UNIK4750 - Measurable Security for the Internet of Things

L13 - System Security and Privacy analysis

György Kálmán,
Mnemonic/NTNU/UiO ITS
gyorgy.kalman@its.uio.no

Josef Noll
UiO ITS
josef.noll@its.uio.no

Overview

- terminology of “classes”
- examples of security classification
  - example domains
- privacy classification
- match between application goals and security/privacy classification

L13 - Expected Learning outcomes

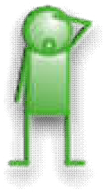
Having followed the lecture, you can

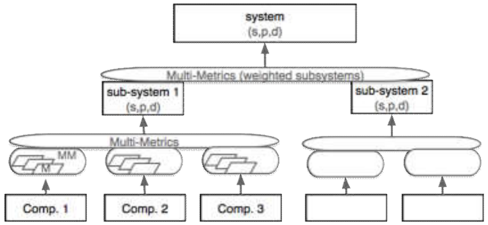
- explain terminology for security and privacy
- provide examples of security classes
- provide examples of privacy data
- reason over relation between System$_{SPD}$ and security/privacy goals of applications

goal

versus

System$_{SPD}$





system of systems

Terminology

- Information System Security based on ISO 27000 standards, named cyber security to avoid mixing with physical security
- Industrial Control Systems (ICS) - designates a set of human and material resources designed to control or operate technical installations
- Sector - here used as industrial areas, e.g. energy, transport, water supply, industry, as well as Building Management System (BMS)
- Data Breach - loss, unauthorized access to or disclosure of personal data as a result of a failure of the organisation to effectively safeguard the data
- Privacy by Design (PbD) - creating methods to protect privacy in the design of systems, a.o. *measurable* and *proven* privacy results

References:
http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

Applicability of security and privacy classes

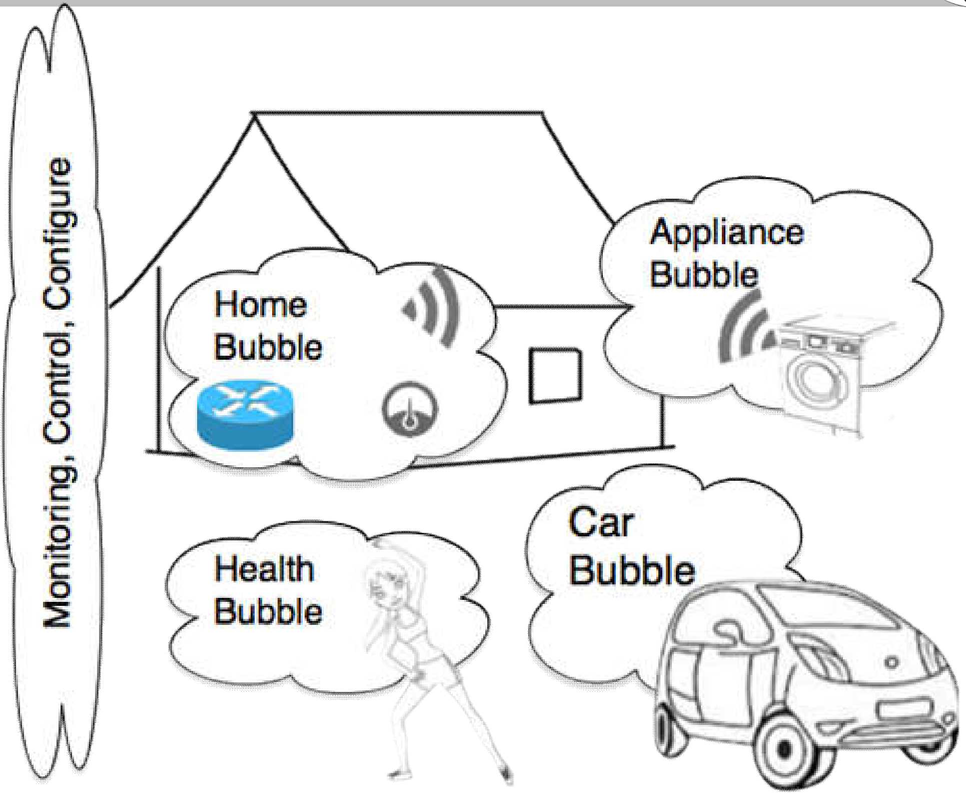
- Applications & application information

Privacy

- abstract principles, rights-based argumentation
- Privacy laws “identifiable information”
- Privacy by design, enforceable privacy
- privacy-invasive services

Security

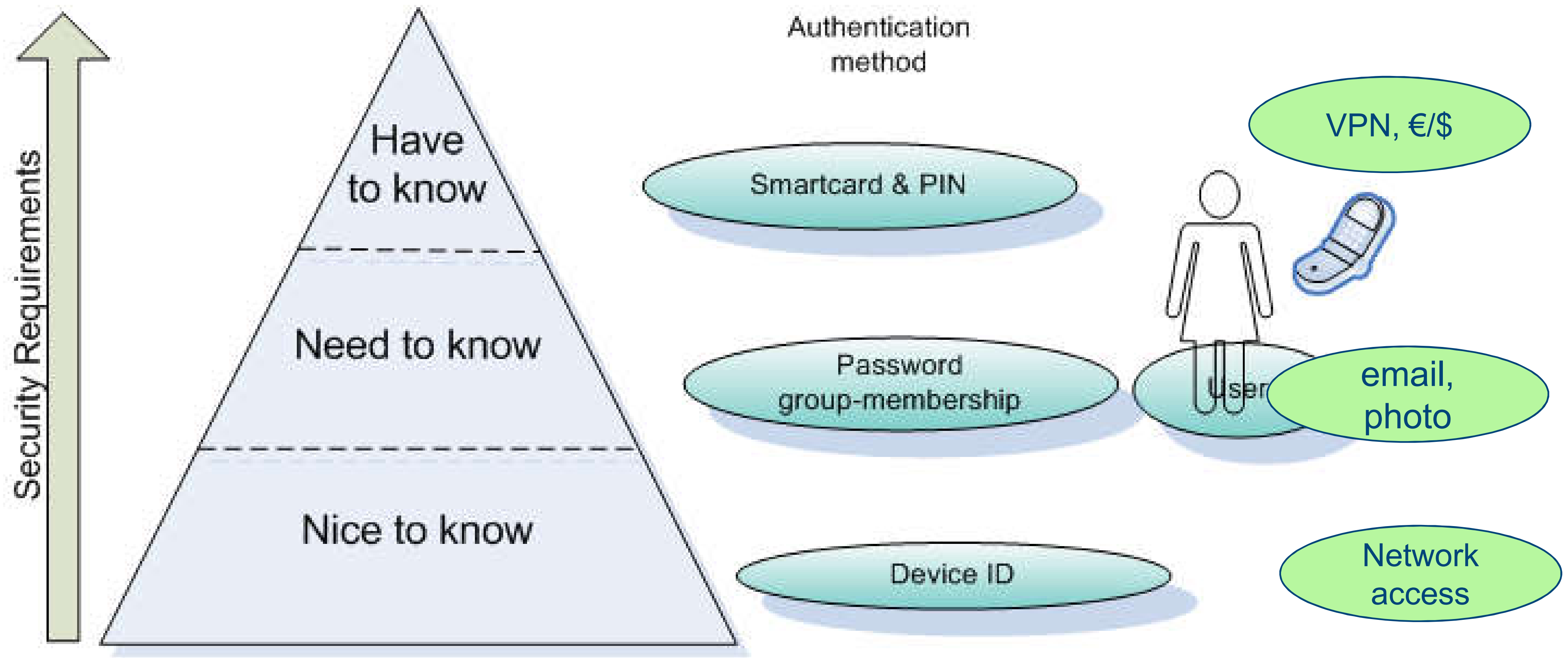
- System classifications
  - code: red, yellow, green



note: Bubble means both applications and system,
e.g. car bubble address
- applications: charging, software update, …
- sub-system: communication, control/identify

Security Requirements

Examples of Services



Information Security Classification

- Class 1: ICSs for which the risk or impact of an attack is low. The measures recommended for this class must be able to be applied in complete autonomy. This class mainly corresponds to rules provided in the ANSSI Healthy Network Guide.
- Class 2: ICSs for which the risk or impact of an attack is significant. There is no state control over this class of ICS, but in the event of inspection or incident, the responsible entity must be able to provide evidence that adequate measures have been implemented.
- Class 3: ICSs for which the risk or impact of an attack is critical. In this class, the obligations are heightened and the conformity of ICSs is verified by the state authority or an accredited body.

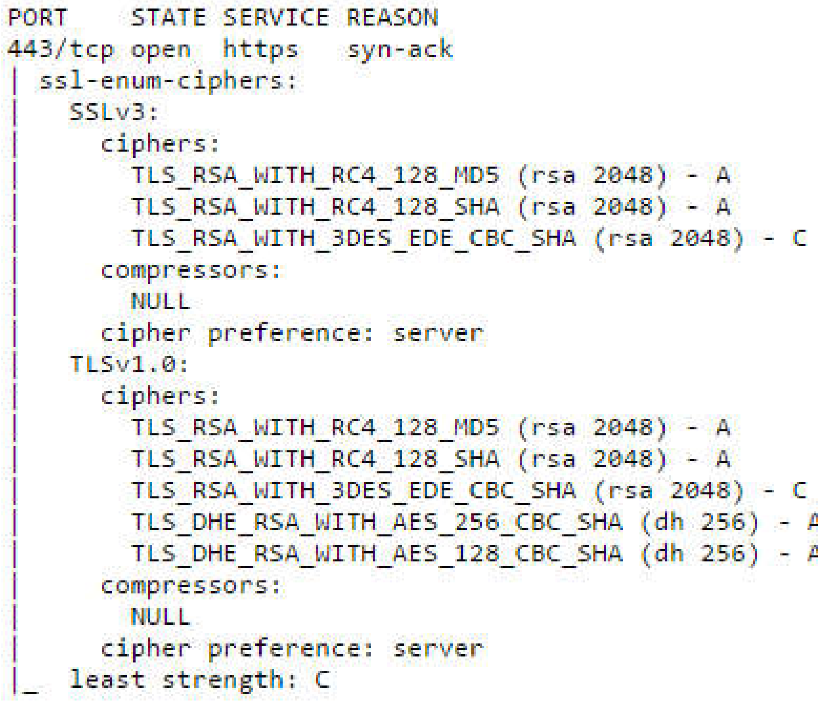
Consequences/measures for

- roles and responsibilities
- risk analysis
- inventory (rapid assessment of system)
- user training, control, certification
- audits
- monitoring process
- business resumption and continuity plan
- emergency modes
- alert and crisis management
- network segmentation and segregation
- remote diagnosis, maintenance and management
- surveillance and intrusion detection methods
- security approval

http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf

Classification example – OpenSSL ciphers

- Nmap: ssl-enum-ciphers script
- Enumerates all the supported cipher suites in the actual openssl installation
- Guides attacks to the weakest supported set – but also administrators to switch off forgotten old or even NULL ciphers (testing)
- In the multi-metric approach, can classes mean certain «goodness» values
- One dimension of a multi-dimensional problem:
  especially in IoT, on board resources can limit the choice of cipher.

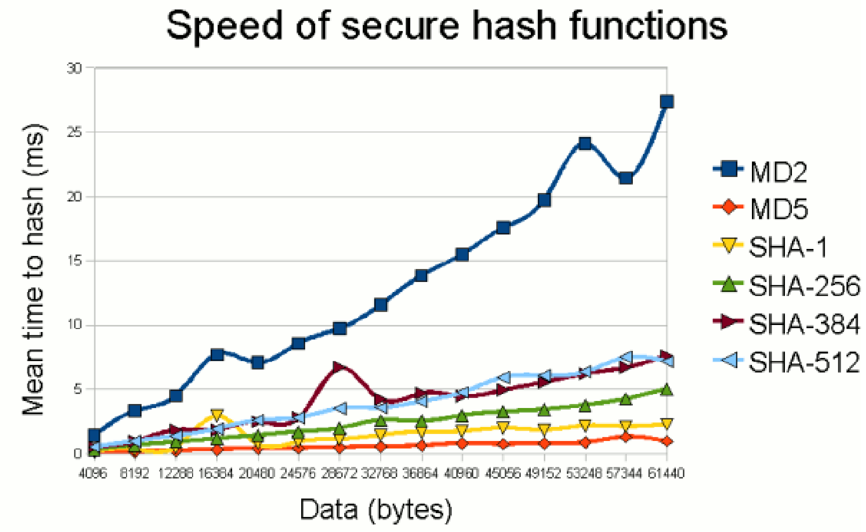


```
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-enum-ciphers:
|   SSLv3:
|     ciphers:
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - A
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_DHE_RSA_WITH_AES_256_CBC_SHA (dh 256) - A
|       TLS_DHE_RSA_WITH_AES_128_CBC_SHA (dh 256) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: C
```

Classification example – time

- Required strength security/integrity protection depends on the data protected – classify with resurce need, typically cycle time
- This is a tradeoff between resource usage and importanc/life time
- See hash example: delay vs security, in IoT a ms can be long time
- Some benchmark examples: https://www.wolfssl.com/wolfSSL/benchmarks-wolfssl.html

```
MD5       25 kB took 0.003 seconds,   8.138 MB/s
POLY1305 25 kB took 0.004 seconds,   6.104 MB/s
SHA       25 kB took 0.006 seconds,   4.069 MB/s
SHA-256  25 kB took 0.014 seconds,   1.744 MB/s
SHA-512  25 kB took 0.042 seconds,   0.581 MB/s
```



http://www.javamex.com/tutorials/cryptography/HashTime.png

Example:
Server Rating (SSL Labs)

Numerical Score	Grade
80 <= score	A
65 <= score < 80	B
50 <= score < 65	C
35 <= score < 50	D
20 <= score < 35	E
score < 20	F

Note: continuous updates over time

Changes in 2009h (30 October 2014)

- Don’t award A+ to servers that don’t support TLS_FALLBACK_SCSV.
- Cap to B if SSL 3 is supported.

Changes in 2009i (8 December 2014)

- Cap to B if RC4 is supported.
- Cap to B if the chain is incomplete.
- Fail servers that have SSL3 as their best protocol.

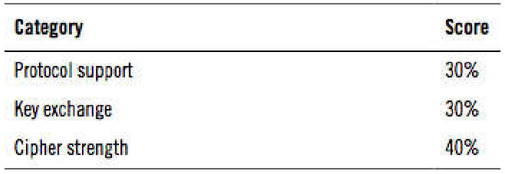
Changes in 2009j (20 May 2015)

- Cap to B if using weak DH parameters (less than 2048 bits).
- Increase CRIME penalty to C (was B).
- Cap to C if RC4 is used with TLS 1.1+.
- Cap to C if not supporting TLS 1.2.

Changes in 2009k (14 October 2015)

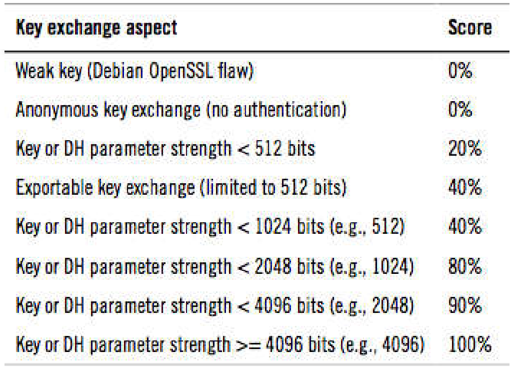
- Fail servers that support only RC4 suites.

Table 2. Criteria categories



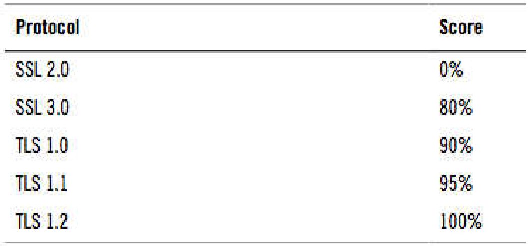
Category	Score
Protocol support	30%
Key exchange	30%
Cipher strength	40%

Table 4. Key exchange rating guide



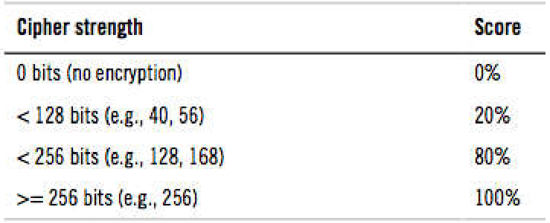
Key exchange aspect	Score
Weak key (Debian OpenSSL flaw)	0%
Anonymous key exchange (no authentication)	0%
Key or DH parameter strength < 512 bits	20%
Exportable key exchange (limited to 512 bits)	40%
Key or DH parameter strength < 1024 bits (e.g., 512)	40%
Key or DH parameter strength < 2048 bits (e.g., 1024)	80%
Key or DH parameter strength < 4096 bits (e.g., 2048)	90%
Key or DH parameter strength >= 4096 bits (e.g., 4096)	100%

Table 3. Protocol support rating guide



Protocol	Score
SSL 2.0	0%
SSL 3.0	80%
TLS 1.0	90%
TLS 1.1	95%
TLS 1.2	100%

Table 5. Cipher strength rating guide

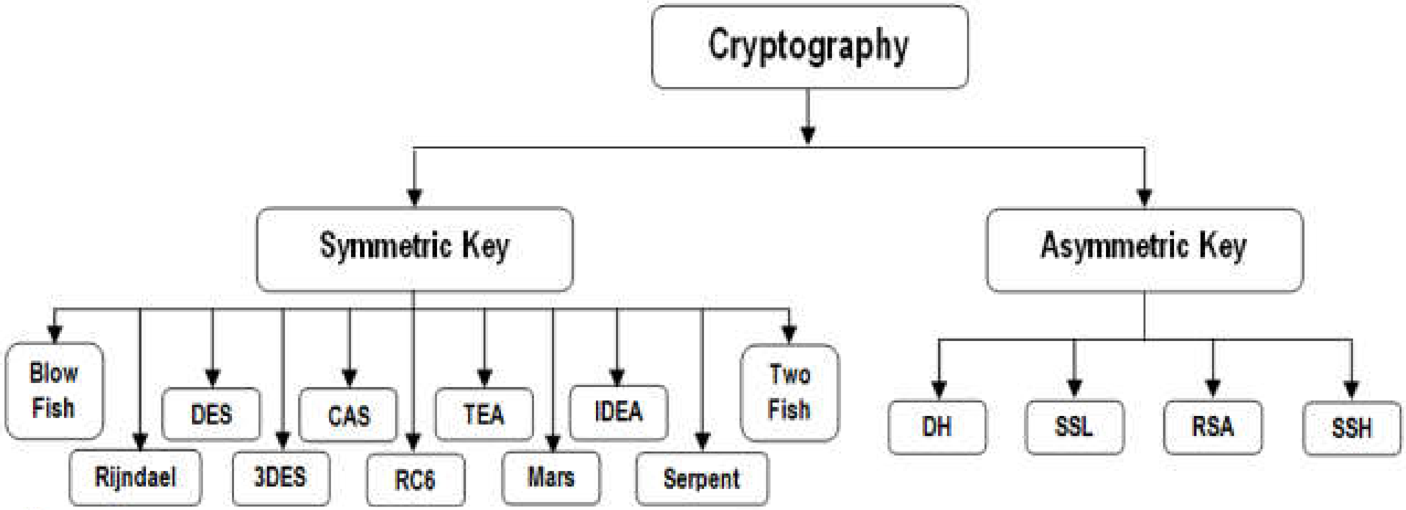


Cipher strength	Score
0 bits (no encryption)	0%
< 128 bits (e.g., 40, 56)	20%
< 256 bits (e.g., 128, 168)	80%
>= 256 bits (e.g., 256)	100%

calculate using mean:
*0.5 * (best + worse)*

https://www.ssllabs.com/downloads/SSL_Server_Rating_Guide.pdf

Example
Symmetric and Asymetric Key Cryptography



Cryptography

Symmetric Key

Blow Fish

Rijndael

DES

3DES

CAS

RC6

TEA

Mars

IDEA

Serpent

Two Fish

Asymmetric Key

DH

SSL

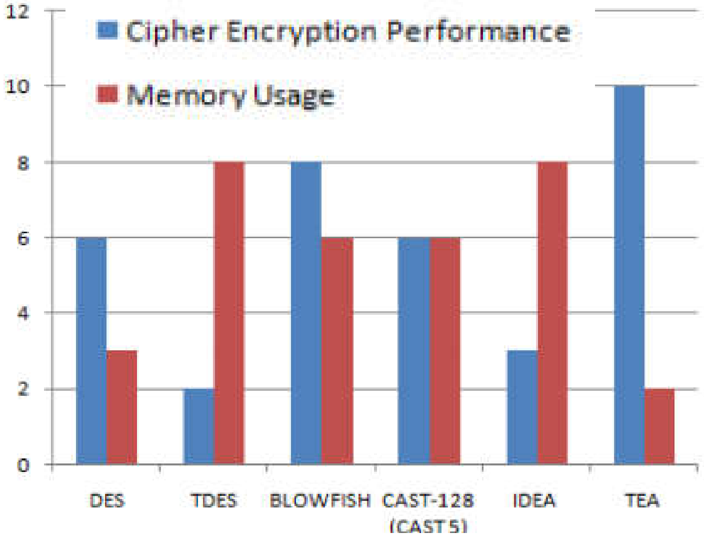
RSA

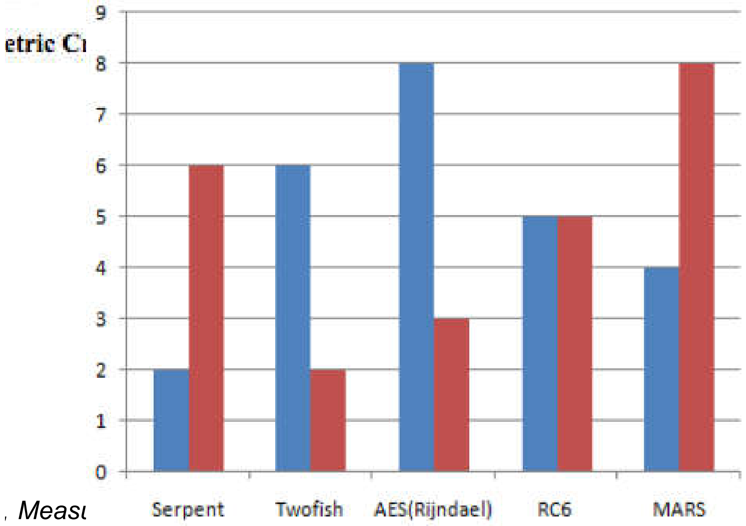
SSH

some flaws in symmetric algorithms such as

- weak keys
- insecure transmission of secret key,
- speed,
- flexibility,
- authentication and reliability

i.e. in DES, four keys for which encryption is exactly the same as decryption





Translate into security measures?

https://arxiv.org/ftp/arxiv/papers/1405/1405.0398.pdf

How to define security?

- We looked at cipher strengths, hash speeds, have defined an interval of acceptable quality of service
- What forms the baseline: in IoT: regulations. We use frameworks to create a security baseline, which fulfills the regulator’s minimal set of requirements
- Several frameworks exist: kind of all the same: provides a structured approach for defining the baseline and also achieving it.
- The choice of framework can depend on industry, the actual contract or personal preference
- Examples are: COBIT, ISA99 (IEC 62443), NERC 1300 (critical infrastructure protection)

About privacy

- 1980: OECD guidelines (oecdprivacy.org) Guidelines Governing The Protection of Privacy and Transborder Flows of Personal Data.
- 2005: Kim Cameron - 7 laws of identity
- 2011 OECD update on privacy guidelines
- 2012 EU Data Protection Reform
  - “Right to be forgotten”
  - Easier access to one’s data; right to data portability
  - Data protection **by design** and **by default**
  - Stronger enforcement of the rules - up to 4% of annual turnover
- From 2018: General Data Protection Regulation (adopted in April 2016)
  - EU-wide harmonization
  - User control
  - More limitations on sending data outside

http://www.oecd.org/sti/ieconomy/49710223.pdf

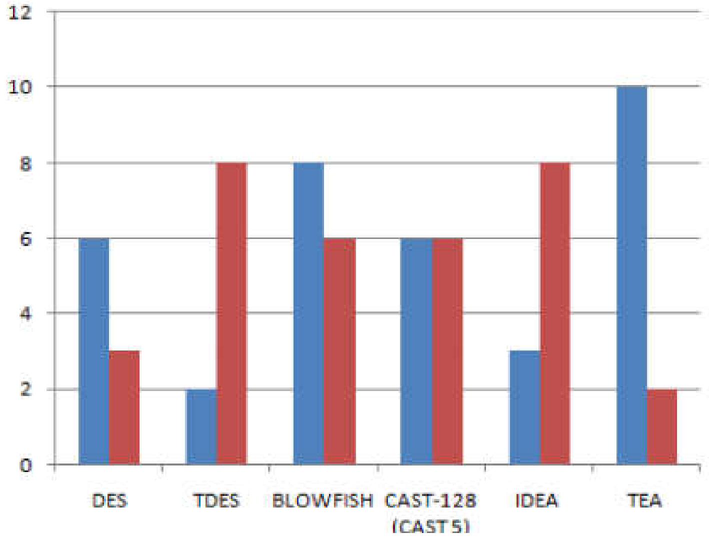
http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

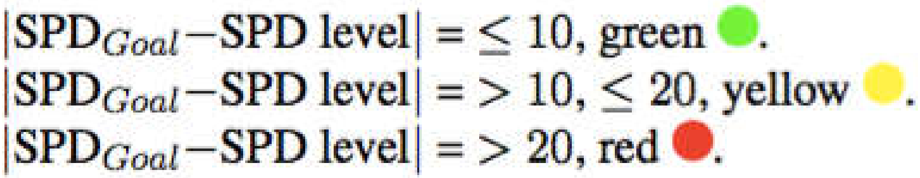
1. Collection Limitation Principle - “limits to the collection of personal data…”
2. Data Quality Principle - “relevant and necessary for the purpose of usage”
3. Purpose Specification Principle - “specified prior to collection - change of purpose”
4. Use Limitation Principle - “non disclosure, not for others than those” - “need consent”
5. Security Safeguards Principle - “protection by reasonable security safeguards”
6. Openness Principle - “about developments, practices and policies”
7. Individual Participation Principle - “individual to have insight, answers in reasonable time…”
8. Accountability Principle - “data controller should be accountable”

Conclusions

- Performed a review on security and security classes
  - Examples: server rating, ssh security
- Privacy and identity
  - ongoing discussion on privacy enforcement

- can we really draw conclusions?





$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = \leq 10$, green ●.

$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = > 10, \leq 20$, yellow ●.

$|\mathrm{SPD}_{Goal} - \mathrm{SPD\ level}| = > 20$, red ●.

Intrusion Detection and Prevention

- What is an Intrusion Detection System
- Flavours of IDS
- Industrial case
  - Comparison to generic cases
  - Physical process and safety
- Industrial examples
- Conclusion

Definitions – as requested – both definitions by ISACA

- Information security: "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)
- Privacy: The rights of an individual to trust that others will appropriately and respectfully use, store, share and dispose of his/her associated personal and sensitive information within the context, and according to the purposes, for which it was collected or derived

- I think, both security and privacy is easier to see from the other way around:
- Losing security and privacy.
- If you loose information security: then you loose confidentiality of important data or the possibility to check its integrity or just can’t access it.
- Same with privacy: if you loose it, then you can not control any more what is happening with private information

What is an Intrusion Detection System

- This is a practical example on fuzzy evaluation of different criteria and taking decisions by evaluating multi-dimension problems
- What is an intrusion: an attempt to break or misuse the system
- Might be internal or external source and can be physical, system or remote
- It is typically a set of entities distributed in the network and monitoring some network parameters

How an intrusion works

- Exploit different programming errors (e.g.: buffer overflow, no input validation)
- Unexpected input (e.g.: tamper with TCP checksum, fragmentation)
- Combination with creating special circumstances
- IDS need a baseline to work properly
- Baseline creation very much depends on the use
- We always assume, that they who attack behave differently

IDS flavours

- IDS can be based on:
  - Anomaly detection (heuristics) – challenge is good training and right set of sensitivity
  - Signature-based – challenge is to deal with new attacks
  - Typically we use a combination
- Or by location:
  - Host-based: the host os or application is running the logging, no additional hardware
  - Network-based: filters traffic, independent of clients

IDS in industrial environments

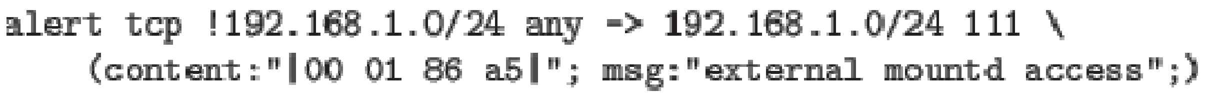
- Two important factors: much more clean traffic baseline is possible and relation to physical process and safety
- We can’t design a system to be secure forever – count with failure: fail-safe, fail-operational, graceful state changes
- Tamper detection and evidence
- The only difference between systems that can fail and systems that cannot possibly fail is that, when the latter actually fail, they fail in a totally devastating and unforeseen manner that is usually also impossible to repair(1)
- In an industrial environment the assumption that attackers will behave differently is not necessarely true

IDS in industrial environments

- IDS is a system: evaluation of logs, evaluation of network traffic, maintenance on firewall and IDS infrastructure (software+taps)
- Getting a reaction is actually easier in the industrial environment: typical to have 24 hours staffing somewhere, also physical security and safety
- Challenges with shared infrastructure and suppliers
- Possible approach: whitelisting, stateful payload analysis (operational envelope)

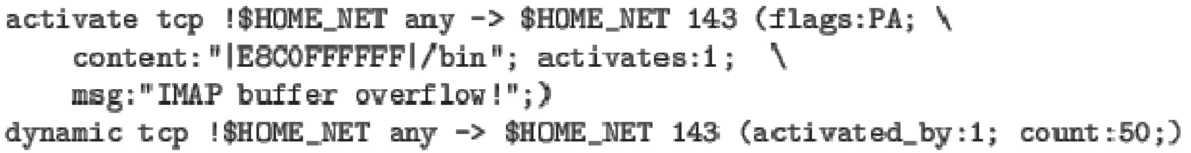
Example rules

- There are different ways, but take this snort rule as an example:



```
alert tcp !192.168.1.0/24 any -> 192.168.1.0/24 111 \
    (content:"|00 01 86 a5|"; msg:"external mountd access";)
```

- Dynamic rule example (both examples are from the snort manual):



```
activate tcp !$HOME_NET any -> $HOME_NET 143 (flags:PA; \
    content:"|E8C0FFFFFF|/bin"; activates:1;  \
    msg:"IMAP buffer overflow!";)
dynamic tcp !$HOME_NET any -> $HOME_NET 143 (activated_by:1; count:50;)
```

Industrial attacks

- No difference here: injection, man-in-the-middle, replay etc.
- Long life, high utilization of equipment and legacy support open for more attacks then in an office case
- SCADA compared to DCS/PCS
- Resilience and restoration
- Because of the use of COTS products, you actually might use the very same exploits, like windows on HMI

Industrial examples, from ICS-CERT (6)

Davis-Besse Nuclear Power Plant [2003]

- The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant
- Disabled a safety monitoring system for nearly five hours
- Power plant was protected by a firewall
- In 1998 the same plant was hit by a tornado (natural disaster)

Industrial examples, from ICS-CERT (6)

Maroochy Shire Sewage Spill [2000]

- First recorded instance of an intruder that “deliberately used a digital control system to attack public infrastructure”
- Software on his laptop identified him as “Pumping Station 4” and after suppressing alarms controlled 300 SCADA nodes
- Disgruntled engineer in Queensland, Australia sought to win the contract to clean up the very pollution he was causing
- He made 46 separate attacks, releasing hundreds of thousands of gallons (264,000) of raw sewage into public waterways

Industrial examples, from ICS-CERT (6)

CSX Train Signaling System [2003]

- Sobig virus blamed for shutting down train signaling systems throughout the east coast of the U.S.
- Virus infected Florida HQ shutting down signaling, dispatching, and other systems
- Long-distance trains were delayed between four and six hours

Conclusions on Intrusion Detection

- Intrusion Detection is an example, where a collection of parameters will serve as an input to a fuzzy system
- Industrial systems might be quite well suited for «sharp» heuristics
- The main difference is the physical process back (both plus and minus)
- Evaluation of the detection system is very much in line with the classification examples shown in previous lectures: one can define a set of metrics and analyise which level the system is can reach.

References - Classification

- Cybersecurity classes: http://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf
- IAEA: Computer Security at Nuclear Facilities: http://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf
- Red Tiger Security: mapping security controls to standards: http://isacahouston.org/documents/RedTigerSecurity-NERCCIPandotherframeworks.pdf
- Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

References – Intrusion Detection

1. https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Zanero.pdf
2. http://www.digitalbond.com/tools/quickdraw/
3. https://www.sans.org/reading-room/whitepapers/ICS/challenges-ids-ips-deployment-industrial-control-systems-36127
4. http://commons.erau.edu/cgi/viewcontent.cgi?article=1071&context=discovery-day
5. https://www.truststc.org/conferences/10/CPSWeek/papers/scs1_paper_8.pdf
6. http://www.clcert.cl/seminario/US-CERT_Chile_2007-FINALv2.ppt