

NSA operation ORCHESTRA

- Annual Status Report



Poul-Henning Kamp

phk@FreeBSD.org

phk@Varnish.org

@bsdphk

What is this ?

This is a fictitious NSA briefing I gave as the closing keynote at FOSDEM 2014

The intent was to make people laugh and think, but I challenge anybody to prove it untrue.

Playlist spoiler:

Electric Light ORCHESTRA: Confusion

ABBA: Money, Money, Money

Backman Turner OVERDRIVE: Taking Care Of Business

QUEEN: Bicycle Race

Beastie BOYS: Sabotage

PASADENA Roof Orchestra: Pennies From Heaven

Operation ORCHESTRA

(TOP SECRET/COMINT)



ORCHESTRA operation at a glance

- * Objective:

- Reduce cost of COMINT collection

- * Scope:

- All above board
- No special authorizations

- * Means:

- Eliminate/reduce/prevent encryption
- Enable access
- Frustrate players

History of ORCHESTRA

- * Origin: The escape of the Inter-Net
- * Outside regulatory reach
 - No prior approval of equipment or coding
- * Hard to collect
 - Non-static routing
 - Too many networks/operators to deal with
- * Attempt to replace with OSI protocols failed
 - Would have continued TELCO+circuit model

ORCHESTRA origin

- * DEEP THOUGHT working group:
 - Gain control with key leverage points
 - Influence process to our advantage
 - Identify low cost/high impact persons

ABBA operations

Problem: Smart inventor

Somebody comes up with an idea that would make COMINT collection harder and/or more expensive

What can we do ?

ABBA operations

* Old School:

- Persuade/Bribe inventor to desist
- Classify patent application
- Swear people to silence
- Lots of paperwork
- Leaves traces
- Involves many people

ABBA operations

* New School:

- Exploit raw capitalism
- Ie: Throw money at the problem

Example ABBA operation

- * Spot a startup which could cause trouble
 - Yes, we read Reddit and HackerNews
- * Informal contact by "Venture Capitalist"
 - "Hello, saw you on HN, I'm rich, I'll drop by"
- * One or two visits to gather intelligence
- * Gain confidence
 - Talk the talk
 - Drop cash \$10K & "Get some better chairs"
 - Dinners, fancy food
 - "Let me know how I can help you out..."

Example ABBA operation /2

- * Locate patent in vicinity of business idea
- * Drop patent holder a hint
 - Direct if FON ("Friend Of NSA")
 - Indirect if not
- * Visit from patent lawyers kills startup
 - Often courtesey call back to VC: "We give up"
- * If patent not already in "good hands"
 - Attempt to locate better patent
 - Inspire patent transfer to good hands
- * Typical cost <\$30k

PASADENA operations

- * Rewarding embedded friends the old way:
 - Fake lottery winnings
 - "Distant relative" leaves fortune
 - Amazing job-offers
 - New identities
 - Loss of contact friend/families

- * Bend lots of rules

- * Hard to hide trails

- * Creation of identities and facts
 - Google made this very expensive

PASADENA operations

- * Rewarding embedded friends the new way:
 - "Hey boss, I quit!"
 - Create "startup"
 - "Locate" Venture Capitalist
 - VC makes heavy "wild chance investment"

PASADENA operations

- * Everything above board
 - Paperwork is routine
 - There are even standard tax-forms for this!
- * Mess around with "startup" for some years
 - Or get paid to surf the web...
- * Failed startup looks good on CV
- * Amazing fact: One PASADENA startup succeed!

OVERDRIVE activities

- * Influence business decisions
- * Using NSA contract/purchasing as leverage
- * Contract law = "Anything goes"
- * Plus
 - Good mechanism to solve big problems
- * Minus
 - Expensive, lawyers, competence
 - Real vs. stated objectives

OVERDRIVE example: Skype

- * Skype = P2P encrypted voice/video
 - Didn't use standard protocols
 - Out of FTC jurisdiction
 - Not open source
 - Did not bite on ABBA
- * Popular with independent actors
 - Human rights groups
 - US adverse political movements
 - Terrorists

OVERDRIVE example: Skype

- * First partner: eBay (SFON)
- * Minor considerations offered (FORN COMINT)
- * eBay buys skype in 2005 (\$4B)
- * Contract bungled by eBay lawyers
 - Only access
 - No source code
 - No control
- * Unclear why lawyers not briefed on objectives

OVERDRIVE example: Skype

- * Attempts to fulfill objectives failed
- * Cannot retry OVERDRIVE with eBay in game
- * 2009 eBay sells Skype back to founder (\$2.5B)
 - Not a happy FON any more.
- * 2011 MicroSoft (SFON) buys Skype (\$8.5B)
 - Ensured lawyers briefed on objectives
- * Microsoft centralized Skype architecture.
 - Full collection, no encryption.
- * Expensive, but necessary.

OVERDRIVE summary

- * Very big hammer for tricky nails
- * Being "In Your Face" is good camouflage
 - Certain FON's never questioned by press
 - Random Acts of Management == Genius

QUEEN activities

- * FOSS and Internet activities are consensus based
- * Nobody has special authority
- * "Rough Consensus and working code"
- * Heavy international participation
- * Significant talent available

QUEEN activities

- * In theory this is all Sec.State's domain
- * But:
 - Foggy Bottom not exactly tech-savy
 - Diplomats have no traction at IETF
- * On the other hand:
 - Works pretty well in ITU, ISO etc
- * Our goals are not always Sec.State's goals
- * Other players: DoC, NIST, DoD, FBI, CIA...

QUEEN activities

- * Leverage existing resources for influence
 - Embedded with FON's
 - Free agents
 - Witless "volunteers"

- * Deploy carefully designed "talking points"
 - "PSYOPS for Nerds"

 - Steer discussion to/from hot spots
 - Disrupt consensus building

QUEEN success example: SSC

- * Self Signed Certificates in Browsers
 - Offers privacy but no authentication
 - No cost to either party
 - Obvious as a no-config default

QUEEN success example: SSC

- * Concerted effort to derail consensus building
 - "Secrecy without authentication is pointless!"
 - "You could be talking to NSA" (!)
 - "Gives false sense of security"

QUEEN success example: SSC



This Connection is Untrusted

You have asked Firefox to connect securely to **ccc.de**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

[Get me out of here!](#)

- ▶ **Technical Details**
- ▶ **I Understand the Risks**

QUEEN success example: SSC



This Connection is Untrusted

You have asked Firefox to connect securely to **ccc.de**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

► Technical Details

▼ I Understand the Risks

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Add Exception...

QUEEN success example: SSC



You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.

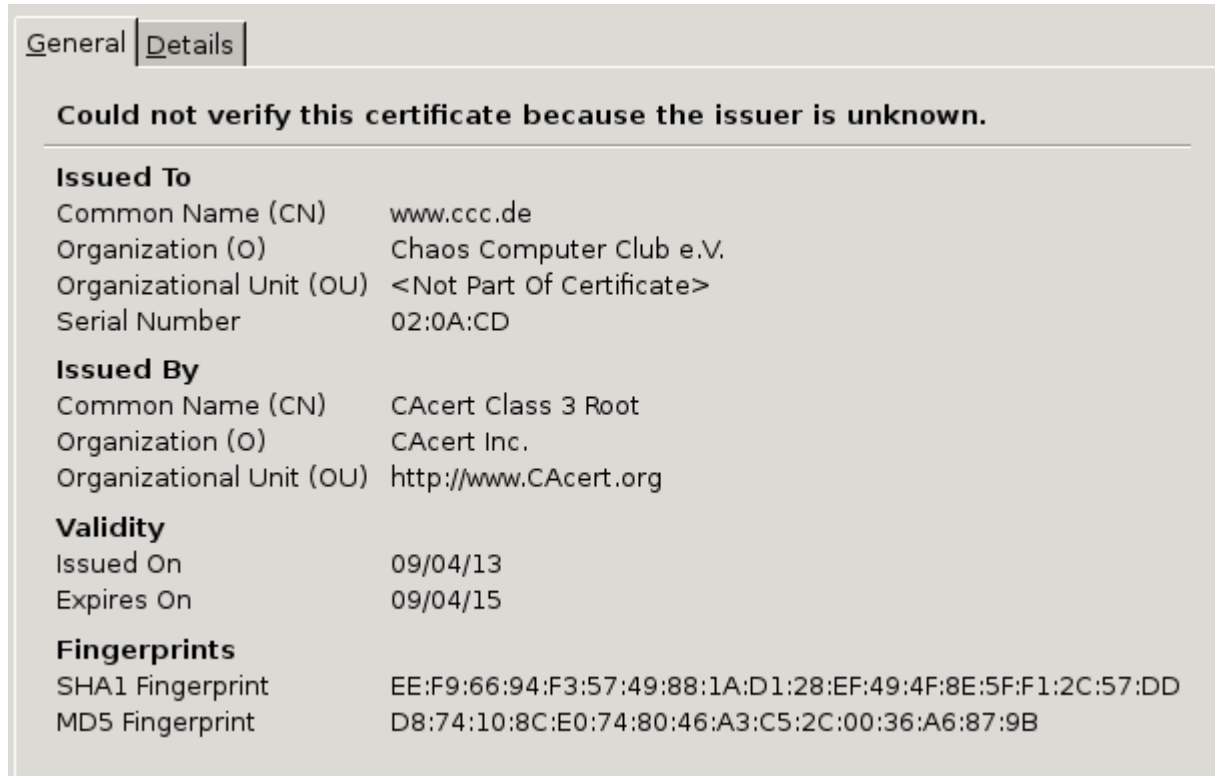
Server
Location:

Certificate Status
This site attempts to identify itself with invalid information.

Unknown Identity
Certificate is not trusted, because it hasn't been verified by a recognized authority using a secure signature.

Permanently store this exception

QUEEN success example: SSC



General | Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.ccc.de
Organization (O)	Chaos Computer Club e.V.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	02:0A:CD

Issued By

Common Name (CN)	CAcert Class 3 Root
Organization (O)	CAcert Inc.
Organizational Unit (OU)	http://www.CAcert.org

Validity

Issued On	09/04/13
Expires On	09/04/15

Fingerprints

SHA1 Fingerprint	EE:F9:66:94:F3:57:49:88:1A:D1:28:EF:49:4F:8E:5F:F1:2C:57:DD
MD5 Fingerprint	D8:74:10:8C:E0:74:80:46:A3:C5:2C:00:36:A6:87:9B

Kudos to CONFUCIUS: X.509 is Genius!

QUEEN achievements

- * No multihome routing without AS
 - Locks users to their ISP
 - Makes collection much simpler
- * No flow-routing in IPv6
- * Incompatible encrypted email
- * Delayed VoIP until Skype

QUEEN recent work

* HTTP/2.0

- Mandatory SSL/TLS
(Bring them into STING)
- Make MiTM Proxies official
- Fallback: Push for EMPTY BUCKET

QUEEN methods

- * FUD
- * Play GPL vs BSD card
- * "Bikeshed" discussions
- * Soak mental bandwidth with bogus crypto proposals

QUEEN recent work

* from CA to DANE

- Realization that PKI/CA
is compromised by everybody.
- Replace PKI/CA with "DANE"
- DANE = Cert validation via DNSSEC

QUEEN recent work

PKI/CA: Trust validation via TCP
+ 100s of compromised Root Certs

DANE: Trust validation via UDP
+ The single DNSSEC Root Cert
"Nudge, nudge, wink, wink,
he said knowingly..."

And: UDP = packet-race attacks

BOYS — A special gift

- * Program inspired by field accident
- * High value resource had to evacuate
- * No Company facilities nearby target area
- * Set up as independent contractor (sleeper)
- * Spent time hacking FOSS project for enjoyment
- * Spotted opportunities for groundwork

BOYS — A special gift

- * FOSS projects are based on trust, merit
- * No formal vetting, weak validation of evidence
- * Submit good patches for some years
 - Trust building exercise
 - Gradually eliminates code review
 - Collect SOCINT on project personnel
- * Once trust is in place
 - Affect code direction & quality

BOYS — A special gift

* Perception:

- "I'm sysad for a this non-profit org"
- "As long as Outlook works, they don't care..."
- "I'm not doing squat, it's all humming..."

* Reality:

- Org is NEIGHBOR shop-front
 - They need:
 - Personel for credibility
 - Non-shop IT support
 - Our man needs:
 - Chair, desk and ethernet
 - A cover story

* Bonus:

- Brass can report "Synergy of operations"

BOYS — A special gift

- * Don't: Obvious vulnerabilities

- Would be found
- Would blow cover

- * Do: Programming "mistakes"

- Self created
- Accepted as patches from 3rd parties

- * Do: General Code obfuscation

- * Do: Misleading docs

- * Do: Deceptive defaults

BOYS – A special gift

- * Doesn't need to work on core code
- * Example:
 - FreeBSD has 20k+ "ports"
 - Almost all crypto code is in ports
 - Ports maintainers work alone
 - Most ports have local FreeBSD patches
 - Nobody reviews those for security
 - Generally only if 'setuid'

BOYS — A special gift

- * Poster boy: Debian random
- * "This code makes Valgrind complain"
- * "doesn't seem to do anything"
- * Commented out
- * only 64k different random states for two years
- * Brute-forcing OpenSSL generated keys = trivial

BOYS — A special gift

- * Crown jewel: OpenSSL
- * Go-to library for crypto services
- * API is a nightmare
- * Documentation is deficient and misleading
- * Defaults are deceptive

Operation ORCHESTRA current status

- * Fantastic value for money
 - Less than 0.003% of COMINT budget
 - Have kept InterNet traffic in plaintext
- * No action ever exposed or traced back to us

Operation ORCHESTRA current status

- * SNOWDEN has no ORCHESTRA docs
 - All buried in "boring" departments:
 - Purchasing (OVERDRIVE)
 - Facility Management (BOYS)
 - Personnel (ABBA, PASADENA)