

# Cryptographic Applications in Industry (II)



For COINS Winter School 2016 @ Finse

Anders Paulshus, Director System Security Conax

# Bio

- Anders Paulshus
- Industrial mathematics, NTNU
- Research Scientist Crypto, NSM
- Director System Security, Conax
- External examiner «[UNIK4220 Introduction to cryptography](#)» @ UiO

# Pay-TV threat model

- Pay-TV is a global marketplace
- Classical pirates know how to monetize on obvious assets (TV-content, keys, hardware etc)
- However, in real world applications, it may be misguided to narrow down the threat model
- History tells us the threat to pay-TV may come from many avenues



# In the news (2010)



## – Sendte pirat-TV til tusenvis av kunder

Fra en jungel av ledninger og pc'er i en kjeller skal 41-åringen ha forsynt tusenvis av kunder med ulovlige tv-signaler.

Del med andre:

Twitter Facebook 30 personer anbefaler dette.

Politiet mener de har avslørt det som er Norges største saksomhandler distribusjon av ulovlige tv-signaler.

Så mange som 4 500 husstander, primært i Oslo-området, kan være koblet til det ulovlige pirat-nettet som en 41 år gammel mann skal ha stått bak.

Vel du noe om denne saken? Kontakt TV 2s reporter her!

### Begynte med Norges største sigarettbeslag

Hele saken begynte med at Tollvesen skal kom over et gigantisk lager av ulovlige sigaretter i Oslo rett før jul.

TV 2 har fått tilgang til Tollvesens og politiets egne bilder fra saken de etterforsker



Espen Carlsen  
espen@tv2.no

Publisert: 20.09.2010 20:56  
Oppdatert: 20.09.2010 22:38

Del med andre

Facebook Twitter

Diigo Netty

Tips en venn

E-post til redaktør

Du er innlogget

Du er innlogget

Du er innlogget

Du er innlogget

Du er innlogget

Du er innlogget



BYE HACKING: Canal Digital valgte å bytte en halv million tv-kort for å forhindre med hackere. Her Ståbjørn Thomsen Oust ved en Canal Digital nettside på Telenor Arena i forbindelse med en kamp mellom Statens og Rosenborg United-hersteds. FOTO: SCAMEDIA

## Måtte bytte en halv million tv-kort

Bli kvitt KVISER & URENHETER  
Påve produktene Hollywoodstjerne Longre til dette lille sunn-holiday alle de trenger for skikkelig vakker hud  
kun 1079,-

Canal Digital nektet å forhandle med hackere.

Hackerne startet å knække koden til en halv million tv-kort og ville dermed forhandle med Canal Digital om å bytte ut kortene med nye. Selskapet valgte heller å bytte ut kortene med nye.

Tegningene i Canal Digital ville ikke forhandle med kriminelle og valgte heller å bytte ut alle de millioner knuser med å bytte ut en halv million smartkort, skriver VG.

Sikket på Kjøffa  
Slippe anise er en 47 år

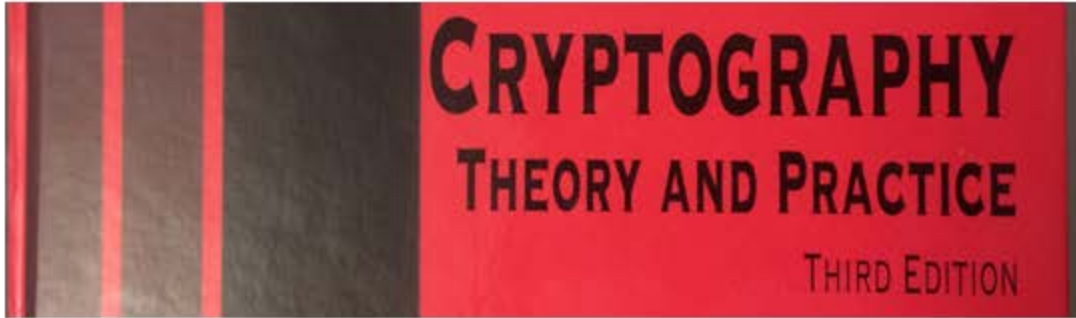
Enneord  
nablar satst digital tv.uss.nablar

C-Date  
Lyst på en spennende date?  
KLIKK HER

Nyheter  
med best bilder 24 timer

Play helikopter til Abu Dhabi for en dags jobb  
På 100 dager har vi for en drage arbeid.

Jeg har slått ham i hodet med hammer



# CRYPTOGRAPHY

## THEORY AND PRACTICE

THIRD EDITION

- Theory:  
Cryptography help you  
hide secrets
- Practice:  
Cryptography gives you  
secrets to hide

### The Cryptography API, or How to Keep a Secret

Robert Colenidge  
Microsoft Developer Network Technology Group

August 19, 1996

#### Abstract

This article describes the Microsoft® Cryptography application programming interface (API) that is available with the new Windows NT® version 4.0 release and upcoming versions of Windows 95. The article explains what is required to use various features of the Cryptography API. The article is available at <http://www.microsoft.com/development/nt40/nt40crypt.htm>.

# The key problems

- Key storage
- Key usage
- Key distribution
  
- In «one word»: Key management

# Classes of crypto equipment

AES  
found  
here

- **Military grade**
  - Strict requirements
  - Evaluated, certified,
  - Controlled distribution
  - Military communications system, CCIS,
- **Industrial grade**
  - Commercially available, possibly evaluated (e.g. CC, FIPS)
  - Mobile phones, banking applications, pay-TV, Networking equipment for businesses (e.g. VPN)
  - Very often hardware
- **«Toy crypto»**
  - Downloadable software, apps, etc.
  - Home networking equipment

# Distinguishers

- Security evaluation, inspection
- Formal security requirements
- Hardware protection
- Key management



# Claim #1

- Cryptographic strength in industrial applications is limited by its key management system
  - Cryptographic strength < algorithmic strength

# Claim #2

- Real cryptographic strength cannot be assessed independent of its physical implementation

# Claim #3

- Cryptographic strength in industrial applications is best measured by penetration tests.

# The key problems

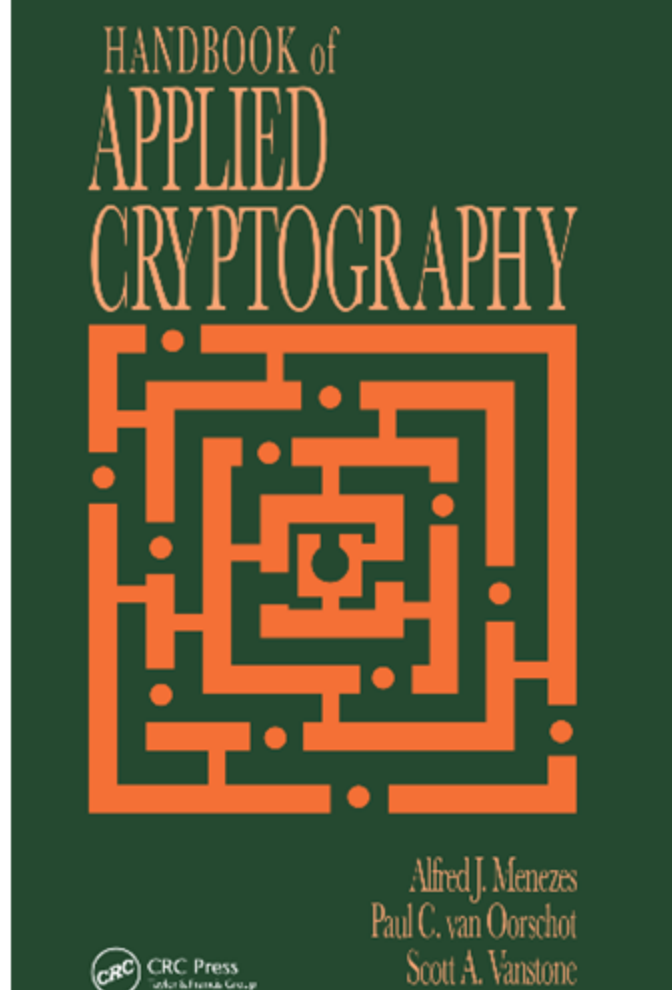
- Key storage
- Key usage
- Key distribution

# Key storage

- A cryptographic key cannot be reliably remembered.
  - Passwords (and KDFs) isn't sufficient for industrial applications
- Physical/electronic storage is always necessary.


# Key storage

- Exercise:
  - Pick up your favourite text book on cryptography and look up «key storage».
- You're designing cryptography to withstand adversaries with computing powers of teraFLOPS, or even quantum computers...



# Key storage in software

- Plaintext keys in machine-readable memory are prone to attacks.
- Cryptographic keys have special properties that allows for easy detection and identification:
  - Key wrap standards, entropy, bit-lengths, parity bits (DES), primality testing (RSA)
- Cryptography can help you reduce the problem to (minimum) one key.
  - Key hierarchies
  - One «master key»
- For software algorithms, keys may be reconstructed from remnants of key schedules etc. (e.g. [Maartmann-Moe, Thorkildsen & Arnes, 2009](#))



available at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

Journal homepage: [www.elsevier.com/locate/din](http://www.elsevier.com/locate/din)

Digital Investigation

---

## The persistence of memory: Forensic identification and extraction of cryptographic keys

Carsten Maartmann-Moe<sup>a,\*,1</sup>, Steffen E. Thorkildsen<sup>b</sup>, André Arnes<sup>a,2</sup>

<sup>a</sup>Department of Telematics, Norwegian University of Science and Technology, O.S. Bragstads plass 2B, N-7031 Trondheim, Norway  
<sup>b</sup>National Criminal Investigation Service, Norway  
<sup>c</sup>Norwegian Information Security Laboratory, Qvæk University College, PO Box 291, N-2022 Qvæk, Norway

---

### ABSTRACT

**Keywords:**  
Digital forensics  
Data hiding and recovery  
Memory analysis  
Memory dumping  
Applied cryptography  
Line analysis  
Cryptographic evidence  
Incident response  
Tooltesting and development

The increasing popularity of cryptography poses a great challenge in the field of digital forensics. Digital evidence protected by strong encryption may be impossible to decrypt without the correct key. We propose novel methods for cryptographic key identification and present a new proof of concept tool named *Invertate* that searches through volatile memory and recovers cryptographic keys used by the ciphers AES, Serpent and Twofish. By using the tool in a virtual digital crime scene, we simulate and examine the different states of systems where well known and popular cryptosystems are installed. Our experiments show that the chances of uncovering cryptographic keys are high when the digital crime scene are in certain well-defined states. Finally, we argue that the consequences of this and other recent results regarding memory acquisition require that the current practice of digital forensics should be guided towards a more forensically sound way of handling live analysis in a digital crime scene.  
© 2009 Digital Forensic Research Workshop. Published by Elsevier Ltd. All rights reserved.

---

### 1. Introduction

Cryptography has grown to become one of the most important contributors to privacy and data security in an increasingly interconnected world. The use of cryptography also represents a challenge for digital forensic investigators, as it may be used to hide data that may shed light on the chain of events that constitutes an incident or crime. Since the nature of cryptography makes it attractive for hiding incriminating data, encrypted material encountered often contain exactly the evidence sought by investigation.

In this paper, we aim to study new methods for the identification and extraction of cryptographic keys from the volatile memory of computing devices as part of the digital forensic process. In this context, the keys and any encrypted contents may be considered to be digital evidence (i.e., digital data that contains reliable information that supports or refutes a hypothesis about an incident [Carrier and Spafford, 2004]) that is part of a digital crime scene. More specifically, the main property of cryptographic keys in the context of digital forensics is that they may be a necessary prerequisite for the successful decryption of encrypted digital evidence.

Digital investigators are often forced to attempt brute-force and dictionary attacks to gain access to encrypted digital evidence, but these methods cannot circumvent strong cryptography and strong passwords. A paradox is that

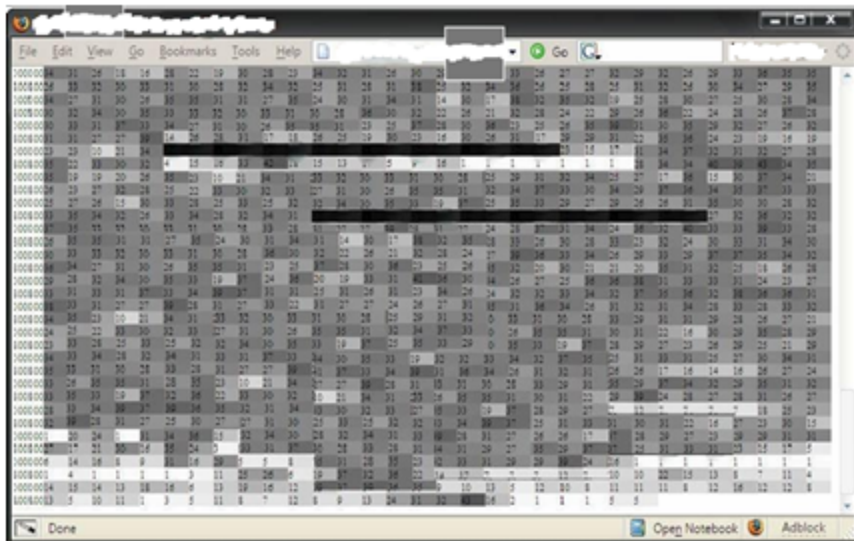
---

\* Corresponding author.  
E-mail addresses: [carsten@kssn.no](mailto:carsten@kssn.no) (C. Maartmann-Moe), [stefan.thorkildsen@police.no](mailto:stefan.thorkildsen@police.no) (S.E. Thorkildsen), [andre.arnes@sig.no](mailto:andre.arnes@sig.no) (A. Arnes).

<sup>1</sup> Carsten Maartmann-Moe is currently a Consultant at Ernst & Young in Norway.  
<sup>2</sup> André Arnes is currently an Adjunct Associate Professor at Qvæk University College and a Security and Identity Management Architect at Oracle Norway.  
1742-2876/\$ – see front matter © 2009 Digital Forensic Research Workshop. Published by Elsevier Ltd. All rights reserved.  
doi:10.1016/j.din.2009.06.002

# Real world key extraction by entropy

- Here is a memory readout of the flash memory
- Simply de-soldered and placed in a socket
- Then they measure entropy ("randomness")
- Keys found





# Key storage in hardware

- Typical in industrial crypto applications.
- Separate key store devices (smart cards, SIM cards, HSMs) or components (chipsets, TPMs)
- Wide use of key hierarchies, with master key in hardware («hardware root-of-trust»)
  - Required in certain applications, like [MovieLabs' ECP requirements](#) adopted by Hollywood studios for 4K content
  - Your PC most likely has a TPM chip, for use with software like e.g. Microsoft Bitlocker

# The key problems

- Key storage
- Key usage
- Key distribution

# Key usage

- Secure key storage is necessary but not sufficient
- Example [Adobe case](#):
  - Adobe put their master key in a HSM. Master key = private key to root code signer certificate
  - Hackers gained access to the server hosting the HSM and signed their own certificates
  - Using these certificates, hackers could deploy malware with valid cryptographic signature passing as authentic Adobe software.
  - The cryptography was designed to stop exactly this attack. How could it happen?
  - Maybe some bad guy violated the threat-model...

Adobe revokes certificate after hackers compromise server, sign malware

28 SEP 2012

Adobe, Security threats, SophosLabs, Vulnerability



## HACKERS BREACHED ADOBE SERVER IN ORDER TO SIGN THEIR MALWARE



A door at Adobe's building in San Francisco. Credit: [Photoburst/Flickr](#)

SHARE

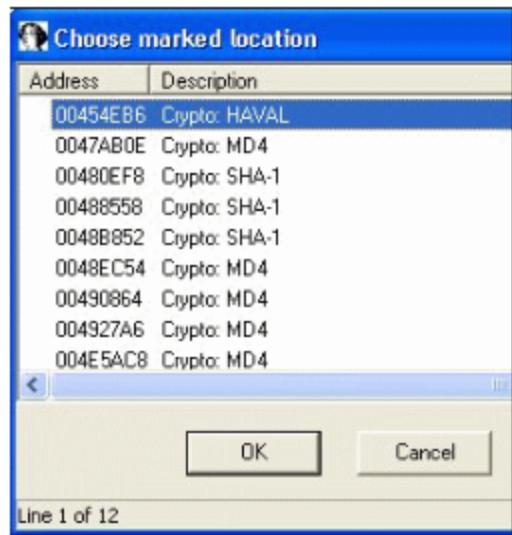


THE ONGOING SECURITY saga involving digital certificates got a new and disturbing wrinkle on Thursday when software giant Adobe announced that attackers breached its code-signing system and used it to sign their malware with a valid digital certificate from Adobe.

Adobe said the attackers signed at least two malicious utility

# Real world key extraction from software

- Use IDA to reverse engineer the software
- Use “FindCrypt” plug-in to identify the algorithm location
- Set break points at this location
- Run the encryption/decryption software
- Extract crypto keys from memory dump



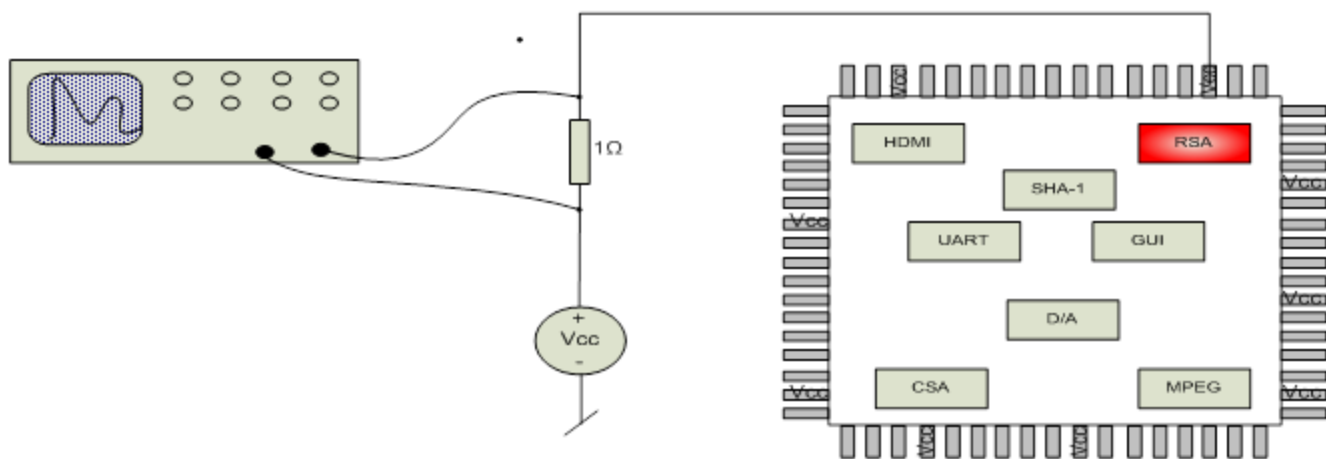
```
Using PEIM_Signature: Microsoft Visual C++ 6.0...
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
40CB08: Found const array Rijndael_Te0 (used in Rijndael)
40CF08: Found const array Rijndael_Te1 (used in Rijndael)
40D308: Found const array Rijndael_Te2 (used in Rijndael)
40D708: Found const array Rijndael_Te3 (used in Rijndael)
40DB08: Found const array Rijndael_Td0 (used in Rijndael)
40DF08: Found const array Rijndael_Td1 (used in Rijndael)
40E308: Found const array Rijndael_Td2 (used in Rijndael)
40E708: Found const array Rijndael_Td3 (used in Rijndael)
```

# Side channel attacks

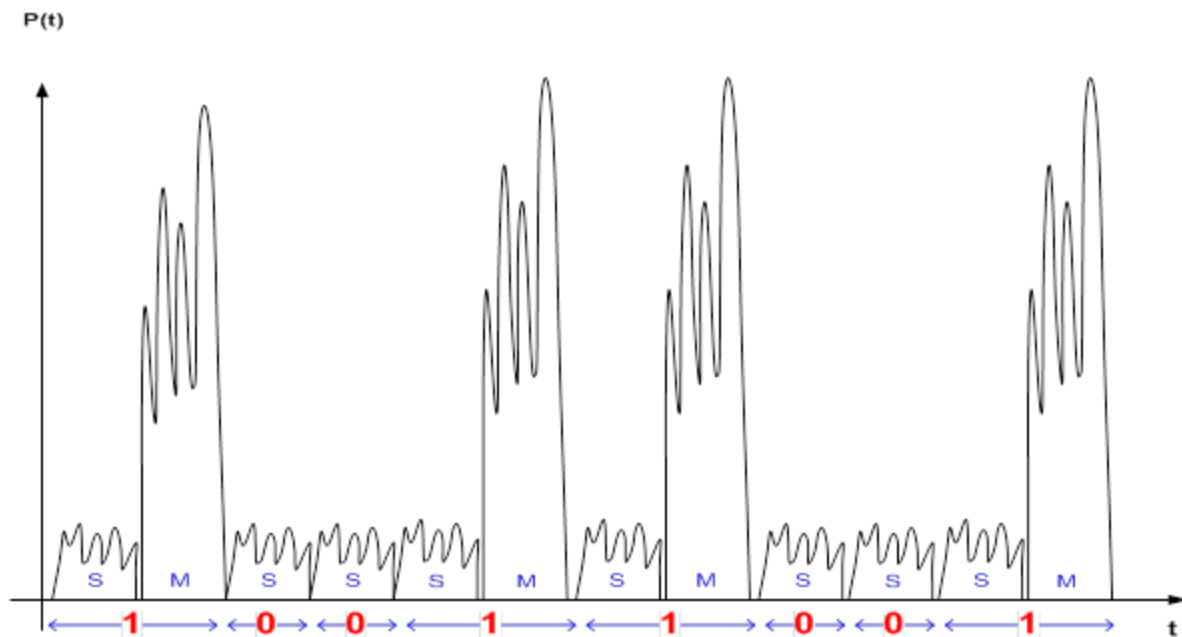
- All key usage pose a threat to the confidentiality of the key
- The processing **will** leak parts of the key, in a strict information theoretical sense, to observable metrics:
  - Power consumption
  - CPU usage
  - EM radiation
  - Heat
  - Response time
  - Etc.

# Example SPA on RSA

- SPA = Simple Power Analysis



# Simple Power Analysis of RSA



# Software fault injection

- The algorithmic implementation may expose logical vulnerabilities that can be exploited (sometimes combined with SCA)
  - E.g. malformed data, buffer overflows etc.
- The cryptographic algorithm in it self may be vulnerable
  - E.g. [plain RSA](#) (without padding) vulnerable to a number of attacks, like simple Chosen Cipher Text Attack.



# Hardware fault injection

- Introducing fault conditions and observing the erroneous output by varying e.g.
  - Supply voltage (generate a spike)
  - Clock frequency (glitching attack)
  - Temperature
  - Expose to intense light (camera flash or laser)

# Example of real life HSM

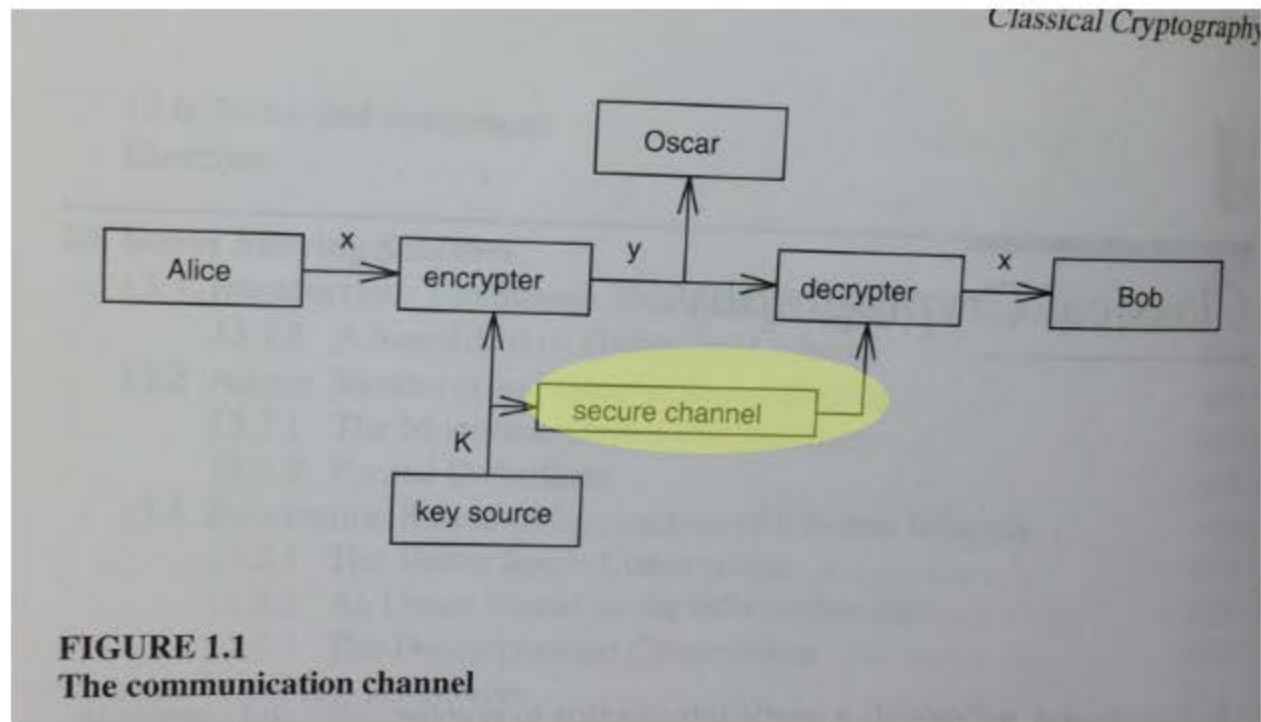
- ◆ Outer metal case
- ◆ Potting material
- ◆ Sensors foil
- ◆ Inner metal case
- ◆ CS circuit board



# The key problems

- Key storage
- Key usage
- Key distribution

# Seen this before?

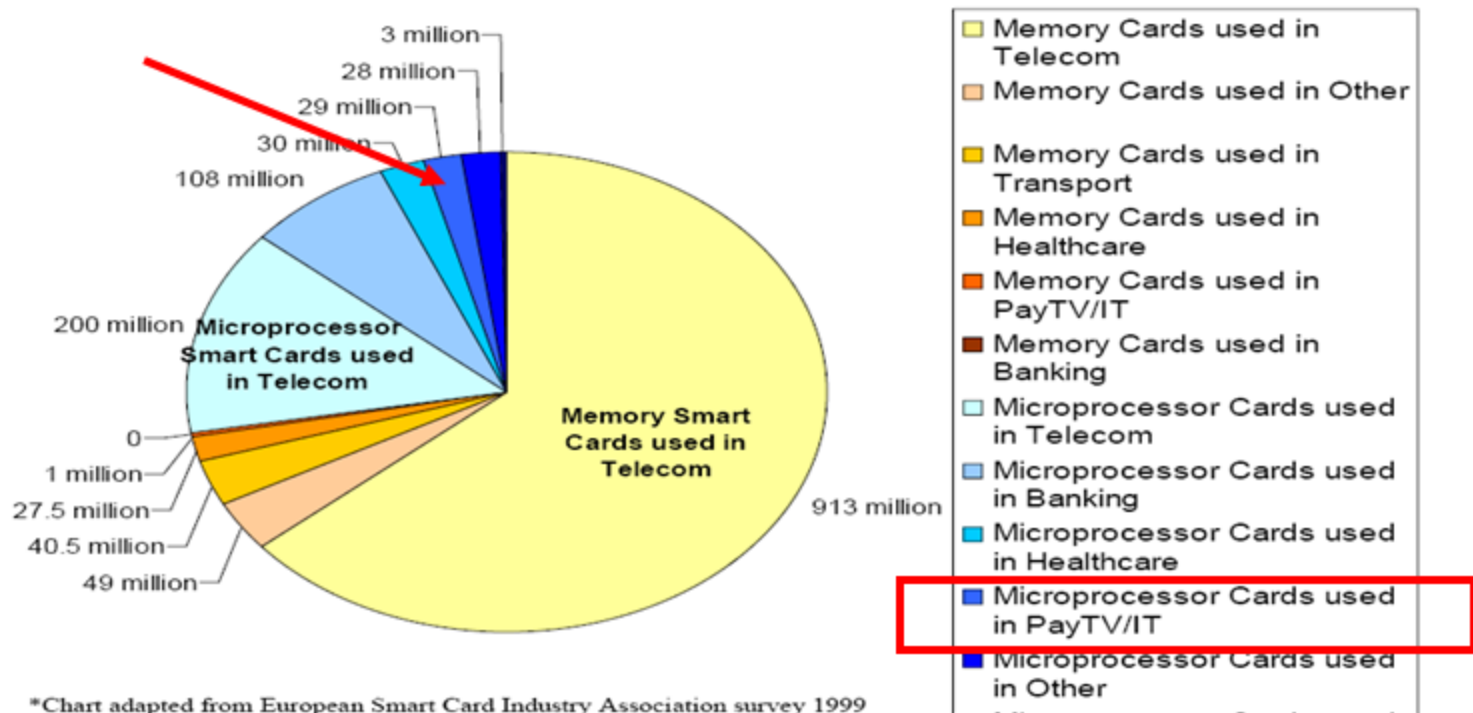


# Secure channel

- Really secure channels are hard to come by
- Those that exist doesn't scale well enough for industrial applications
- PKI was supposed to change all this, but alas, you still need secure provisioning...
- As it turns out, putting keys in a physical secure container (e.g. smart card) and shipping is still one of the most cost-efficient secure key distribution methods.

# Smart card world view

- Security driven by Pay-TV

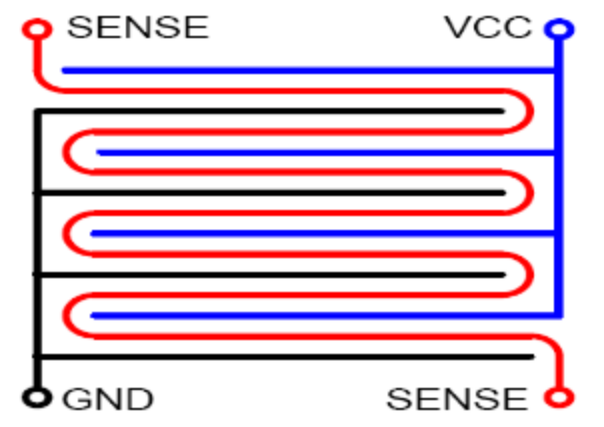


# SC threats – 3 categories

- **Invasive attacks** will destroy the chip
  - Micro probing
  - Metal layer changes (Laser / FIB)
  - Reverse engineering
- **Semi-invasive attacks** go outside the specs
  - Fault injections
  - Glitching
  - Freezing
- **Non-invasive attacks** observe chip operations within the specifications
  - Logical errors
  - Side channels

# Shielding

- Counter measure against invasive and semi-invasive attacks
- Cover surface with signal conductors. Detection if signal is broken.





# Other SC counter measures

- Sensors
  - Voltage
  - Light
  - Temperature
- Dual logic
- CPU separation
- Anti-SCA algorithms

# Security assurance

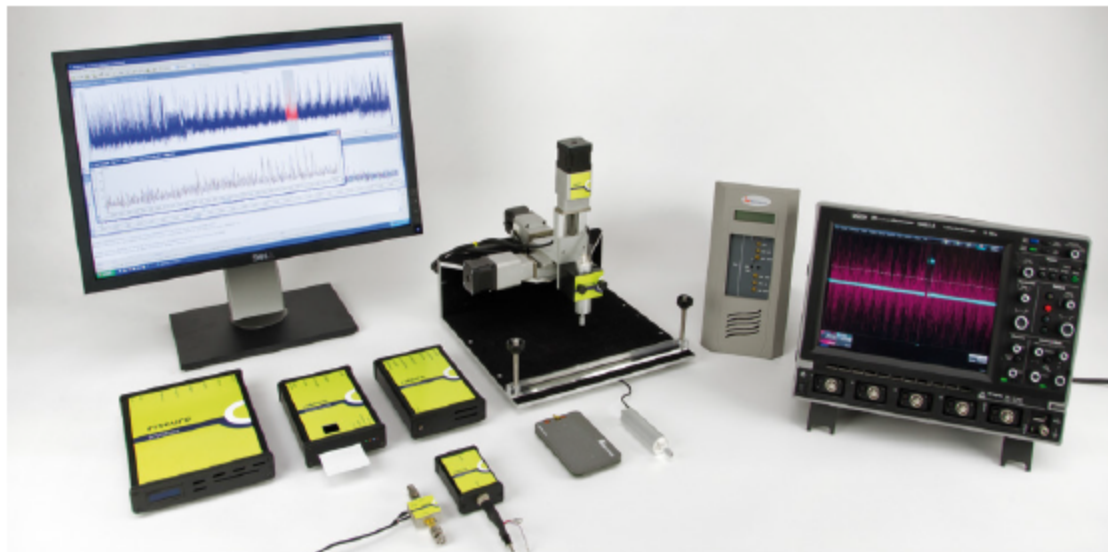
Penetration tests ~ Cryptographic strength  
Cryptanalysis ~ algorithmic strength

- Conax STBs are made by 3rd party companies under license from Conax
- Strict certification and evaluation scheme
- Every design go through a penetration test.

# Automated test tools exist

## From brochure:

- *“Inspector is an advanced integrated tool for side channel analysis and fault injection.”*
- *“Inspector excels in time-efficient analysis and perturbation of evaluation targets with the latest attack techniques and methods.”*



# Security evaluation snapshots

- Removed from publication as informed during presentation

# Claim #1

- Cryptographic strength in industrial applications is limited by its key management system
- **The problem with least amount of usable literature**
- **The «hard» part that is omitted from DVB standardization**
- **The part in crypto that scales poorly**

# Claim #2

- Cryptographic strength cannot be assessed independent of its physical implementation
- **Many key extraction techniques and tools (like “FindCrypt”) are dependent on certain implementations details**
- **Physical attacks can mitigated by mathematical transformation (e.g. use of Edwards curves in ECC)**

# Claim #3

- Cryptographic strength in industrial applications is best measured by penetration tests.
- **Based on the fact that our penetration tests discover and repair many vulnerabilities, despite standardized algorithms and protocols.**

# Thank you

Any MORE questions?

Anders . Paulshus -at- Conax . com