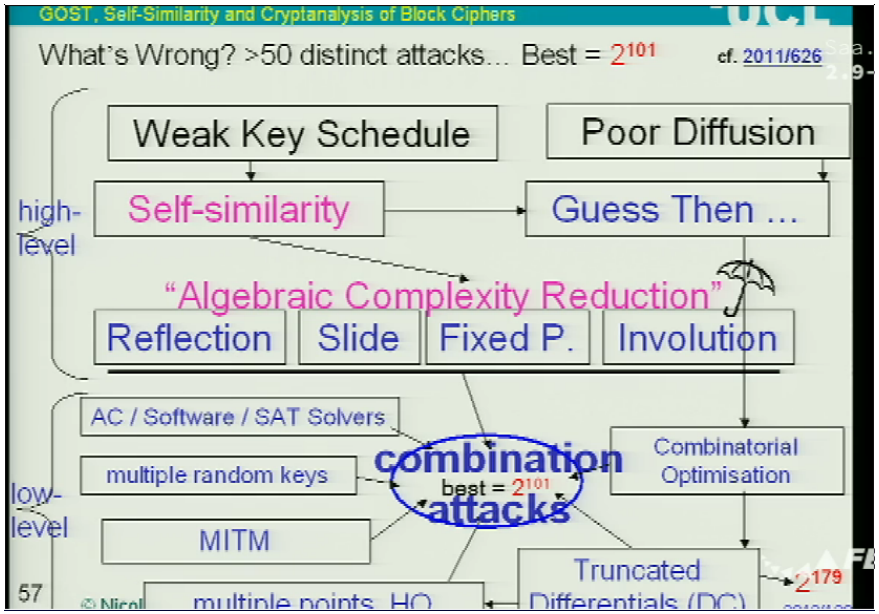


- GOST cipher is the official encryption standard of the Russian federation
- special versions for the most important Russian banks
- ☹ video not available at all mirrors

brmlab hackerspace prague

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

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



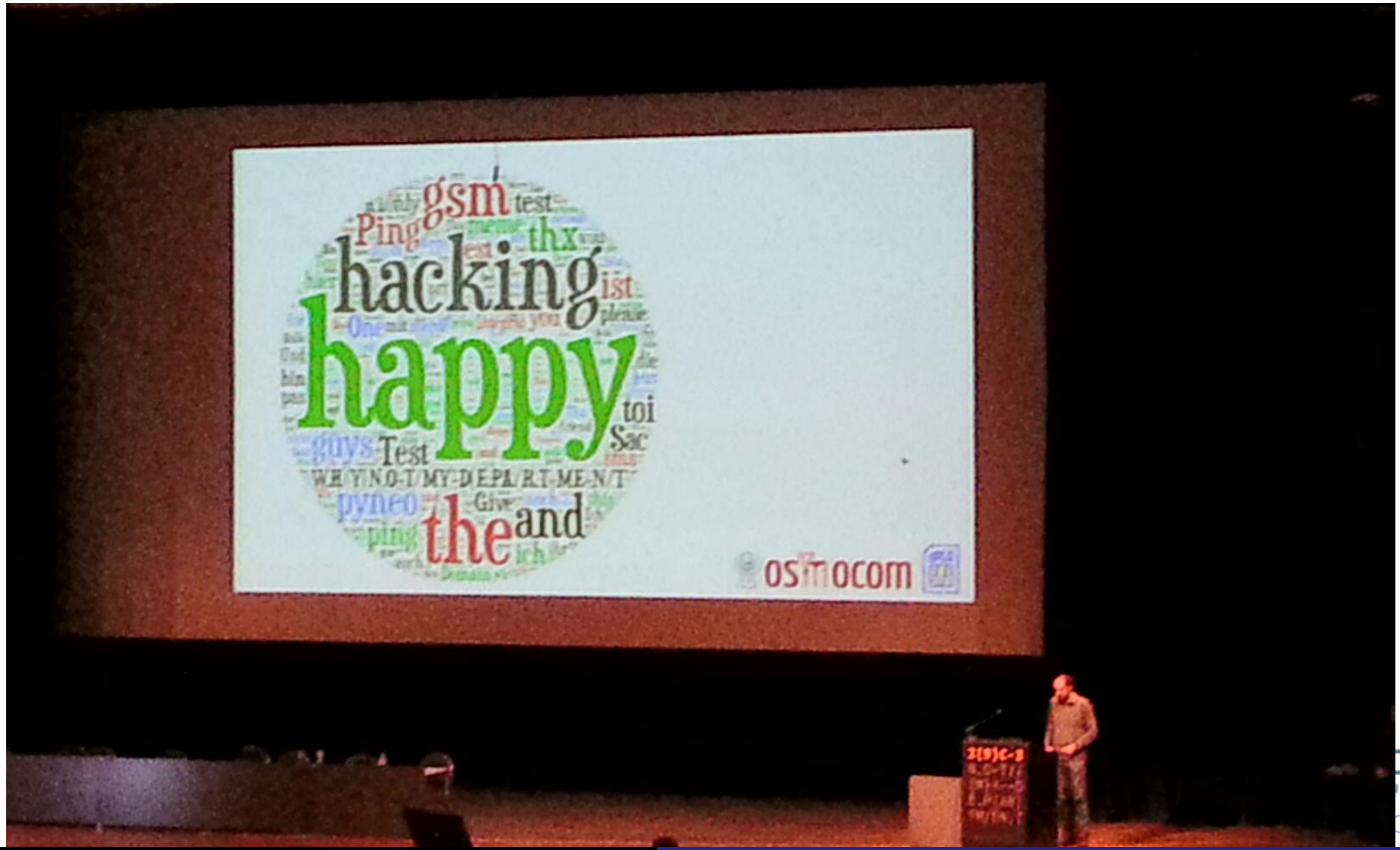
- GOST cipher is the official encryption standard of the Russian federation
- special versions for the most important Russian banks
- ☹ video not available at all mirrors

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

brmlab hackerspace prague