



## Identity, Implementation Security, and the Future

---

[www.cryptography.com](http://www.cryptography.com)  
575 Market St., 11<sup>th</sup> Floor, San Francisco, CA 94105

© 2012 Cryptography Research, Inc. Protected under issued and/or pending US and/or international patents. All trademarks are the property of their respective owners. The information contained in this presentation is provided for illustrative purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of CRI or its partners. Unauthorized copying, use or redistribution is prohibited.

Cryptography Research: Leader In Advanced Cryptosystems™

1



## Who am I?

---

- CTO at Cryptography Research
  - Security research & engineering firm
  - Focused on hard real-world cryptography and hardware security problems
  - In 2011, >5 billion devices shipped with our technologies



Cryptography Research: Leader In Advanced Cryptosystems™

2

## Examples of designs & technologies

---

- DPA countermeasures technology & patents
  - >5B devices: smart cards, ID chips, DRM systems, firmware loaders...
- CryptoFirewall™: Tamper-resistant hardware core
  - Used to stop product counterfeiting, pay TV piracy
- BD+: Renewable security for optical disc formats
  - Part of the Blu-ray disc format [tech. sold to Macrovision]
- SSL3/TLS: Secure web browser connection protocol

## A History of Authentication

## Command authorizations

- Egyptian signet ring
  - Used by pharaohs & officials
  - ~500BC



- Mark of the fisherman
  - Individualized for each pope
  - On death, Cardinal Carmerlengo to locate ring & destroy seal
  - Earliest note in 1265



Images courtesy British Museum, flickr:favoritethings

## Command authorizations



US nuclear "football"  
(also: UK Letters of Last Resort)



Starfleet auto-destruct  
procedure

## Identification papers

The Roman citizen was required to register the birth of his children within thirty days before a Roman official, and **he received a wooden diptych recording the declaration, which acted as a certificate of citizenship for the child** for the rest of his life.



Roman diptych

Like the military *diplomata* this contained the names of **seven witnesses**, and provided a presumptive proof of citizen status. ...complete validation of a claim [required confirmation against] the official archive

*Sherwin-White, The Roman Citizenship, 316.*



US CAC

Image courtesy Princeton University

## Symmetric ciphers (1900's)



WW2 Enigma machine

**Standard cipher, secret key.**

...but Enigma broken due to:

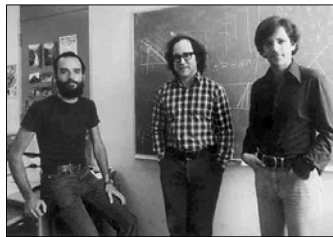
- Operational weaknesses
  - Operator session key re-use
- Bad keylength (brute force)
  - British 3-rotor bombe
  - US 4-rotor bombe
- Cryptanalysis
  - Bletchley park enlisted crossword puzzle experts

## Asymmetric crypto (1970's)



**Public key crypto simplifies key management and enables digital signatures.**

- Diffie-Hellman key exchange (1976)
- RSA algorithm (1977)
- Elliptic curve cryptography



Stanford News Service


## Authentication properties

- Authenticity
- Integrity
- Availability
- Non-repudiation
- Confidentiality



# Tamper Resistance

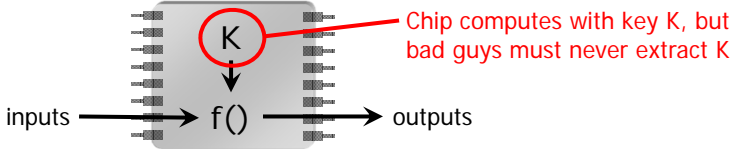
Cryptography Research: Leader In Advanced Cryptosystems™ 11



CRYPTOGRAPHY  
RESEARCH  
a division of Rambus

## Tamper resistance

- Security chips must protect their secret keys



Chip computes with key K, but bad guys must never extract K

- Critical building block for many applications

- Payments
- Identity
- Anti-counterfeiting
- Anti-piracy
- Communications
- (and more)

Cryptography Research: Leader In Advanced Cryptosystems™ 12

## Brute force attacks



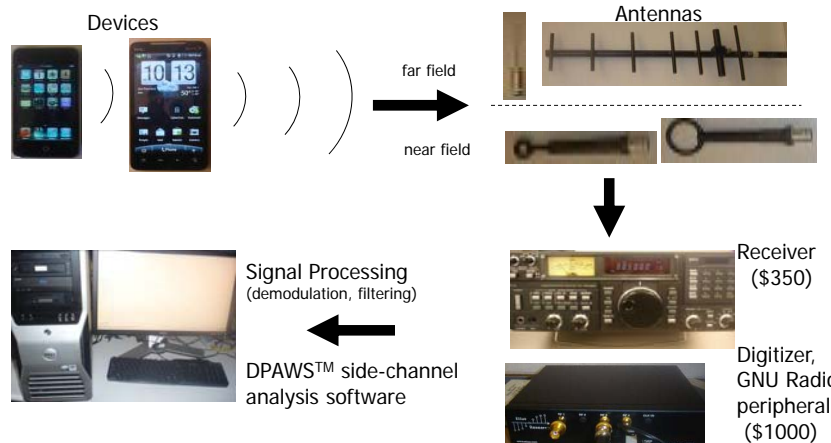
**US Navy Bombe, 1943**  
Contains 16 four-rotor Enigma equivalents to perform exhaustive key search.



**DES Keysearch Machine, 1998**  
(Cryptography Research, AWT, EFF)  
Tests 90+ billion keys per second, exhaustively searches 56-bit DES keyspace in 9 days.

## Side channel attacks

- Simple EM attack with a radio
- Usable signals even at 10 feet away

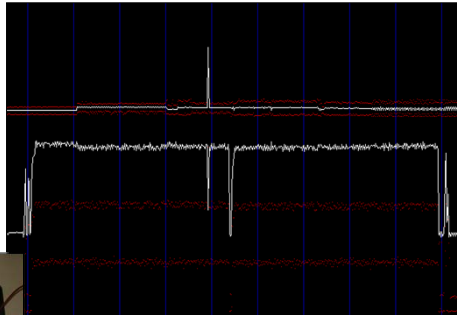
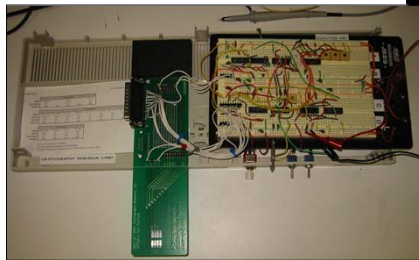






## Inducing defective computations

- Electrical glitch
- Temperature
- Laser light

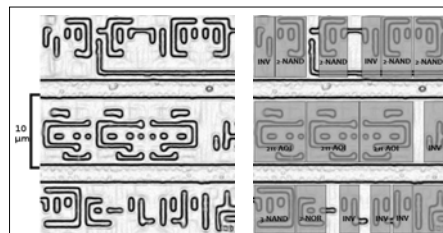


## Invasive extraction of secrets

- Extract keys, algorithms
- Optical microscopes, focused ion beam
- Algorithm reconstruction via imaging attack



FEI V400ACE Focused Ion Beam



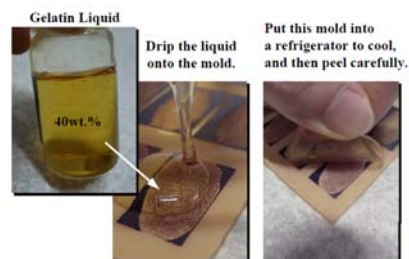
Reconstructed standard cells from optical microscope image

Nohl, Evans, Starbug, Henryk Plotz, Reverse-Engineering a Cryptographic RFID Tag, USENIX 2008

If an adversary recovers an identity device...

## Study device state

- Recover user state
  - Make gelatin finger from print
  - PIN button residue
- "Freeze" digital state
  - Low power mode
  - DRAM and cold spray



Lest We Remember: Cold Boot Attacks on Encryption Keys, J. Alex Halderman Et Al, 2008 USENIX Security Symposium  
Impact of artificial "gummy" fingers on fingerprint systems, Matsumoto Et Al, Optical Security and Counterfeit Deterrence Techniques IV

## Monitor a session

- Observation techniques
  - RF measurements
  - Log I/O
  - Watch pin pad
  
- Go where sessions happen
  - E-commerce point
  
- Force a session
  - Generate crypto event
  - Force re-authentication
  - Send email to user



**Bus analyzer**



**Antenna & radio receiver**

## Extract info from unsuspecting user

### Fake authentication station



**Fake ATM**  
Riveria Hotel, Las Vegas  
2009

### I/O relay to credential



**Contactless passport relay  
with mobile phone**  
2011

Practical relay attack on contactless technologies by using NFC mobile phones, IACR eprint 618, 2011

How do I use my Trust Anchor?  
or...  
Do Command & Control Approaches Still Work?



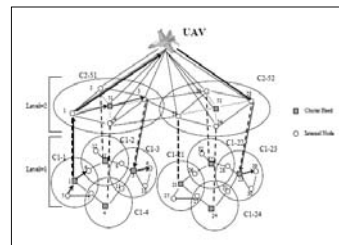
## Ad-hoc resource sharing

- Decentralized access control decisions
- Cross-agency collaboration
- Fluid working groups with role-based membership




### Challenges:

- Key management and revocation
- Access first, accountability later
- As vulnerable as weakest node?



UAV Intelligent Wireless Network Routing



CRYPTOGRAPHY  
RESEARCH  
a division of Rambus


## Convergence of IT & physical security

---

*Two different (and complementary) mindsets*

IT security	Physical security
Service oriented	Containment oriented
Interoperability focus	Proprietary
Role-based permissions	Inflexible permissions
Porous boundaries	Rigid security boundary
Single point of failure	2-person controls
"Best-effort" logs	Robust audit records

Cryptography Research: Leader In Advanced Cryptosystems™
25



CRYPTOGRAPHY  
RESEARCH  
a division of Rambus

## Cloud computing / mesh networking (1/2)

- Shared, dynamically re-allocated resource
- Varying degrees of node/process cooperation
- Examples:
  - Inter-agency hosting
  - Peer-to-peer network connections

**Hey, You, Get Off of My Cloud:  
Exploring Information Leakage in  
Third-Party Compute Clouds**

Thomas Ristenpart\* Eran Tromer† Hovav Shacham\* Stefan Savage\*

\*Dept. of Computer Science and Engineering  
University of California, San Diego, USA  
{tristenp,hovav,savage}@cs.ucsd.edu

†Computer Science and Artificial Intelligence Laboratory  
Massachusetts Institute of Technology, Cambridge, USA  
tromer@csail.mit.edu

**ABSTRACT**


Third-party cloud computing represents the promise of outsourcing as applied to computation. Services, such as Microsoft's Azure and Amazon's EC2, allow users to instantiate virtual machines (VMs) on demand and thus purchase precisely the capacity they require when they require it. In turn, the use of virtualization allows third-party cloud computing and software capabilities are outsourced on demand to shared third-party infrastructure. While this model, exemplified by Amazon's Elastic Compute Cloud (EC2) [5], Microsoft's Azure Service Platform [26], and RackSpace's Mosso [27] provides a number of advantages—including economies of scale, dynamic provisioning, and low capital expenditures—it also introduces a range of new risks.

Cry
m s™
26

## Cloud computing / mesh networking (2/2)

- Risks from compromised actors
  - Resource degradation
  - Data extraction
  - System compromise
  
- Implementation challenges
  - NPE credential management
  - Redundant partitioning approaches (crypto)
  - Key management by proxy (HSMs)

## BYOD

- Personal IT equipment
  - Less controlled (and less secure)
- 
- Risk management in commercial identity systems
    - Use multiple identifying elements
    - Offers secondary communications channel
    - Use as token

- BYOD risk vs. supply chain risk?
- Risk scoring tool or gatekeeping technology?
- Threat vector or authenticable digital personality?




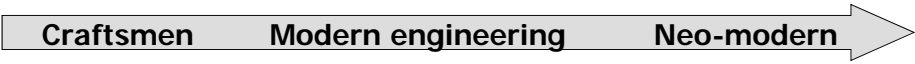
# Conclusion

Cryptography Research: Leader In Advanced Cryptosystems™ 29

CRYPTOGRAPHY RESEARCH  
a division of Rambus

## Challenges in Identity Management

Craftsmen      Modern engineering      Neo-modern



*White House situation room, 1967*

<b>unique token</b>	<b>modern ciphers</b>	<b>dynamic boundaries</b>
<b>recordkeeping</b>	<b>binding ID to person</b>	<b>tamper resistance</b>
	<b>two-factor</b>	<b>task-based auth.</b>

Cryptography Research: Leader In Advanced Cryptosystems™ 30

## Contact Information

Benjamin Jun  
ben@cryptography.com  
415.397.0123  
**www.cryptography.com**

© 1998-2012 Cryptography Research, Inc. Protected under issued and/or pending US and/or international patents. All trademarks are the property of their respective owners. The information contained in this presentation is provided for illustrative purposes only, and is provided without any guarantee or warranty whatsoever, and does not necessarily represent official opinions of CRI or its partners. Unauthorized copying, use or redistribution is prohibited.