


Using Cryptography Well


Prof. Bart Preneel
COSIC
Bart.Preneel(at)esatDOTkuleuven.be
<http://homes.esat.kuleuven.be/~preneel>

© Bart Preneel. All rights reserved



Outline

- 1. Cryptology: protocols
 - identification/entity authentication
 - key establishment
- 2. Public Key Infrastructures
- 3. Secure Networking protocols
 - Internet Security: email, web, IPSEC, SSL
- 4. Using cryptography well
- 5. New developments in cryptography



Outline

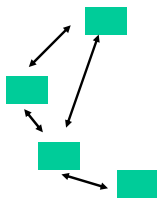
- Architecture
- Network protocols
- Security APIs
- Key establishment: protocols, generation, storage

Symmetric vs. Asymmetric Algorithms

• hardware costs: 5K–100K gates	• hardware costs: 100K–1M gates
• performance: 100 Mbit/s – 70 Gbit/s	• performance: 100 Kbit/s – 10 Mbit/s
• keys: 64-256 bits	• keys: 128-4096 bits
• blocks: 64-128 bits	• blocks: 128-4096 bits
• power consumption: 20-30 µJ/bit	• power consumption: 1000-2000 µJ/bit

Architectures (1a)

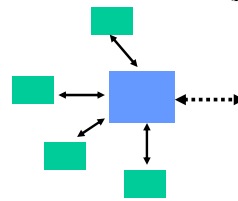
• Point to point	• Number of keys: 1 or n^2
• Local	• Manual keying
• Small scale	



Example: ad hoc PAN or WLAN

Architectures (2a)

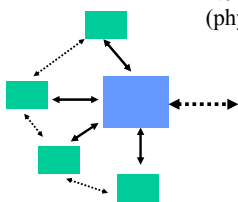
• Centralized	• Number of keys: n
• Small or large scale	• ! Central database: risk + big brother
• Manual keying	• Non-repudiation of origin? (physical assumptions)



Example: WLAN, e-banking, GSM

Architectures (3a)

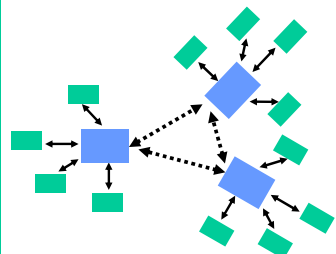
- Centralized
- Small or large scale
- Manual keying
- Number of keys: $n + 1/\text{session}$
- ! Central database: risk + big brother
- Non-repudiation of origin? (physical assumptions)



Example: LAN (Kerberos)

Architectures (4a)

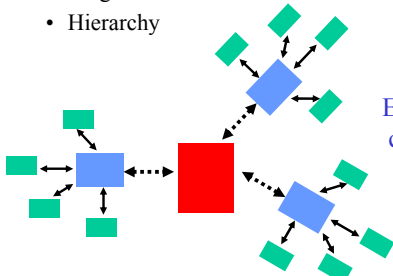
- Decentralized
- Large scale
- Number of keys: $n + N^2$
- Risks?
- Trust
- Hard to manage



Example: network of LANs, GSM

Architectures (5a)

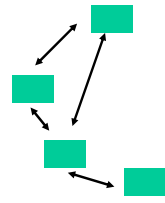
- Centralized
- Large scale
- Hierarchy
- Number of keys: $n + N$



Example: credit card and ATM

Architectures (1b)

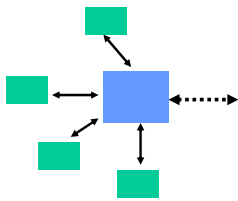
- Point to point
- Worldwide
- Small networks
- No CA (e.g. PGP)



Example: P2P, international organizations

Architectures (2b)

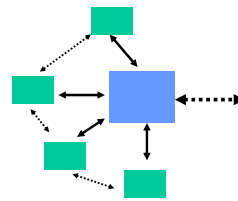
- Centralized
- Large or small scale
- Reduced risk
- Non-repudiation of origin



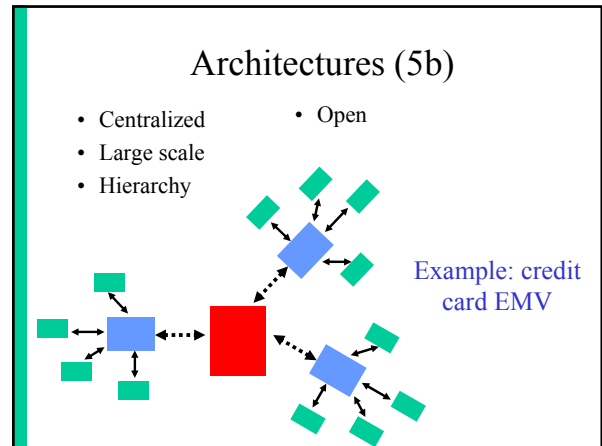
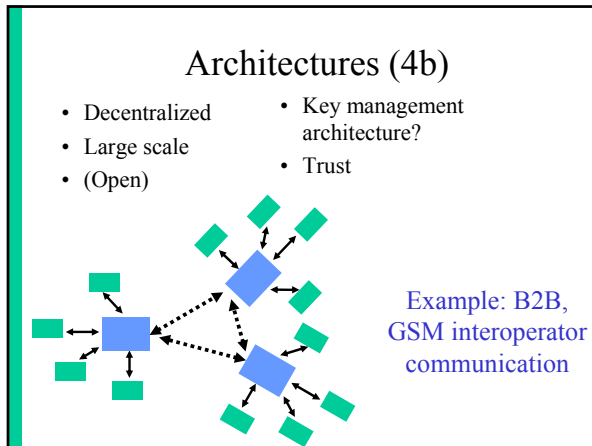
Example: B2C e-banking

Architectures (3b)

- Centralized
- Small or large scale
- Reduced risk
- Non-repudiation of origin



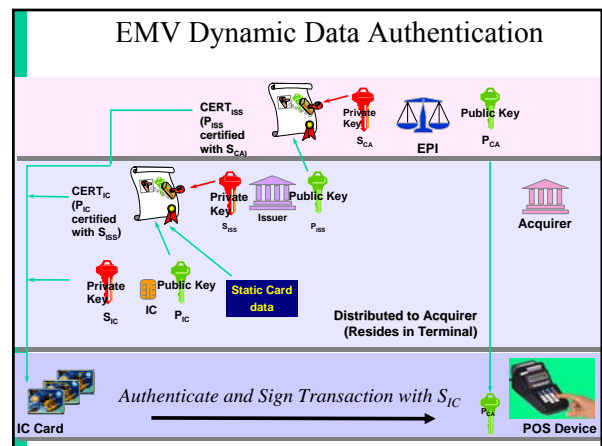
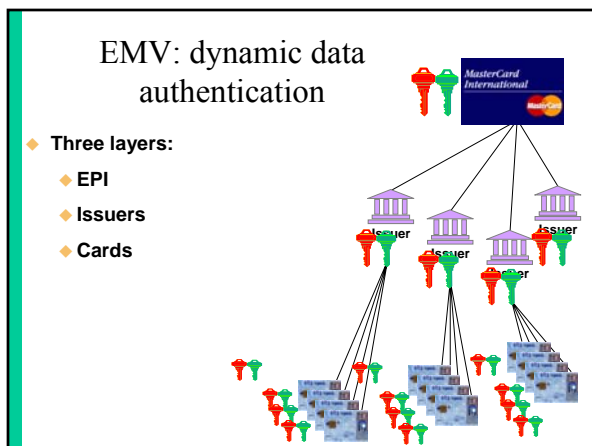
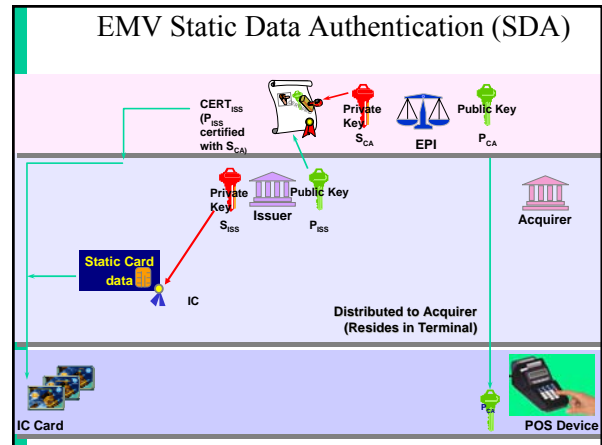
Example: B2B and e-ID

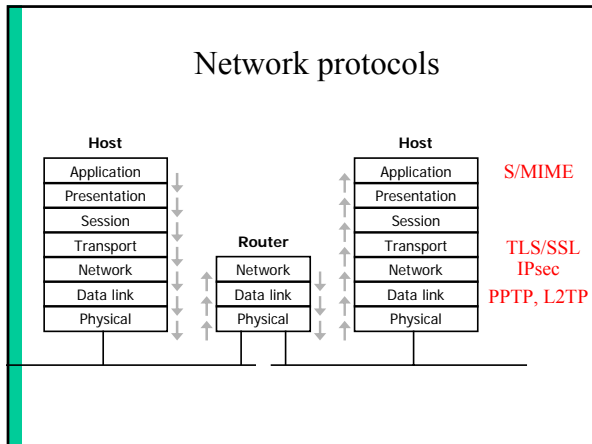


When asymmetric cryptography?

- if manual secret key installation not feasible (also in point-to-point)
- open networks (no prior customer relation or contract)
- get rid of risk of central key store
- mutually distrustful parties
 - strong non-repudiation of origin is needed
- fancy properties: e-voting

Important lesson: on-line trust relationships should reflect real-world trust relationships





Where to put security?

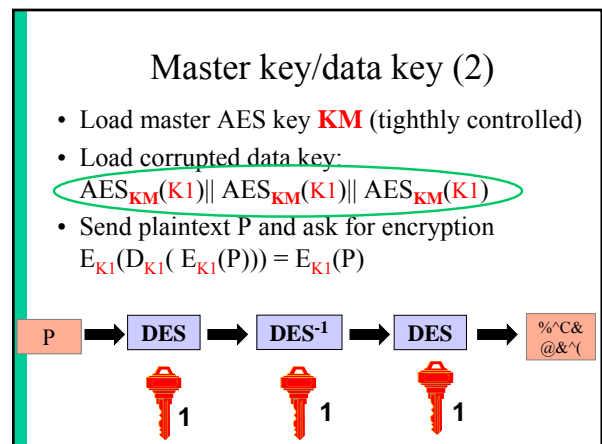
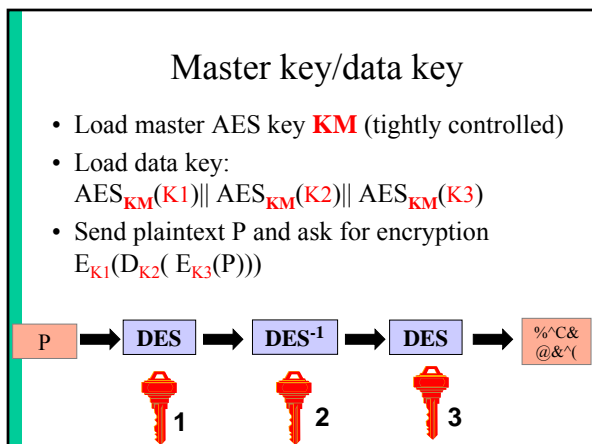
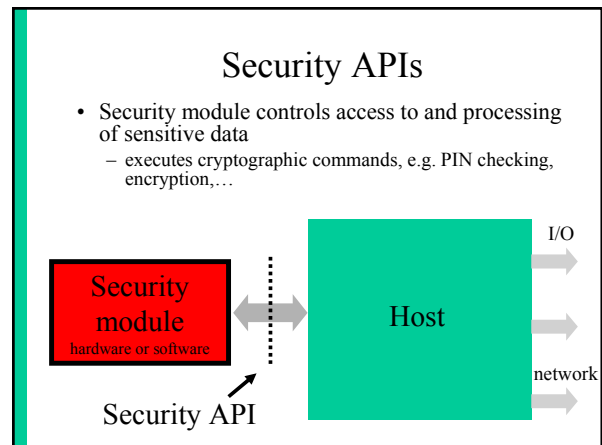
- Application layer:
 - closer to user
 - more sophisticated/granular controls
 - end-to-end
 - but what about firewalls?
- Lower layer:
 - application independent
 - hide traffic data
 - but vulnerable in middle points
- Combine?

Where to put security? (2)

From: Bob@crypto.com
 To: Alice@digicrime.com
 Subject: Re: Can you meet me on Monday at 3pm to resolve the price issue?

This proposal is acceptable for me.

-- Bob



Control vectors in the IBM 4758 (1)

- Potted in epoxy resin
 - Protective tamper-sensing membrane, chemically identical to potting compound
 - Detectors for temperature & X-Rays
 - “Tempest” shielding for RF emission
 - Low pass filters on power supply rails
 - Multi-stage “latching” boot sequence
- = **STATE OF THE ART PROTECTION!**

IBM 4758



Control vectors in the IBM 4758 (2)

- Control vector: *type* (e.g., PIN, data, MAC)
 $E_{K_m + \text{type}}(k), \text{type}$
- High security: triple control
 - Import K_m as $K_{m_A} + K_{m_B} + K_{m_C}$
- User C performs one correct and one fraudulent import by entering the 2nd time $K_{m_C} + \Delta$ with $\Delta = \text{type}_{\text{DATA}} + \text{type}_{\text{PIN}}$
- Result: $K_m^* = K_m + \Delta$

Control vectors in the IBM 4758 (3)

K_m : master key
 $K_m^* = K_m + \Delta = K_m + \text{type}_{\text{DATA}} + \text{type}_{\text{PIN}}$
or $K_m^* + \text{type}_{\text{DATA}} = K_m + \text{type}_{\text{PIN}}$
 k = PIN encrypting key

Normally: $D_{K_m + \text{type}_{\text{PIN}}}(E_{K_m + \text{type}_{\text{PIN}}}(k)) = k$
But attack: $D_{K_m^* + \text{type}_{\text{DATA}}}(E_{K_m + \text{type}_{\text{PIN}}}(k)) = k$



The system now believes that k is a key to decrypt data, which means that the result will be output (PINs are never output in the clear)

Security APIs

- Complex – 150 commands
 - Need to resist to insider frauds
 - Hard to design – can go wrong in many ways
- See: Mike Bond, Cambridge University
<http://www.cl.cam.ac.uk/users/mkb23/research.html>

Key management

- Key establishment protocols
- Key generation
- Key storage
- Key separation (cf. Security APIs)

Key establishment protocols: subtle flaws

- Meet-in-the middle attack
 - Lack of protected identifiers
- Reflection attack
- Triangle attack

Attack model: Needham and Schroeder [1978]:

We assume that the intruder can interpose a computer in all communication paths, and thus can alter or copy parts of messages, replay messages, or emit false material. While this may seem an extreme view, it is the only safe one when designing authentication protocols.

Meet-in-the middle attack on Diffie-Hellman

- Eve shares a key $k1$ with Alice and a key $k2$ with Bob
- Requires *active* attack

$k1 = (\alpha^{y1})^{x1} = (\alpha^{x1})^{y1}$ $k2 = (\alpha^{y2})^{x2} = (\alpha^{x2})^{y2}$

Entity authentication

- Alice and Bob share a secret k

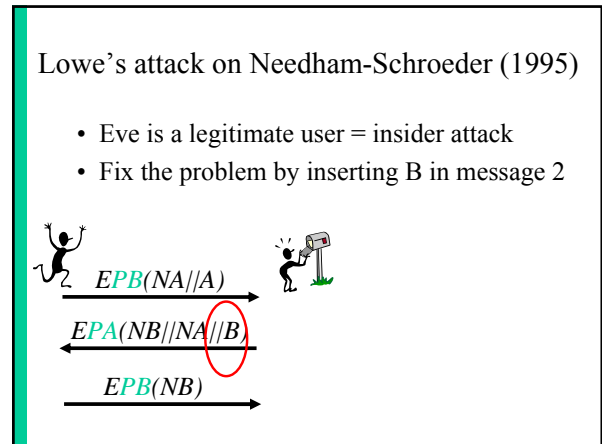
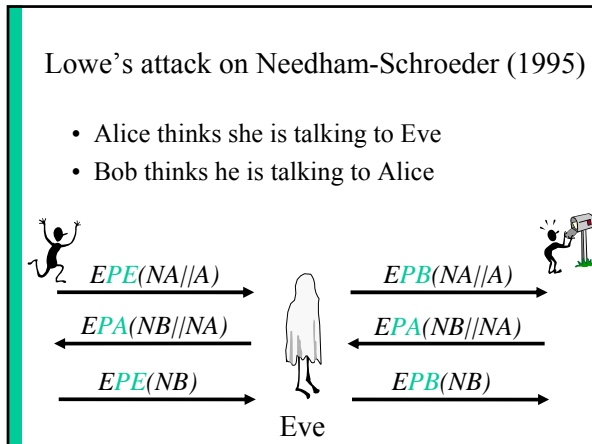
Entity authentication: reflection attack

- Eve does not know k and wants to impersonate Bob

Needham-Schroeder (1978)

- Alice and Bob have each other's public key PA and PB

Derive a session key k from $NA||NB$



Lessons from Needham-Schroeder (1995)

- Prudent engineering practice (Abadi & Needham): include names of principals in all messages
- **IKE v2 – plausible deniability**: don't include name of correspondent in signed messages:
<http://www.ietf.org/proceedings/02nov/I-D/draft-ietf-ipsec-soi-features-01.txt>

Rule #1 of protocol design

Don't!

Why is protocol design so hard?

- Understand the security properties offered by existing protocols
- Understand security requirements of novel applications
- Understanding implicit assumptions about the environment underpinning established properties and established security mechanisms

And who are Alice and Bob anyway?

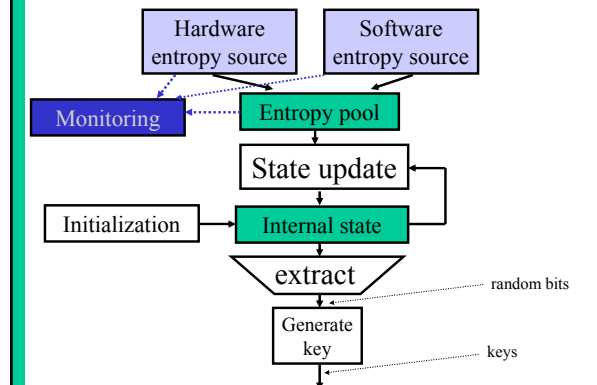
- Users?
- Smart cards/USB tokens of the users?
- Computers?
- Programs on a computer?

If Alice and Bob are humans, they are vulnerable to social engineering

Random number generation

- “The generation of random numbers is too important to be left to chance”
- John Von Neumann, 1951: "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin”
- Used for
 - Key generation
 - Encryption and digital signatures (randomization)
 - Protocols (nonce)

Key generation: overview



Key generation: hardware entropy sources

- radioactive decay
- reverse biased diode
- free running oscillators
- radio
- audio, video
- hard disk access time (air turbulence)
- manually (dice)
- lava lamps

Risk: physical attacks, failure

Key generation: software entropy sources

- system clock
- elapsed time between keystrokes or mouse movements
- content of input/output buffers
- user input
- operating system values (system load, network statistics)
- interrupt timings

Risk: monitoring, predictable

Key generation: monitoring

- Statistical tests (NIST FIPS 140)
- typical tests: frequency test, poker test, run's test
- necessary but not sufficient
- 5 lightweight tests to verify correct operation continuously
- stronger statistical testing necessary during design phase, after production and before installation

State update

- Keep updating entropy pool and extracting inputs from entropy pool to survive a state compromise
- Combine both entropy pool and existing state with a non-invertible function (e.g., SHA-512, $x^2 \bmod n, \dots$)

Output function

- One-way function of the state since for some applications the random numbers become public
- A random string is not the same as a random integer mod p
- A random string is not the same as a random prime

What **not** to do

- use `rand()` provided by programming language or O/S
- restore entropy pool (seed file) from a backup and start right away
- use the list of random numbers from the RAND Corporation
- use numbers from <http://www.random.org/>
 - **66198 million random bits served since October 1998**
- use digits from π , e , π/e , ...
- use linear congruential generators
 - $x_{n+1} = a x_n + b \text{ mod } m$

RSA moduli

- Generate a 1024-bit RSA key
Use random bit generation to pick random a integer r in the interval $[2^{512}, 2^{513}-1]$
If r is even $r:=r+1$
Do $r:=r+2$ until r is prime; output p
Do $r:=r+2$ until r is prime; output q

What is the problem?

What to consider/look at

- There are no widely used standardized random number generators
- Learn from open source examples: `ssh`, `openpgp`, linux kernel source
- `/dev/random` (slow)
- Yarrow/Fortuna
- ANSI X9.17 (but parameters are marginal)
- Web resource:
<http://www.cs.berkeley.edu/~daw/rnd/>

How to store keys

- Disk: only if encrypted under another key
 - But where to store this other key?
- Human memory: passwords limited to 48-64 bits and passphrases limited to 64-80 bits
- Removable storage: Floppy, USB token, iButton, PCMCIA card
- Cryptographic co-processor: smart card USB token
- Cryptographic co-processor with secure reader and keypad
- Hardware security module

How to back-up keys

- Backup is essential for decryption keys
- Security of backup is crucial
- Secret sharing: divide a secret over n users so that any subset of t users can reconstruct it

Destroying keys securely is harder than you think