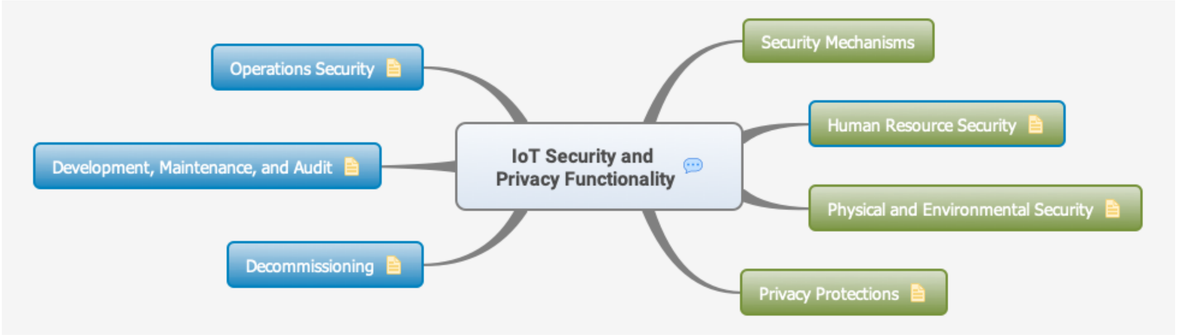
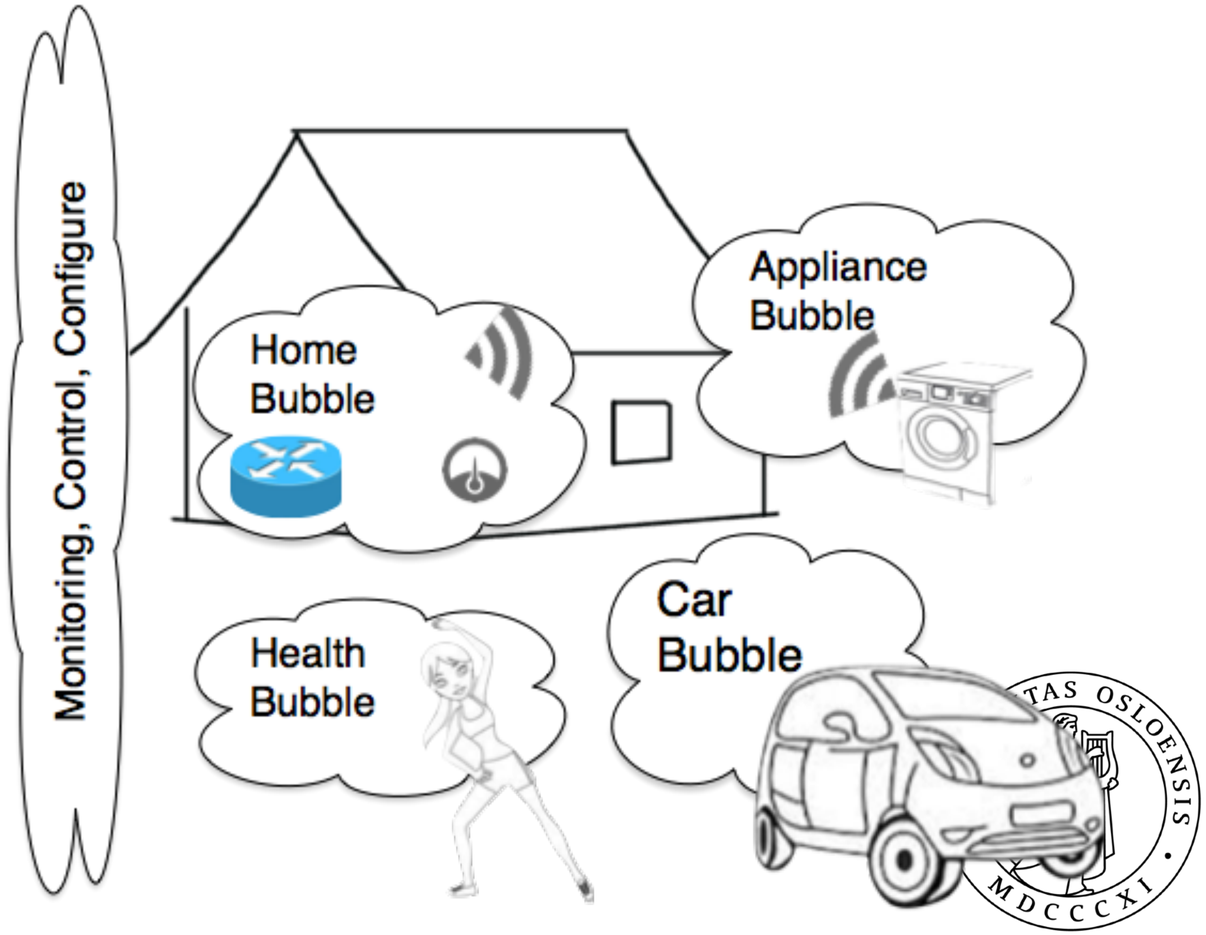
UNIVERSITY OF OSLO



TEK5530 Measurable Security for the Internet of Things

L9 - System Security and Privacy analysis



Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

L9 - 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

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, unauthorised 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

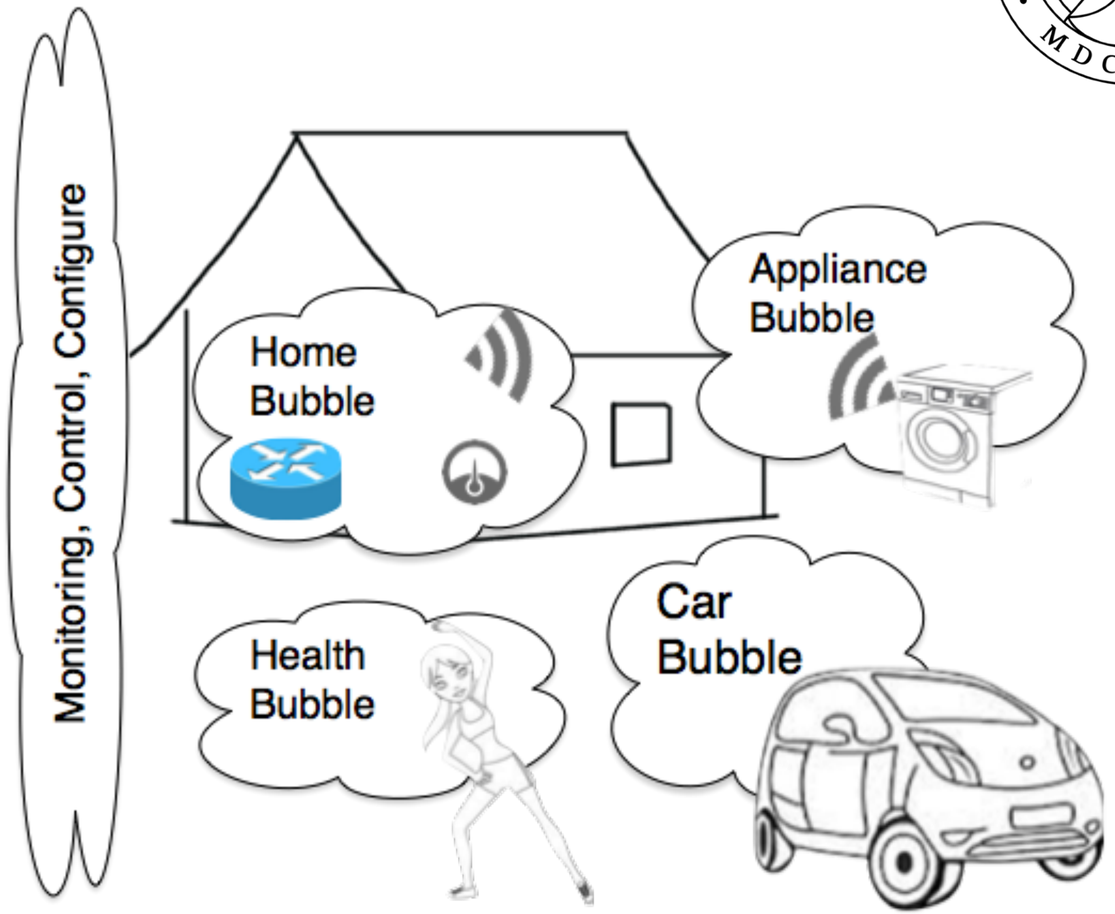
- Applications & application information

Privacy

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

Security

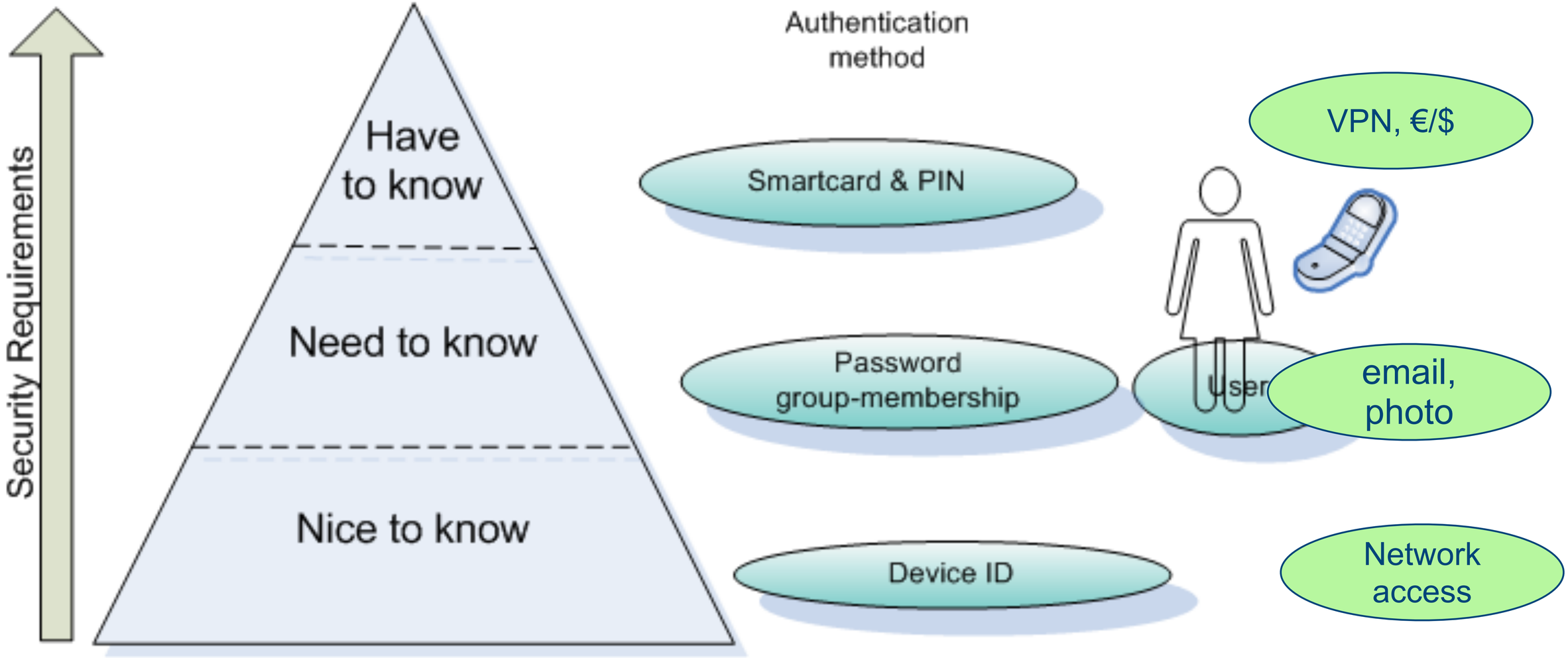
- System classifications
  - code: red, yellow, green



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

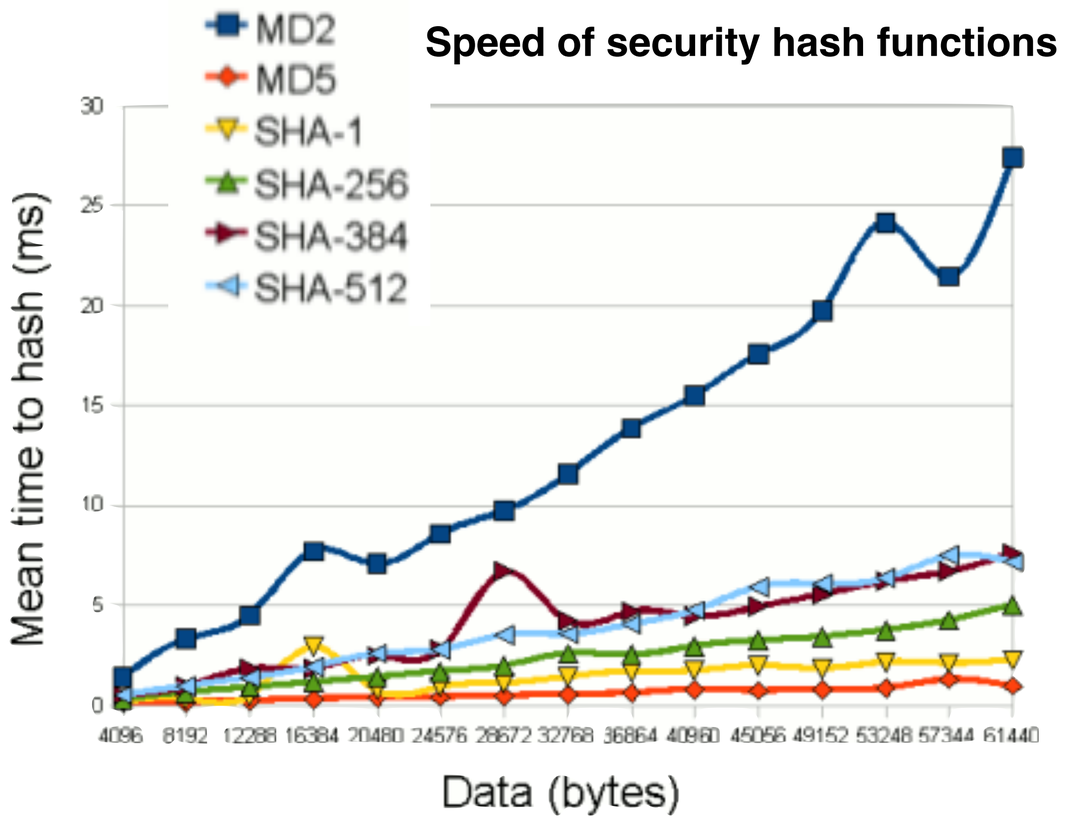
- Nmap: ssl-enum-ciphers script
- Enumerates all the supported cipher suites in the actual openssl installation
- Guides attacks to the weakest supported set – but also administrators to switch off forgotten old or even NULL ciphers (**testing**)
- In the multi-metric approach, can classes mean certain «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 resource 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%

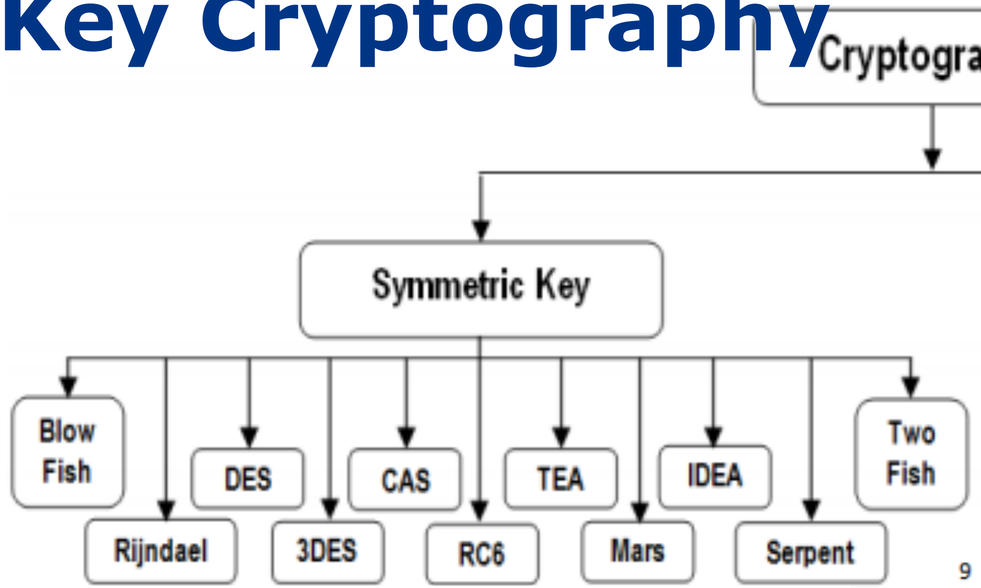
Table 5. Cipher strength rating guide

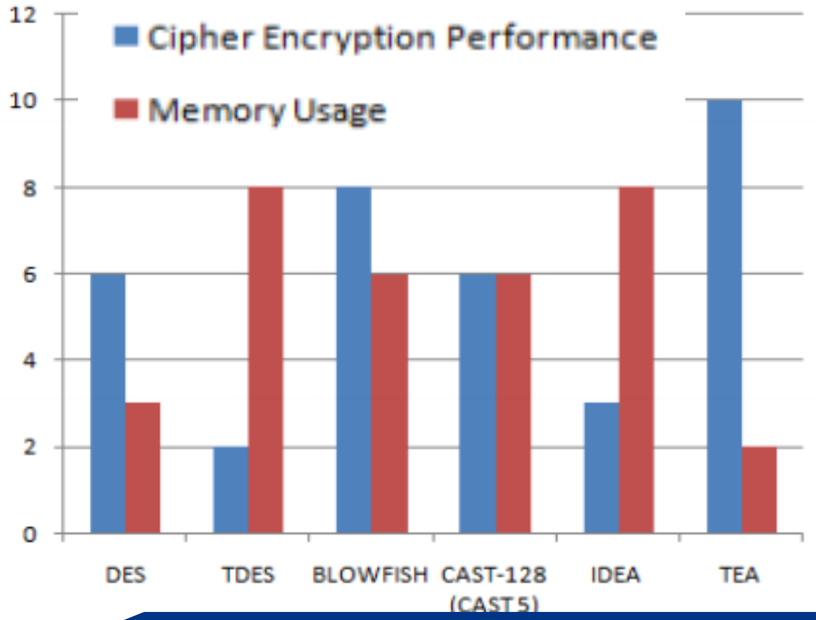
Cipher strength	Score
0 bits (no encryption)	0%
< 128 bits (e.g., 40, 56)	20%
< 256 bits (e.g., 128, 168)	80%
>= 256 bits (e.g., 256)	100%

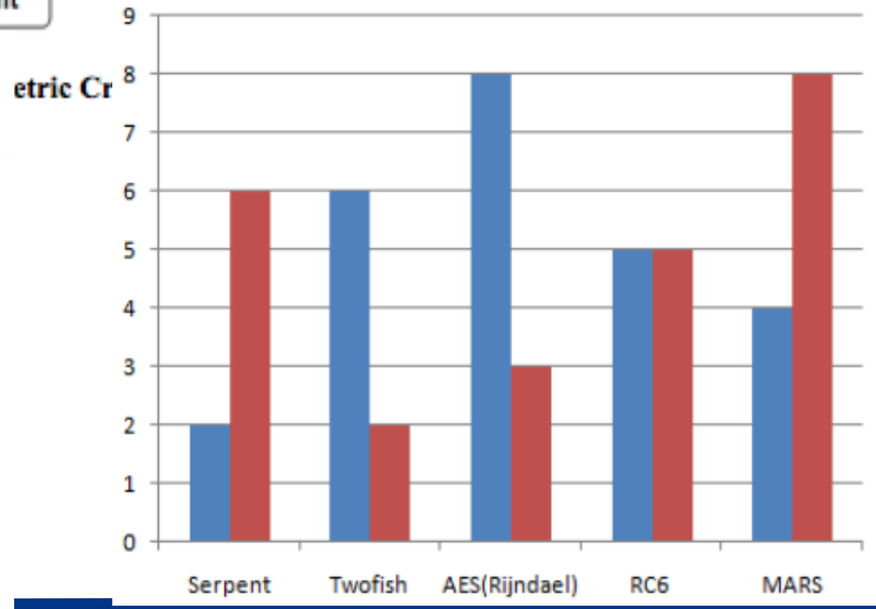
*calculate using mean: 0.5 * (best + worse)*

https://github.com/ssllabs/research/wiki/SSL-Server-Rating-Guide

Example: Symmetric and Asymetric Key Cryptography







some flaws in symmetric algorithms such as
- weak keys
- insecure transmission of secret key,

- speed,
- flexibility,

- authentication and reliability

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 fulfils 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 turnove
- From 2018: General Data Protection Regulation
  - EU-wide harmonisation (adopted by CA, AU, NZ,…)
  - User control
  - More limitations on sending data outside

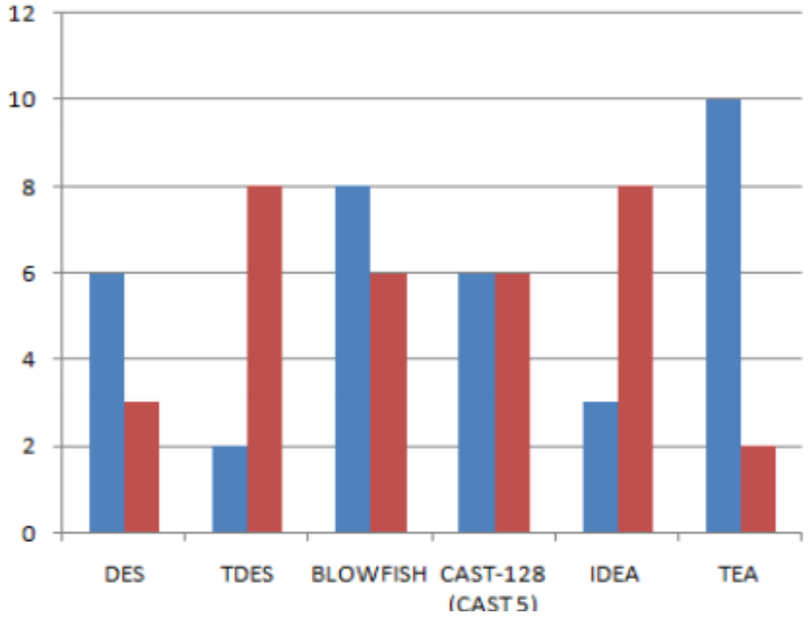
http://www.oecd.org/sti/ieconomy/49710223.pdf

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.

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://redtigersecurity.com/services/scadaics-security-consulting/scada-security-maturity-model/
- Standards for Security Categorization of Federal Information and Information Systems, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf