CS915/435 Advanced Computer Security - Hardware Security

HSM

Outline

- Introduction
- Hardware Security Module
  - How to attack crypto processors?
- Smart cards and Microcontrollers
  - How to attack smart cards?

Introduction

- Security is all about trust, but where does trust come from?
- What’s a trusted third party?
  - By definition, a trusted third party is someone who can break your security policy
  - A completely trustworthy third party doesn’t exist.
- Common sources of trust
  - Number theory: e.g., factorization, discrete log
  - Tamper resistance: basis for trusted computing

Tamper Evident vs Tamper Resistant

- Tamper evident -- **detectable** upon tamper
- Tamper resistant - **robust** against tamper

Hardware Security Module

- Main functions
  - Onboard secure generation
  - Onboard secure storage
  - Use of cryptographic and sensitive data
  - Offloading application servers for crypto operations
- Secure erasure of secret data upon tamper
- Disaster recovery with smart cards

How to hack a cryptoprocessor (1) - Master key

- Attack on master key
- In early banking system, the master key was stored in a Programmable ROM (PROM)
- But content of PROM can be easily read
- <u>Solution was shared control</u>: two or three PROMs were combined to derive master key.
- How the cryptoprocessor was maintained?
    1. Custodians open lid and erase live keys before engineers open the HSM.
    2. Maintenance engineers load test keys for diagnosis or repairs
    3. Custodians re-load live keys, but in practice they just handed keys over to engineers
- What are the problems with the above approach?

How to hack a cryptoprocessor (2) - Casing

- Early devices were vulnerable to attackers cutting through the casing
- Lid switch added to provide tamper evidence
- But the hard problem is to prevent attacks by maintenance staff
- Modern products separate components that need to be serviced (e.g., batteries) from core (tamper sensor, cryptoprocessor, memory)
- Core components potted in epoxy

How to hack a cryptoprocess (3) - epoxy

- Potting the device is not perfect
- One may scrape away the potting with a knife
- Use a probe to tab the bus lines in the core
- Data on the bus lines usually unencrypted
- Solution: tamper-sensing membrane whose penetration will trigger destruction of the secrets inside.

How to hack a cryptoprocessor (4) - Memory remanence

- All computer memory retains some traces of data especially in low temperature
- Researchers from Princeton University did an experiment on DRAM in 2008
- See “Last We Remember: Cold Boot Attacks on Encryption Keys” at Usenix’08
- http://www.youtube.com/watch?v=JDaicPIgn9U&feature=relmfu
- In fact, memory remanence reported earlier by Skorogatov in 2002 PhD thesis (Cambridge)

How to hack a cryptoprocessor (5) - Frozen memory

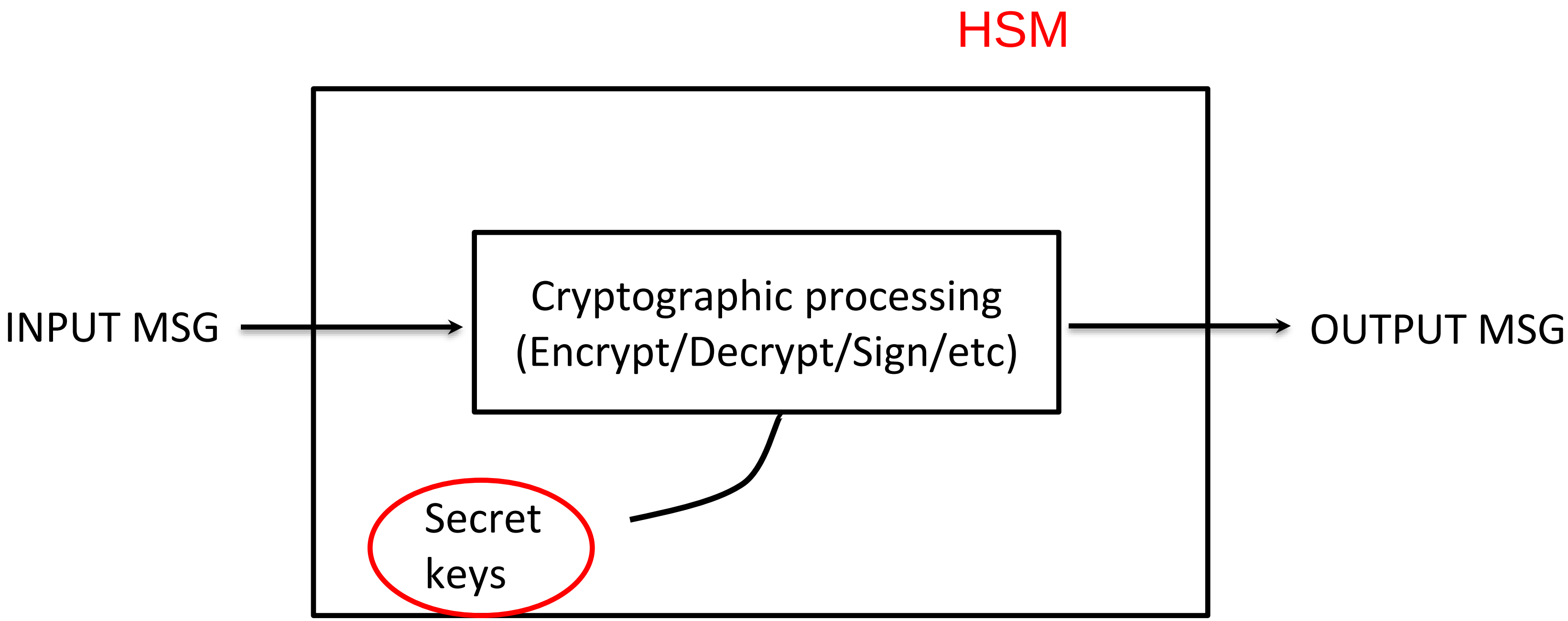
- RAM content can be “frozen” below -20 C for a few seconds to several minutes
- An attack may break the tamper resistance
  - Freeze a device
  - Remove the power
  - Cut through membrane
  - Take random chips
  - Power up and extract keys

- Using thermite charge can ensure secure erasure of secret data

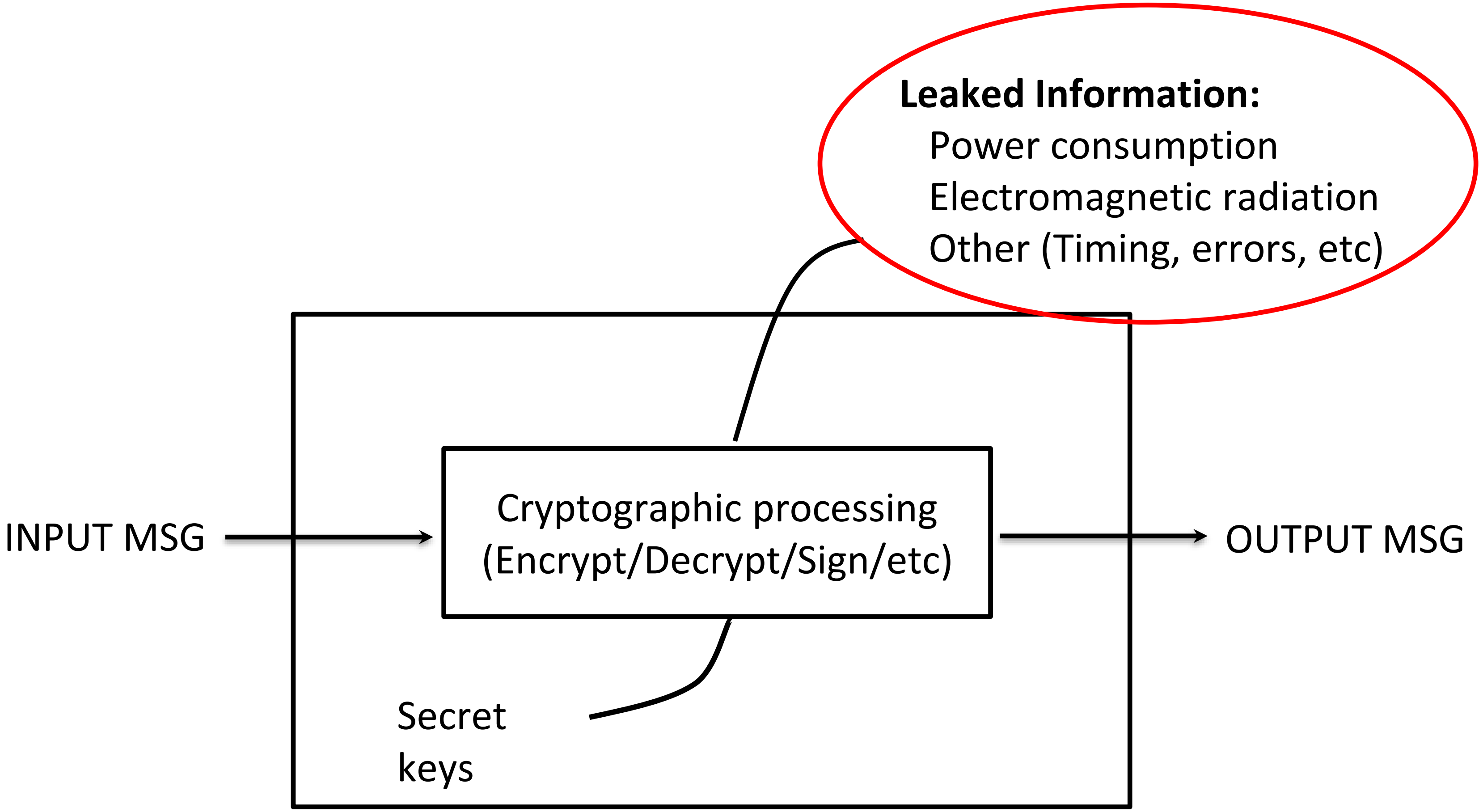
How to hack a cryptoprocessor (6) - Side channel attacks

- Monitor the RF, power, timing to deduce secret keys
- RF analysis
- Timing analysis
- Power analysis
- Optical, acoustic and thermal side channels

Traditional Cryptographic Assumptions



Actual Information Available

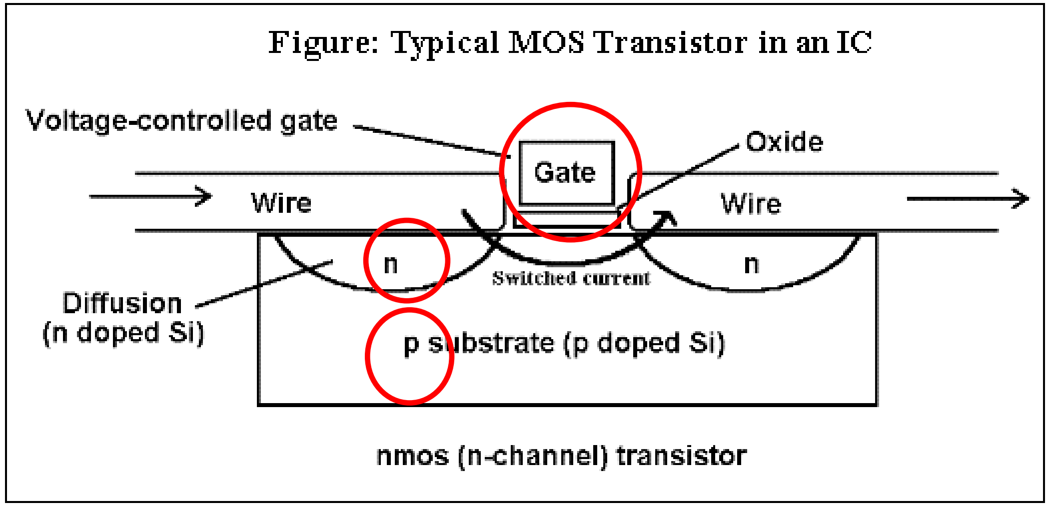


What’s wrong with the code?

```
boolean comparePassword (char [] pwdInput, char[] pwdSecret){
	if (pwdInput.length != pwdSecret.length){
		return false;
	} else {
		for (int i = 0; i < pwdInput.length; i++) {
			if (pwdInput [i] != pwdSecret [i]) {
				return false;
			}
		return true;
	}
```

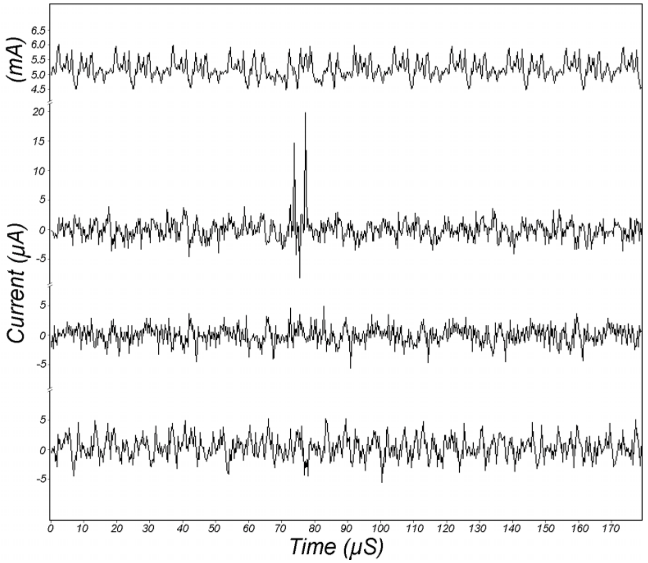
Power Variation

- Integrated circuits are built out of individual transistors, which are voltage-controlled.
- The motion of electric charge consumes power and produces electromagnetic radiation – which follows predictable patterns



Power analysis

- Simple Power Analysis (SPA): directly interpreting power consumption measurements
- Differential Power Analysis (DPA): examining the difference between power traces



DPA traces, one correct and two incorrect, with power reference

- See Paul Kocher et al. "Introduction to Differential Power Analysis and Related Attacks", 1998.

Example of power analysis

- How to compute g^x mod p where x is w bits?
  - Convert x to w bits
  - Repeated squaring either from left or from right
  - For example, 2^{133} mod 11?

2^{133} mod 11 = $2^{128+4+1}$ mod 11

$2 \quad 2^2 \quad 2^4 \quad 2^8 \quad 2^{16} \quad 2^{32} \quad 2^{64} \quad 2^{128}$

Multiply 2, 2^4 , and 2^{128}

res = 1; base = 2;

res’ = 1

for i = 0...w-1

if x[i] = 1

*res = res * base*

else { *base = base * base*

res’ = res’ * base }

return res

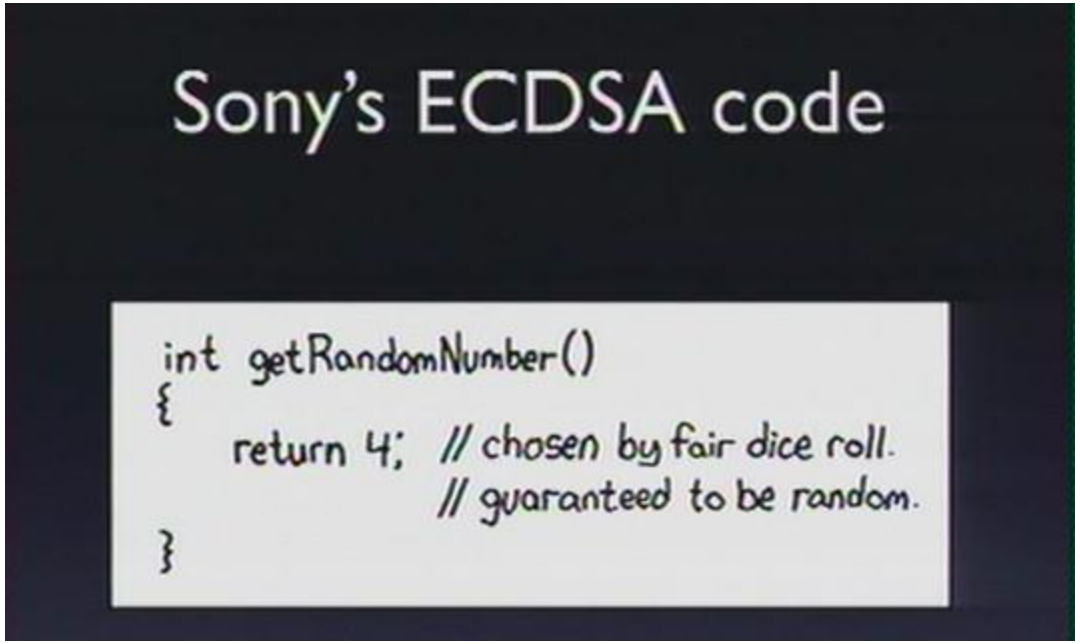
How to hack a cryptoprocessor (7) - logic interface

- Most effective attacks on Hardware Security Modules are logical rather than physical
- Known as API attacks (will detail in the next lecture)

How to hack a cryptoprocessor (8) - implementation error

- Many of the security failures are due to implementation errors
- 2010, hackers extracted PS3 private key from the “tamper-resistant” hardware.
- The attack exploited a fatal error in the implementation of ECDSA signing algorithm by Sony.

What went wrong?



Why it worked

- We use DSA to illustrate (ECDSA is very similar to DSA)

  To sign a message m using DSA Private key x

  - Select a random k in [0, q-1] **(changed to fixed k)**
  - Calculate r = (g^k mod p) mod q
  - Calculate s = (k^{-1}(H(m) + x r) mod q
  - The signature is {r, s}

$$s = (k^{-1}(H(m_1) + x\, r) \bmod q$$

$$s = (k^{-1}(H(m_2) + x\, r) \bmod q$$

$$s = (k^{-1}(H(m_3) + x\, r) \bmod q$$

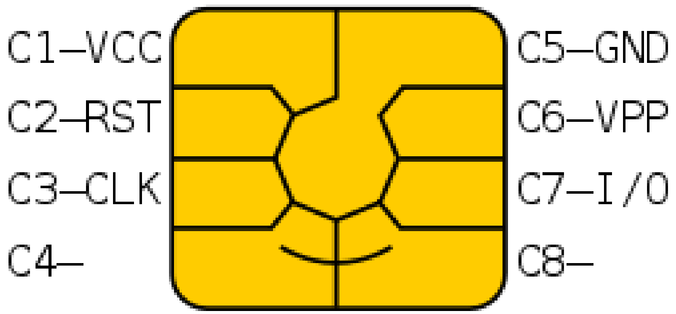
Outline

- Introduction
- Hardware Security Module
  - How to attack crypto processors?
- **Smart cards and Microcontrollers**
  - How to attack smart cards?
- API attacks

Smartcards and Microcontrollers

- Smartcards are often called chip cards or IC cards.
- Early smart cards were memory cards
  - Contain a memory chip
  - Cannot be reprogrammed
  - Discarded after use (good ice scraper though)
  - Not really smart
- Microprocessor card are much more secure
  - Contains a processor
  - Feature built-in cryptographic support
  - Can be programmed for multi-applications
  - Can be reprogrammed
  - “Smart cards” normally refer to microprocessor cards

Smart card Hardware



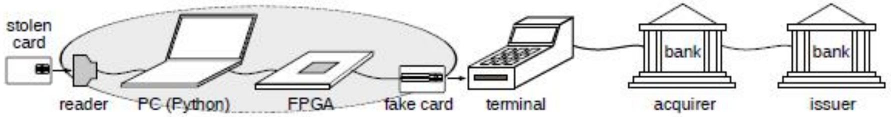
- Contact smartcard has eight contact points, standardized in ISO 7816
- Central processing Unit
  - 8 bit microcontroller
  - Clock 5 MHz
- Cryptographic coprocessor
  - Expediting modular calculations
- Memory system
  - ROM: burned during the *masking* process
  - EEPROM: persistent storage, 100,000 write cycles and data retention for 10 years. Reading is fast, but writing is 1000 slower than RAM.
  - RAM: temporary working space for storage/processing. It can be accessed an unlimited number of times.

Smart Card Communication

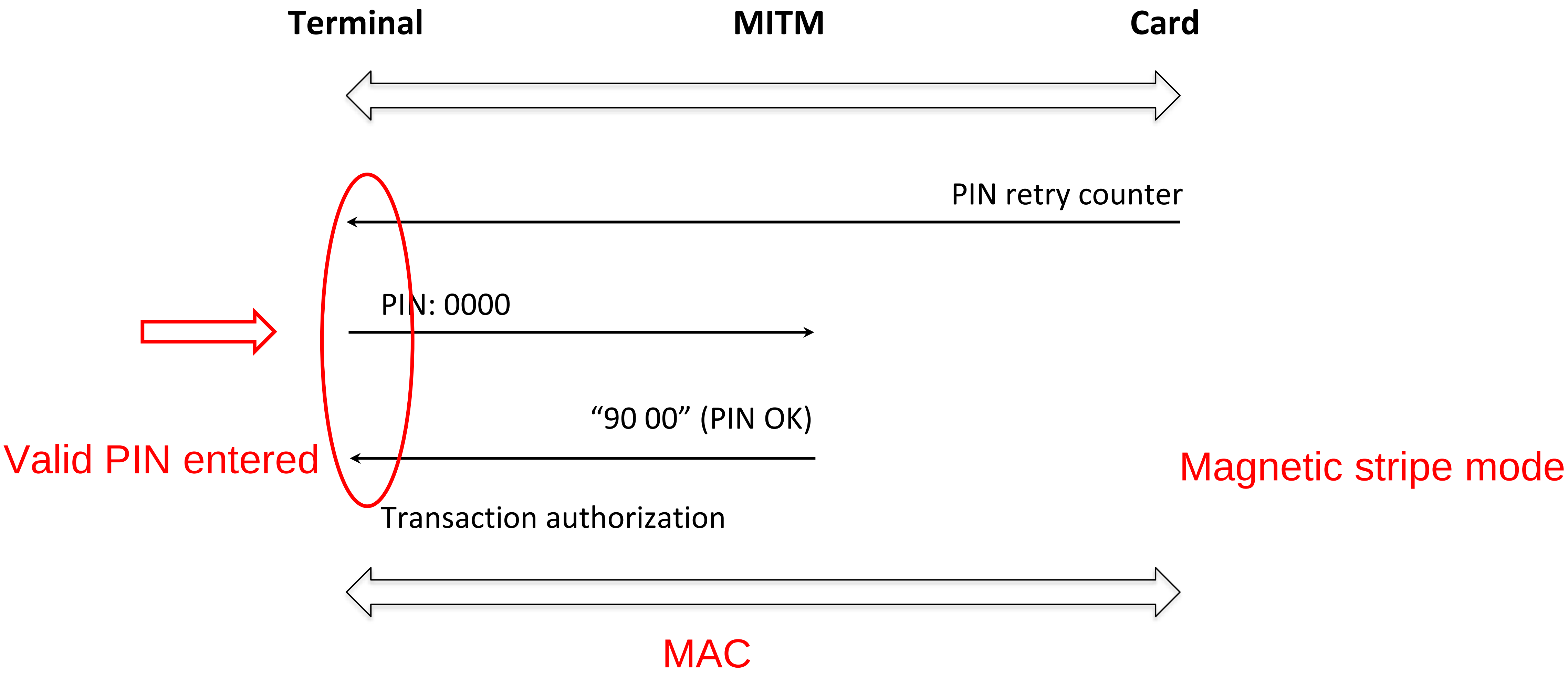
- Master-slave model
- A smart card always plays the passive slave
  - Host -> card: command APDU
  - Card -> Host: response APDU
- APDU protocol specified in ISO 7816-4

How to hack a smartcard
- exploit flaws in the protocol

- Physical attack: expensive and very difficult
- Logic attacks: often far more effective
- Cambridge No-PIN attack (Murdoch et al.’10)
- http://www.youtube.com/watch?v=3MD6WEGMmag (French)
- http://www.youtube.com/watch?v=OkMQHHfP_1E



What went wrong?



Best practice

- What you need to know when designing a system based on smartcards?
  - Use standard algorithms if possible
    - Security-by-obscurity should be abandoned
  - Extensive public scrutiny
    - Chip-and-Pin cards didn’t get public reviews
  - Defense in depth
    - Increase the attack efforts and time
  - Tamper resistance is hard to achieve
    - Need to be not only physically secure, but also logically secure
  - Stop loss
    - Don’t put all eggs in one basket!
    - Don’t load the same master key for all smart cards.