BUSLab

Brno University Security Laboratory

JAP Anonymity & Privacy

ANONYMITY IS NOT A CRIME

Secure logging of retained data

Stefan Köpsell* and Petr Švenda`

*TU Dresden, Germany, <*sk13@inf.tu-dresden.de*>

‘Masaryk University, Czech Republic, <*svenda@fi.muni.cz*>

Data Retention in the EU

- Regulated by: *"**DIRECTIVE 2006/24/EC** OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 March 2006 **on the retention of data** generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC"*
- Purpose: "retention of certain data …, in order to ensure that the data are available for the purpose of the **investigation, detection and prosecution of serious crime**, as defined by each Member State in its national law "
- Data to retain: "**traffic and location data** … to identify … registered user … **not** … the **content** of electronic communications, including information consulted using an electronic communications network. "
- Retention period: "**not less than six months** and **not more than two years** from the date of the communication"
- Access to retained data: „only … competent **national authorities** in **specific cases** and in **accordance with national law** "

Data Retention in the EU

- Article 5 of the Directive regulates in more details which data has to be retained:
  - to trace and identify the source and destination of a communication
  - to identify the date, time and duration of a communication
  - to identify the type of communication
  - to identify users' communication equipment
  - to identify the location of mobile communication equipment

The *AN.ON* project

- Shall realize anonymity even against strong attackers eavesdropping all communication links
- Shall support low latency applications, especially Web surfing
- Project carried out by Dresden University of Technology, University Regensburg and Independent Centre for Privacy Protection, Schleswig-Holstein, Germany
- Test version available
  - http://anon.inf.tu-dresden.de

How it works

„JAP" has to be configured as a proxy in the browser

User A

User B

User C

User D

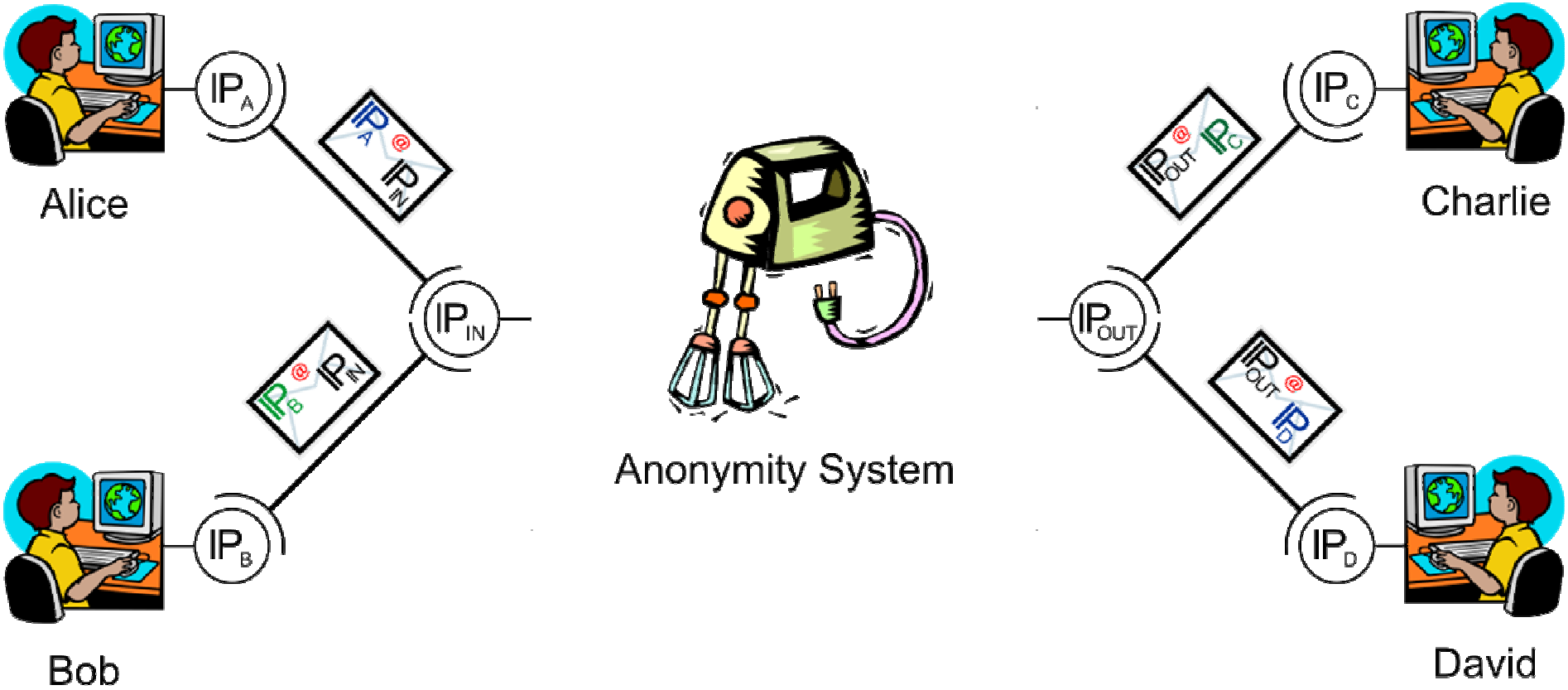
User E

Mix 1

Mix 2

Mix 3

Application of the Data Retention Rules on AN.ON

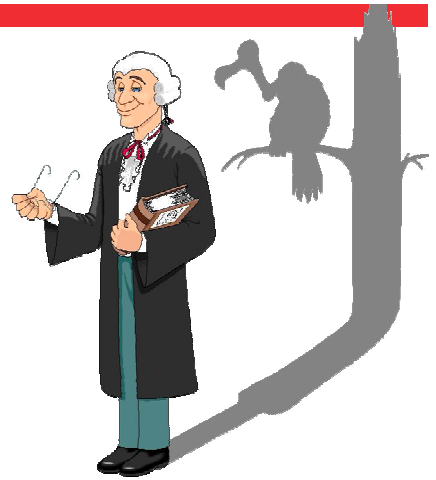


- All mixes have to work together to deanonymise a communication relation!

Do we need secure logging here?

- Do anonymity services (AN.ON, TOR...) fall within the scope of data retention directive?
  - unclear situation, probably yes
- Secure logging mechanism is necessary
  - several schemes already exist
  - but attacker model changed!
- Data retention introduces new risks for operators
  - access gate to retained data
  - enforcement of data retention period
  - unintentional disclosure of confidential data

Implications of law requirements

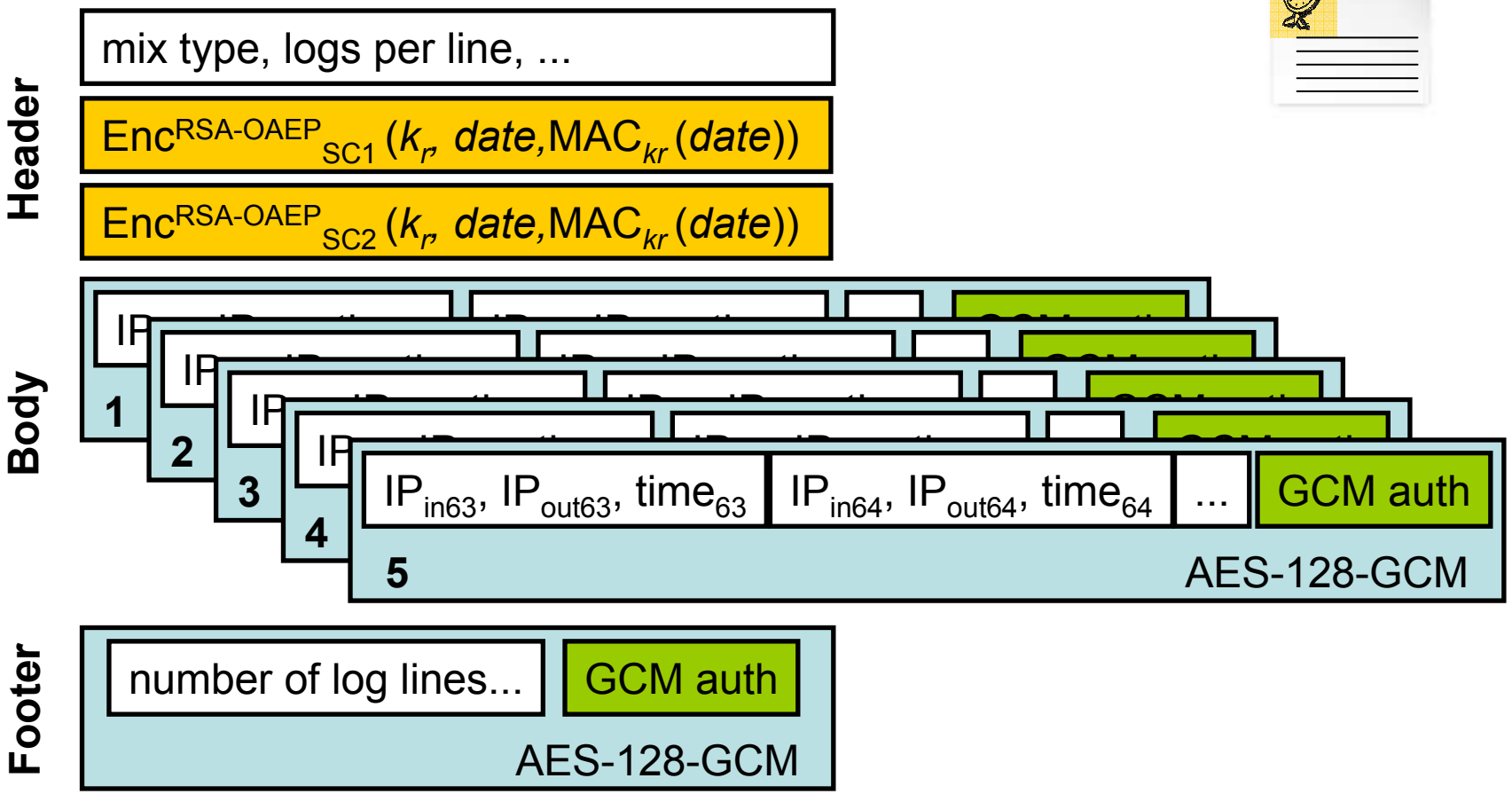


- Logged data has to identify the source of a communication
  - IP addresses for Interned services, alteration of IPs for AN.ON
- Logged data has to be deleted after a determinate period
  - storage only for limited period (6-24 months)
  - physical/logical (erase of encryption keys) deletion (ideally both)
- Logged data need to be accessible for law enforcement
- Logged data has to be secure
  - no access/modification from unauthorized person
- The logging process should not significantly degrade overall performance of the system

Main attacker goals

- Obtain retained data
  - inside/outside data retention period
  - police, government, censorship, data miners
- Modify retained data
  - user to hide misbehaving
  - corrupted police to forge evidence
- Erase part of retained data
  - user to hide misbehaving
- Prevent access to retained data
  - user to hide misbehaving

Core scheme


Header
mix type, logs per line, ...
Enc^RSA-OAEP_SC1 (k_r, date, MAC_kr (date))
Enc^RSA-OAEP_SC2 (k_r, date, MAC_kr (date))
Body
1
2
3
4
5
IP_in63, IP_out63, time_63
IP_in64, IP_out64, time_64
...
GCM auth
AES-128-GCM
Footer
number of log lines...
GCM auth
AES-128-GCM

Cryptographic smart card

- Used as secure storage for private keys
  - private key never leaves the card
- Trusted device to enforce data retention period
  - log key returned only inside data retention period
  - operator cannot be forced to do otherwise
- But how to securely obtain current date?
  - smart cards usually do not have internal time
  - set by operator (but he can be pressed)
  - trusted time server(s)

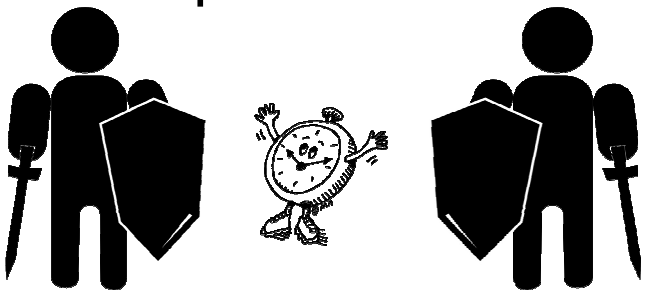
```
short monthsDifference = (short) ((short) (m_dateYear - year)
    * MONTHS_PER_YEAR + m_dateMonth - month);

// INCLUDE DAYS
if (m_dateMonth < month) {
  if (m_dateDay > day) monthsDifference--;
  if (m_dateDay < day) monthsDifference++;
}

// CHECK FOR RETENTION PERIOD
if (monthsDifference < DATA_RETENTION_PERIOD) status = TRUE;
else status = FALSE;
```

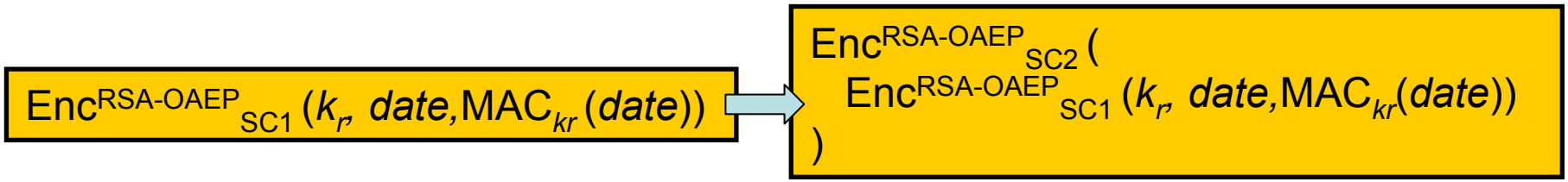
Current time from trusted time server

- Important feature that prevents log access outside data retention period
  - even when operator is pressed by an attacker (police)
- Direct communication between card and server
  - PC only as proxy, cannot manipulate communication
  - operator cannot be forced to set wrong date
- Activated during key recovery request
  - key K_r is returned only when retention period is valid



Plausible deniability

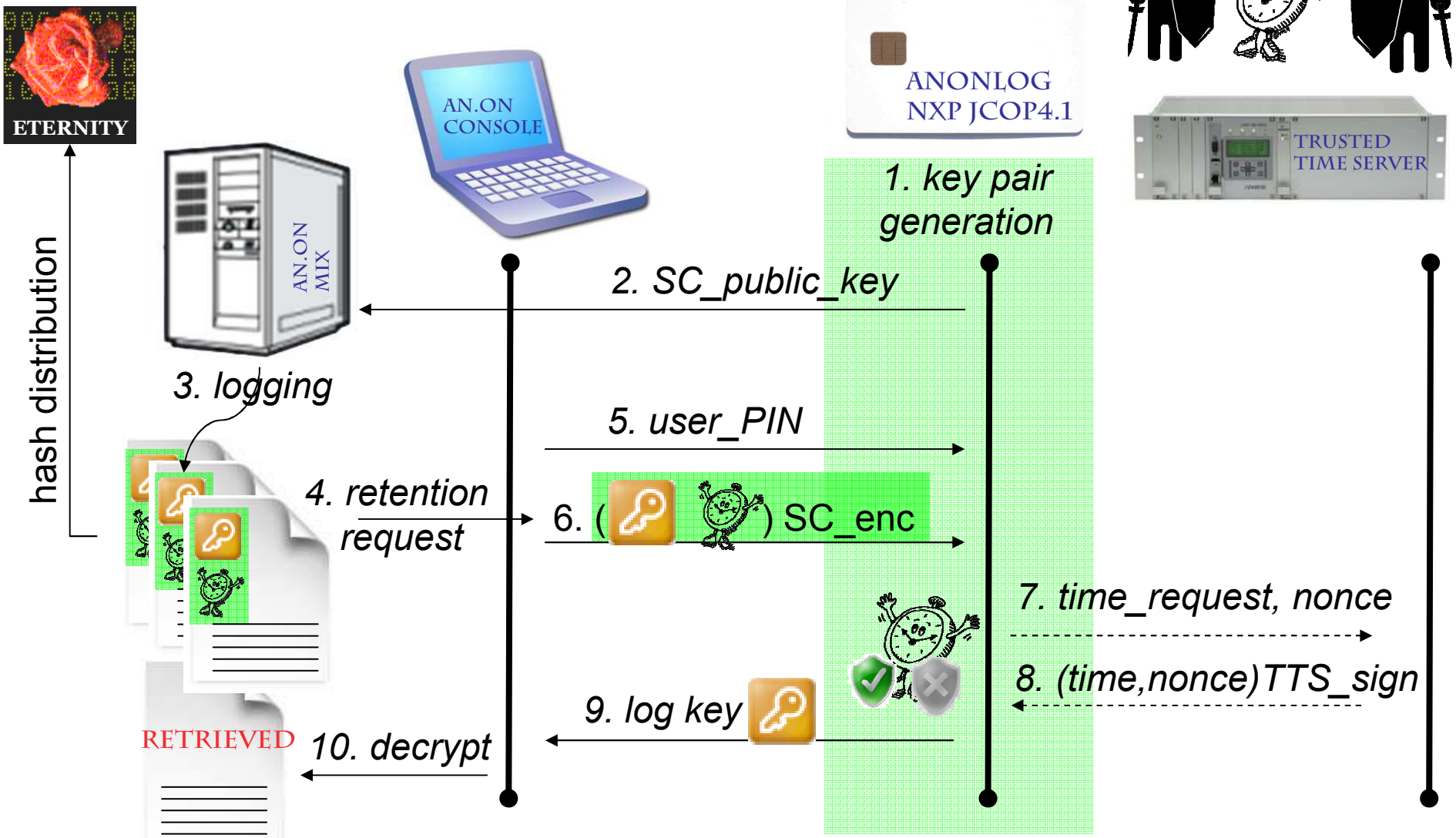
- Operator cannot pretend that no logs are stored
  - inside data retention period
- Giving wrong copy of log files
  - structurally correct, but wrong data
  - probably hard to make it plausible
- No outputs of decrypted logs in clear form
  - decryption key rewrapped by authority public key, need for PKI
- Multiple cards (and operators) required to access
  - multiple re-encryptions of key block



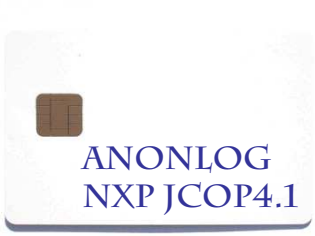
Forward-secure stream integrity

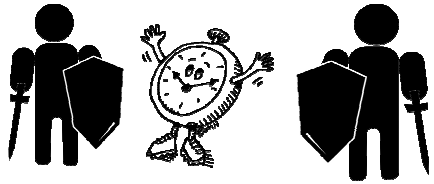
- How to protect integrity of data of compromised mix logged before compromise?
- Forward Secure Sequential Aggregate Authentication
  - (Ma and Tsudik, 2009)
  - 5.55 ms per single log entry (Intel dual-core 1.73 GHz)
  - but AN.ON produce >10 million log entries/day!
- We need something “faster”
  - periodic public distribution of log files hashes
    - Eternity service, P2P file sharing

Secure logging for AN.ON mixes



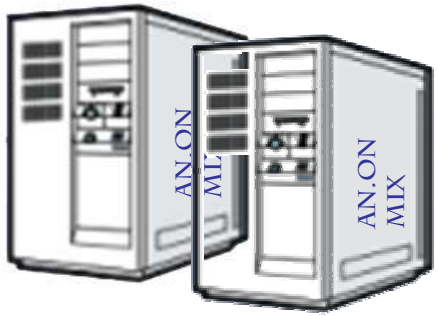
Attack: Access to stored log files

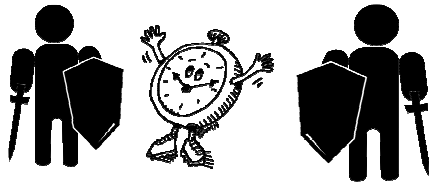




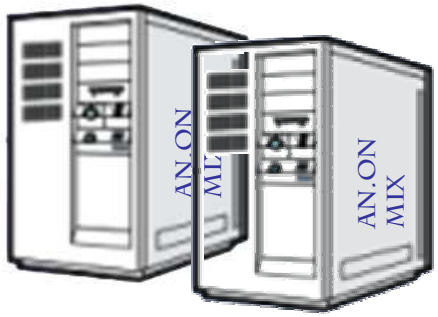
Attack: Particular mix(es) compromised

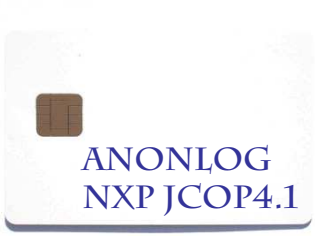
Attack: Data, card and tools accesible

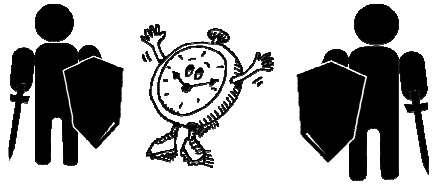


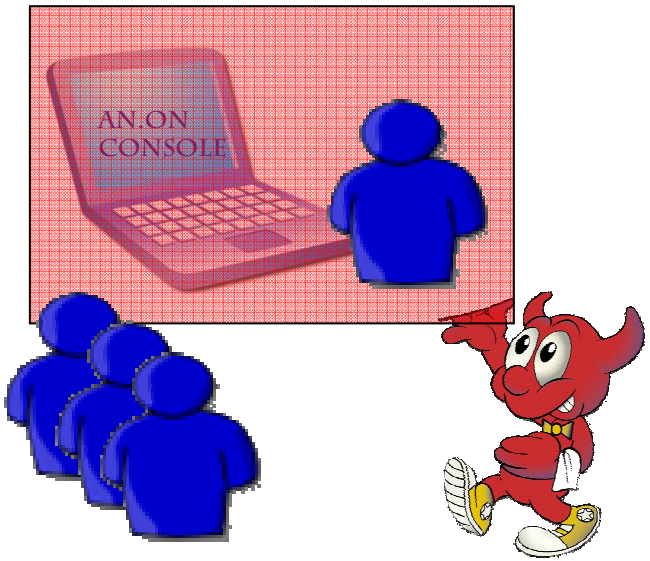


Attack: Personal pressure from attacker

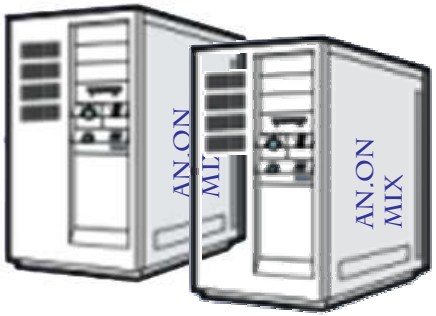


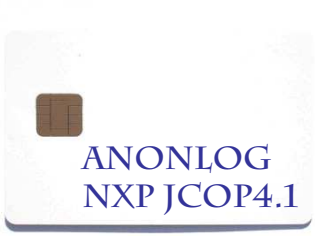


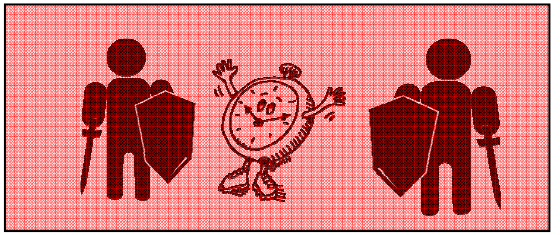




Attack: Compromise of trusted time server





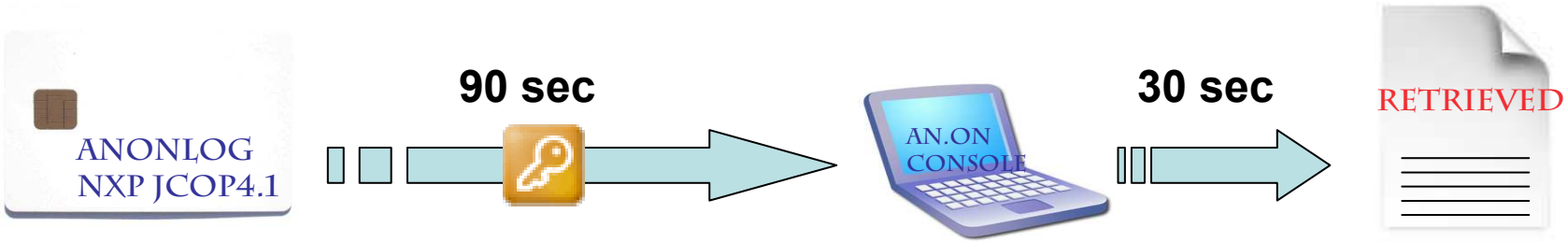


Logging performance

- AN.ON system generate log files on daily basis
  - roughly 85000 blocks/day, block contains 128 entries
  - more than 10 million log entries every day
  - 85 MByte/s for AES-128 in GCM mode
  - (Intel Core 2 DUO T7700 2.4 GHz CPU)
- Performance impact
  - single log entry needs less than 20 bytes
  - overhead for single log entry less than 0.25 μs

Search performance

- 630 seconds to decrypt whole log file
  - not necessary to decrypt whole file
  - around 30 seconds for typical retention request
- But 90 second to retrieve key from smart card
  - caused by software-only implementation of SHA2-512
  - coming smart card hardware support will solve this



Conclusions

- Data retention introduced new attacker scenarios
  - and new threats for operators
  - existing secure logging schemes not suitable
- Our proposal uses smart cards combined with trusted time servers
  - to remove attack surface from operator
  - to robustly enforce data retention period
  - to have low performance impact
  - and to provide usual CIA requirements in patent-free way

Questions ?