Life or Death Cryptology

It's not about the encryption algorithm

Intro

- Paul Bakker
- Maintainer of PolarSSL (Embedded SSL library in C and OpenSSL alternative)
- Fox Crypto (part of Fox-IT) develops products to protect information at a government level up to Top Secret
- All statements and opinions are personal

Later on

‘No Comment’

Later on

‘No Comment’ =~ /^No Comment$/

‘No Comment’ !~ /^Yes, .+$/

‘No Comment’ !~ /^No, .+$/

Small poll

- Among security experts and (other) paranoid people
- Security measures: What, how and why?

What secrets are people protecting

- Personal information
  - Chat logs
  - Personal photos
  - Emails
- Passwords
- Key material
- Financial / Banking Information

Measures taken

Virtual Machines

Firewalls

Anti-virus

SSH tunnels

(Open)VPN

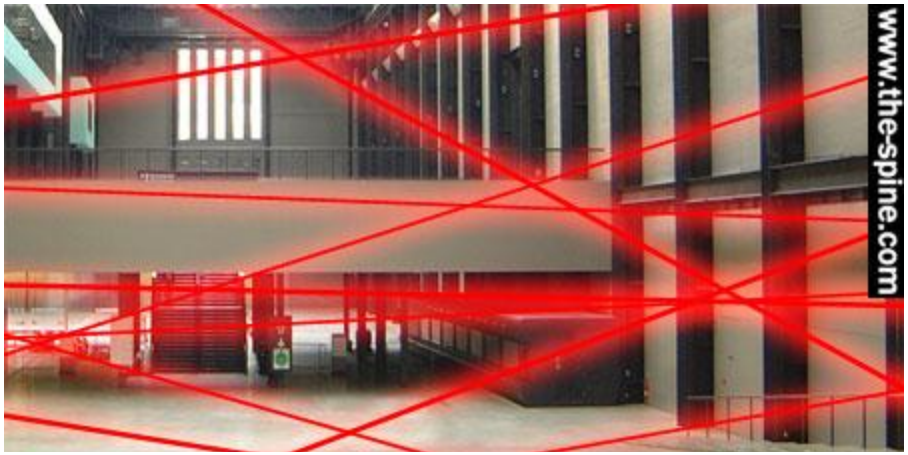
Password guidelines

Disk Encryption

Encrypted Containers

Extreme people, extreme measures

Laser Alarm and Tripwire



bit.ly/Hm6a3

Threats / Adversaries

- Mainly protection of privacy
- Random hackers
- Prevention of Identity Theft

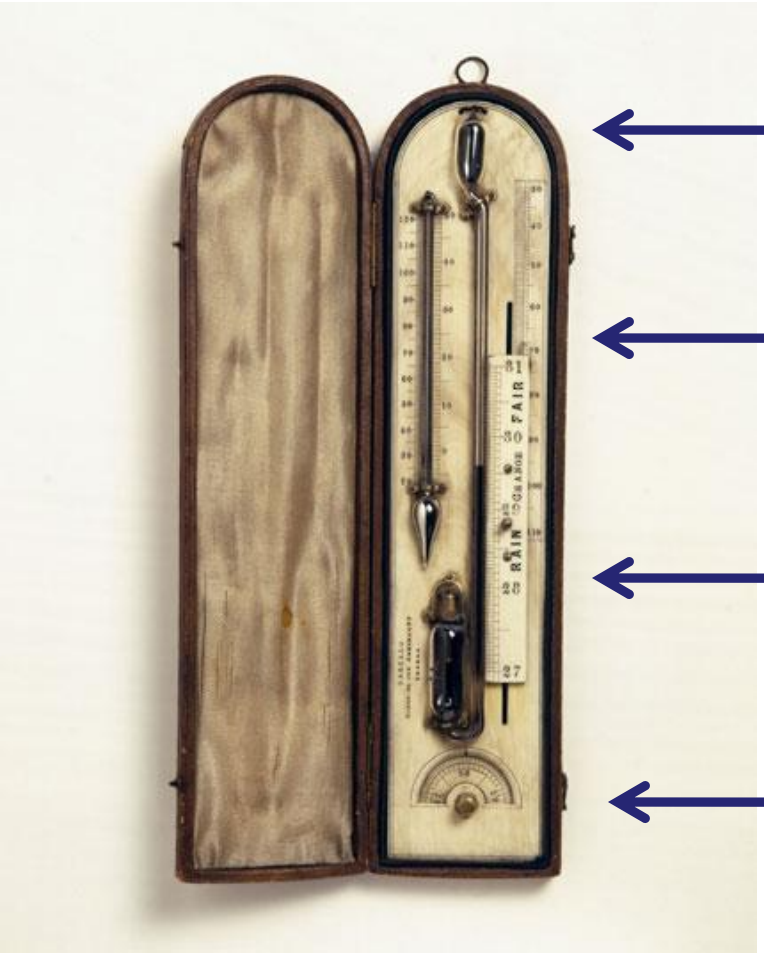
Poll conclusion

- Protection measures cover basic untargeted attacks and mass attacks
- No ‘real’ adversaries named (but most likely they would not tell me, would they?)
- But what about governments and law enforcement?

Real adversaries

- What happens if you do have real adversaries?
- Hard to tell
- But we might be able to use Espionage and National Security environments as an indicator

Security barometer



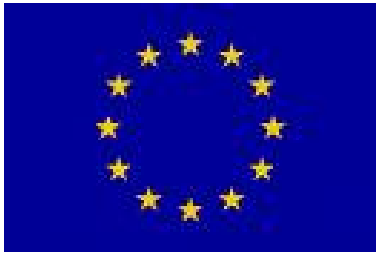
- Governments against espionage
- Interesting zone
- Security-aware person
- The average person

Differences in government sectors

- Budgets are higher, funded adversaries
- Stakes are huge
  - Economic stakes
  - National Security
  - Threats to autonomy
- Targeted attacks (e.g. Ghostnet)

bit.ly/1Asl4P

But aren’t we all friends?



Laws and regulations

- Espionage allowed (e.g. USA, UK, France)
  - NSA launches spy satellites and builds huge data centers (Not for gaming)
- Wiretapping (e.g. USA, Sweden)
- Limiting cryptographic products (Wassenaar Arrangement)

bit.ly/1gtkTa, bit.ly/1UNdID, bit.ly/cPsnP, bit.ly/3dreS

Facts or fiction?

- It’s a very shadowy and secret world

- Almost no facts exist
- We can only learn by looking at what history tells us

Cryptography

- Used to be an all government business (prior to the seventies)
- Governments: Cracking the codes
  - Enigma success story
- Major funded governments ahead of the competition

bit.ly/T6Vsp

Governments ahead of public in 70s

- Large amount of research in cryptographic theory
- But on the brute force front cracks are showing

DES

- Introduced in 1976
- Cryptographical knowledge ahead of the public
  - Extremely resistant to differential cryptanalysis (publicly found in 1990)
- Brute force capacity problems?
  - Key size crippled from 128 bits to 56 bits

bit.ly/13RHNd

What to do?

key_size > max_brute_force_capacity

Intentional (public) crippling examples

- Workload Reduction Factor
- A5/2
- Clear Zone

Workload Reduction Factor

``We deliver 64 bit keys to all customers, but 24 bits of those in the version that we deliver outside of the United States are deposited with the American government."

Eileen Rudden, vice president at Lotus

http://bit.ly/j4pi0

A5/2

- A5/x - used for securing over-the-air communication between mobile phone and tower
- A5/1 is default

  (And not so secure either)
- A5/2 is deliberately weakened for export

bit.ly/uTb2y, bit.ly/12jRcx

Clear Zone

- Group of 13 countries headed by Cisco

  Including Microsoft, Netscape, Sun, Network Associates

- ‘Clear Zone functionality exists in most firewalls, VPN devices and encrypting routers.’

bit.ly/80ULj, bit.ly/IqITO, bit.ly/sKpFf

Export laws less strict in 2000

- Brute forcing of encrypted data is near impossible
- Theoretical security is very high

So?

export prevention of secure algorithms

and

limiting key sizes

fails

Emissions

- 1954: the Soviets suddenly start using very strict interference guidelines for communication equipment and teletypewriters

bit.ly/d5UN

Emissions

- Discovery in 1964 in the US embassy in Moscow:
  - more than 40 regular microphones
  - unpublicized gadgets with microphones
  - Large metallic grid in the ceiling with a wire attached

—Associated Press Wirephoto

LISTENING DEVICES FROM U.S. MOSCOW EMBASSY
Instruments displayed at State Department in Washington

U.S. Finds Microphones In Its Moscow Embassy

40 Electronic 'Ears' Dug From Walls; Search Continues For Other Devices

WASHINGTON, May 20 (AP)—U.S. security agents have dug more than 40 secret microphones out of the walls of the American embassy building in Moscow during the past month and are searching for others

bit.ly/AFxgc

Tempest: A Signal Problem

TEMPEST: A Signal Problem

**The story of the discovery
of various compromising radiations
from communications and Comsec equipment.**

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of inspecting the area around his little cryptocenter. As required, he was examining a zone 200 ft. in radius to see if there was any "clandestine technical surveillance." Across the street, perhaps a hundred feet away, was a hospital controlled by the Japanese government. He sauntered past a kind of carport jutting out from one side of the building and, up under the eaves, noticed a peculiar thing—a carefully concealed dipole antenna, horizontally polarized, with wires leading through the solid cinderblock wall to which the carport abutted. He moseyed back to his headquarters, then quickly notified the counter-intelligence people and fired off a report of this "find" to Army Security Agency, who, in turn, notified NSA. He was directed to examine this antenna in detail and perhaps recover it, but although the counter-intelligence folks had attempted to keep the carport under surveillance that night, the antenna had mysteriously disappeared when they checked the next day. Up on the roof of the hospital was a forest of Yagi's, TV antennae, all pointing towards Tokyo in the normal fashion, except one. That one was aimed right at the U.S. cryptocenter.

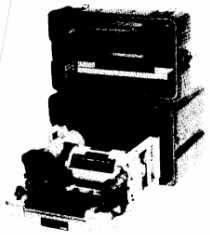
You may recall the highly publicized flap which occurred in 1964 when more than 40 microphones were discovered in the U.S. embassy in Moscow. Most people were concerned about all the conversations that may have been overheard and the resultant compromise of our diplomatic plans and intelligence activities associated with the embassy. We were concerned with something else: What could those microphones do to the cryptomachines used there? And what were the unpublicized gadgets also found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the Department of State communications area? A grid with a wire leading off somewhere. And what was the purpose of the wire that terminated in a very fine mesh of smaller hair-like wires? And, while we were at it, how did these finds relate to other mysterious finds and reports from behind the Curtain—reports dating clear back to 1953?

Why, way back in 1954, when the Soviets published a rather comprehensive set of standards for the suppression of radio frequency interference, were those standards much more stringent for their teletypewriters and other communications equipment than for such things as diathermy machines, industrial motors, and the like, even though the teletypewriters were much quieter in the first place?

Behind these events and questions lies a long history beginning with the discovery of a possible threat, the slow recognition of a large number of variations of that threat, and, lumbering along a few months or a few years afterwards, a set of countermeasures to reduce or eliminate each new weakness that has been revealed.

The Problem Defined

To state the general nature of the problems in brief: Any time a machine is used to process classified information electrically, the various switches, contacts, relays, and other components in that machine may emit radio frequency or acoustic energy. These emissions, like tiny radio broadcasts, may radiate through free space for considerable distances—a half mile or more in some cases.



The TSEC/KL-7, Electromechanical Literal Cipher Machine, a crypto-equipment long in use by the U.S. and its Allies

The TSEC/KL-7A, the version of the KL-7 modified

Anomalies

bit.ly/d5UN

TEMPEST

“Tiny ElectroMagnetic Particles Emitting Secret Things”

First public references:

- 1985, Wim van Eck: "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?”

Current developments

- In academic world in the last 10 years:
  - Eavesdropping on CRT, TFT by radiation
  - Acoustic Keyboard eavesdropping
  - Laser assisted Keyboard eavesdropping
  - Keyboard snooping by Power emissions

bit.ly/BSebh, bit.ly/2vaYYC

Emission eavesdropping

There seems to be a very large gap between real academic results and government involvement

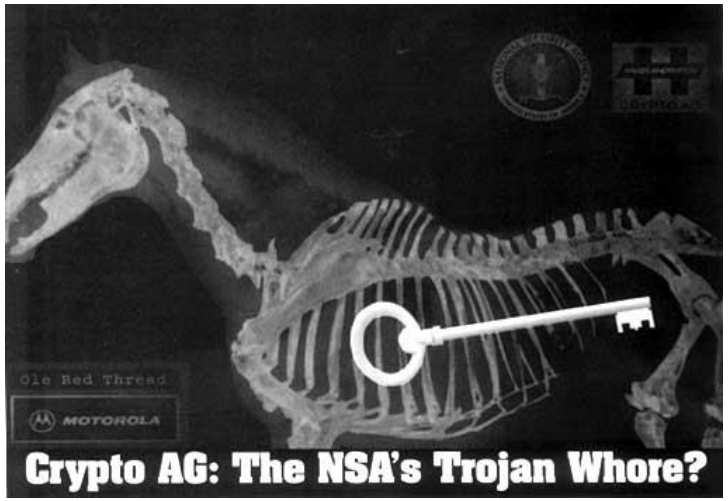
Shifting interests

- Brute forcing encryption is near impossible
- Limiting maximum key lengths not really effective
- Eavesdropping via emanations requires a (temporary) physical presence
- New venues have opened: Backdoors

Crypto A.G.

- Major developer and distributor of cryptographic equipment

- NSA involvement discovered in 1992
- 1956: secret alliance between NATO and Swiss



bit.ly/iZVDt

Crypto A.G.

“While the United States and other leading Western countries required completely secure communications, Mr. Hagelin explained, such security would not be appropriate for the Third World countries that were Crypto's customers.”

bit.ly/whpYY

Greek tapping scandal

- Until 2005 more than 100 mobile phones of government officials tapped
- “Stealth software” in the Vodafone system that ‘enabled’ Ericsson’s lawful interception feature
- Day before announcement a software engineer committed ‘suicide’

bit.ly/hgM4w, bit.ly/4OB9b

Blackberry UAE incident

- Blackberry subscribers for Etisalat received a WAP Push to download a JAR named “registration”
- Surveillance software inside JAR for sending information to government organizations

bit.ly/FTnSJ

Blackberry USA

“While BlackBerry e-mail traffic is encrypted, a US federal law enforcement source said it can all be recovered. “You can get the whole suite” of services, including e-mail, voice calls, text messages and direct BlackBerry-to-BlackBerry PIN messages, which take another route, he said.”

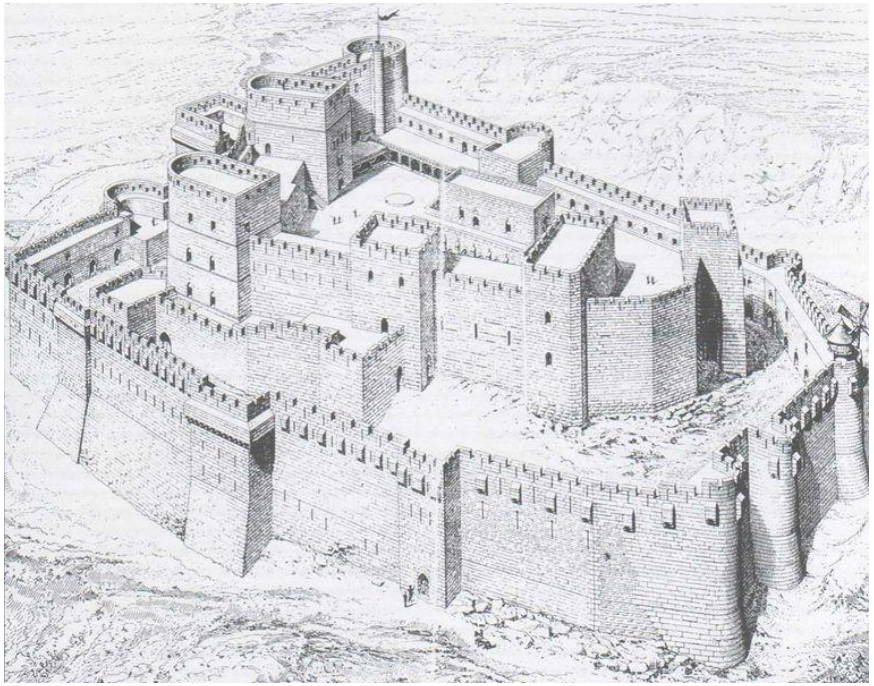
bit.ly/2NTDaK

So what now?

Can’t we trust anything anymore?

Protecting secrets at government level

- Defense in depth
- Countermeasures:
  - Physical
  - Technical
  - Procedural
  - Environment
  - Transport



Protecting secrets at government level

- Red/Black separation
  - Separating the encrypted and unencrypted information (Digital and analog)
  - Strict interfaces between two domains
- Shielding of equipment
  - Filtering of Power Supply
  - Filtering of emissions
  - Single point grounding

Protecting secrets at government level

- Tamper resistance
  - Preventing manipulations
  - Preventing attachment of extra hardware / antenna's
  - Also seen in HSM's within financial sector
- Secure boot process
  - Guarantee integrity of system
  - Gaining ground even in commercial markets (Game systems, PS, Xbox, etc.)

Secure Design

But even secure design is not enough!

Trusted Development

Crypto A.G.

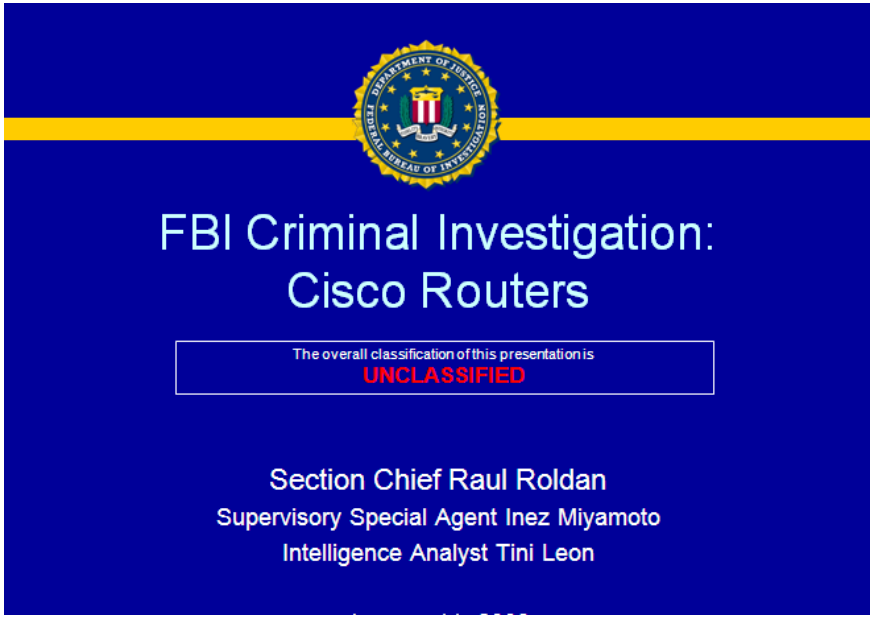
Production Backdoors

- Embedding backdoors in processors before production
- Minimal changes needed

bit.ly/OuCqz

Supply Chain Backdoors

- 2008: FBI finds Critical Infrastructure Threat
- Counterfeit Cisco equipment are found all over government.
- Backdoors anyone?



bit.ly/j1bZG , bit.ly/4mIx0d

Protecting secrets at a government level

Trust is everything

Afterthoughts

- Protecting secrets is hard
- Protecting very valuable secrets is extremely hard
- It all boils down to trusting your security measures
- So what now?

What now?

Don’t have too many secrets!

What now?

Don’t worry

(You are probably not THAT important)

What now?

- Gain trust in your security measures
  - Open Source might give you the right measure of trust
  - Open Hardware is still in the early phase
- Be aware of the risks if you really do have something important.
- Protect your assets from manipulation

Question

Is your laptop currently

unattended

in your tent?

Contact Info

HAR2009:

At the Fox-IT tent on field E

After HAR2009:

E-mail: p.j.bakker at brainspark dot nl

PolarSSL: http://www.polarssl.org

Presentation: http://bit.ly/7wP1Y