Systems Security Group | Lancaster University

Security Fundamentals

Learning Objectives

- Revisit basic definitions used in security
- Learn the main security principles
- Learn about threats to security and ways to protect

Common information security targets

The classic top aspects of information security are the preservation of

- **Confidentiality:** ensuring that information is accessible only to those authorised to have access
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods
- **Availability:** ensuring that authorised users have access to information and associated assets when required

Other definitions…

- Anonymity/Untraceability
- Pseudonymity
- Unlinkability
- Copy protection, information flow control
- Data protection/personal data privacy

Aspects of integrity and availability protection

- Rollback
- Authenticity
- Non-repudiation
- Audit

Common questions regarding security

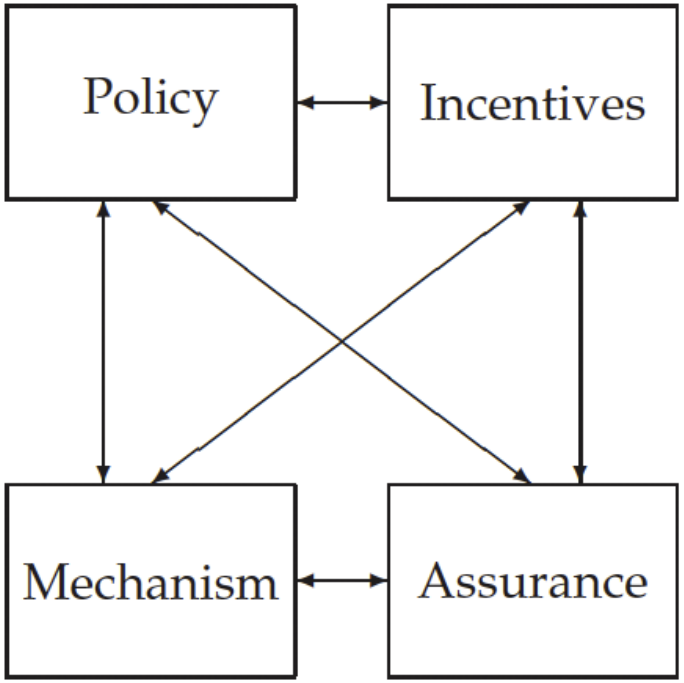
- Is my system secure?
- Factors that affect security
- What's required for an effective protection?

Security engineering

- *'… about building systems to remain dependable in the face of malice, error, or mischance'* [1]

- Focuses on tools, processes and methods
- Why?
  - Design, implement, test systems
- How easy is it?
  - Protect the wrong things…
  - Protect things in the wrong way…

A framework



Security Engineering Analysis Framework [1]

- **Policy:** What you are supposed to achieve
- **Mechanism:** What you assemble to implement the policy
- **Assurance:** Reliance you place on a mechanism
- **Incentive:** Motive for people or attackers to protect or attack a policy

What is a system?

'Simply stated, a system is an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.'

'Ignoring the human components, and thus neglecting usability issues, is one of the largest causes of security failure' [1]

Security principles

- Why do we need them?
- The security principles helps to achieve information security goals
  - Confidentiality, Integrity, Availability
- … most essential principles, regardless of the actual domain…

Simplicity

- *'Keep the design as simple and small as possible' [5]*
- It's easier to understand simple solutions.
- A simple solution may be less likely to have vulnerabilities (compared to a complex solution)
- How about analysing and reviewing the system?

Open design

- *'The design should not be secret'* [5]
- The protection mechanism of a system shouldn't depend on secrecy
- Secrets may be hard to protect…

Compartmentalisation

- Organise resources into isolated groups or similar needs.
- Limit access to information based on tasks
- Have to identify similar needs
  - Object oriented programming

Least privilege

- *'Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.'* – J. Saltzer
- Privileges should be reduced to the absolute minimum
- Subjects of a system should not be granted access to objects other than those needed to complete their job

Trust and trustworthiness

- Trust Vs. Trustworthiness
  - A trusted system may misbehave and not meet the user's expectations
  - A trustworthy system satisfies the user's expectations
- Trust has to be minimised
- Trustworthiness has to be maximised

Fail-safe defaults

- A system should start in and return to a secure default state in case of failure
- A security mechanism can be enabled at system start-up and re-enabled whenever it fails
- It's an important principle in access control
  - Permission is denied unless explicitly granted
    - Whitelist approach

Complete mediation

- *'Every access to every object must be checked for authority'* [5]
- Access to any object must be monitored and controlled
- Ensure that access control mechanisms cannot be bypassed
- Protect sensitive information during transit/in storage, which requires data to be encrypted to achieve complete mediation

No single point of failure

- Build redundant security mechanisms
- Security should not rely on a single mechanism
- Prevent single points of failure
- Also known as defence in depth.

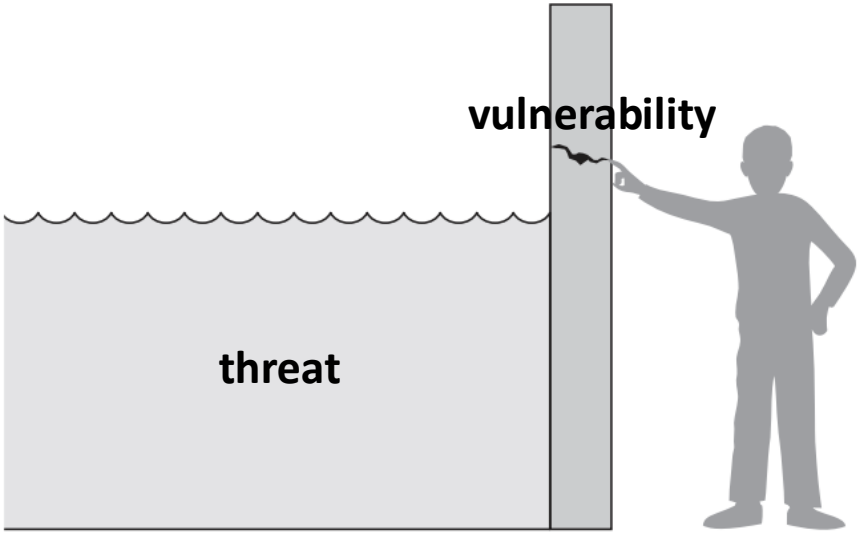
Usability

- Design usable security mechanisms
  - Security mechanisms should be easy to use
- Not only concerned with end users
  - System administrators, auditors, software engineers, etc.
- Security mechanisms should be designed with these users in mind

Threats to security and ways to protect

Vulnerabilities and threats [2]

- A **vulnerability** is a weakness in a system that might be exploited and cause loss or harm
- A **threat** to a system is a set of circumstances having the potential to cause loss or harm



Threats, controls and vulnerabilities[2]

Attacks and control

- The exploitation of a vulnerability perpetrates an **attack** on the system
- **Controls** are protective measures that could address problems

Threats Vs. Controls Vs. Vulnerabilities

'A *threat* is blocked by *control* of a *vulnerability*' [2]

Access controls under attack

- In reality most attacks take place on some type of access control
- What makes it difficult for security professional is that there are several ways for a system to be attacked
- Before securing them, they should be identified

Security issues – Vulnerability analysis

- Look for security issues

- Carry out a vulnerability analysis
  - Look for holes that could be exploited
  - Carried out by scanning systems and identifying missing patches, misconfigured settings, programming code mistakes, etc.

What can go wrong…?

What can go wrong after running a vulnerability scanner and fixing all the issues?

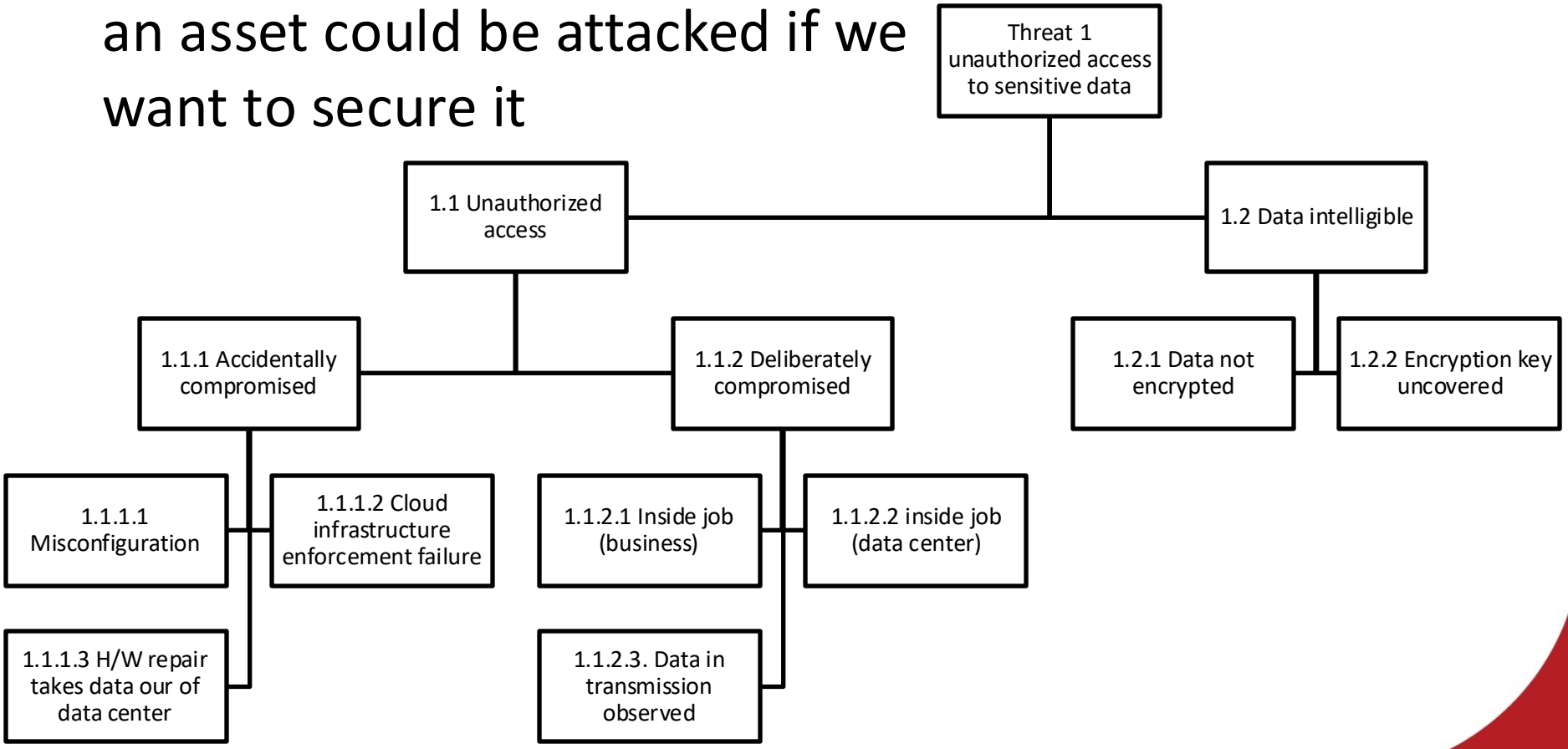
- How is this system connected to other systems?
- Are the sensitive data encrypted while in storage and transit?
- Who has access to this system?
- Can someone steal this system?
- Can someone insert a USB device and extract the data?
- What are the vectors that malware can be installed on the system?
- Is the system protected in the case of a disaster?
- Are there any access channels that are not auditable?

Threat modelling

- Threat modelling is a structured approach to identify potential threats that could exploit vulnerabilities
- Who would likely want to attack us?
- How could they successfully do this?
- Looks outward and try to figure out all the ways a structure could be attacked.

What has to be done?

Have to think about all the ways an asset could be attacked if we want to secure it

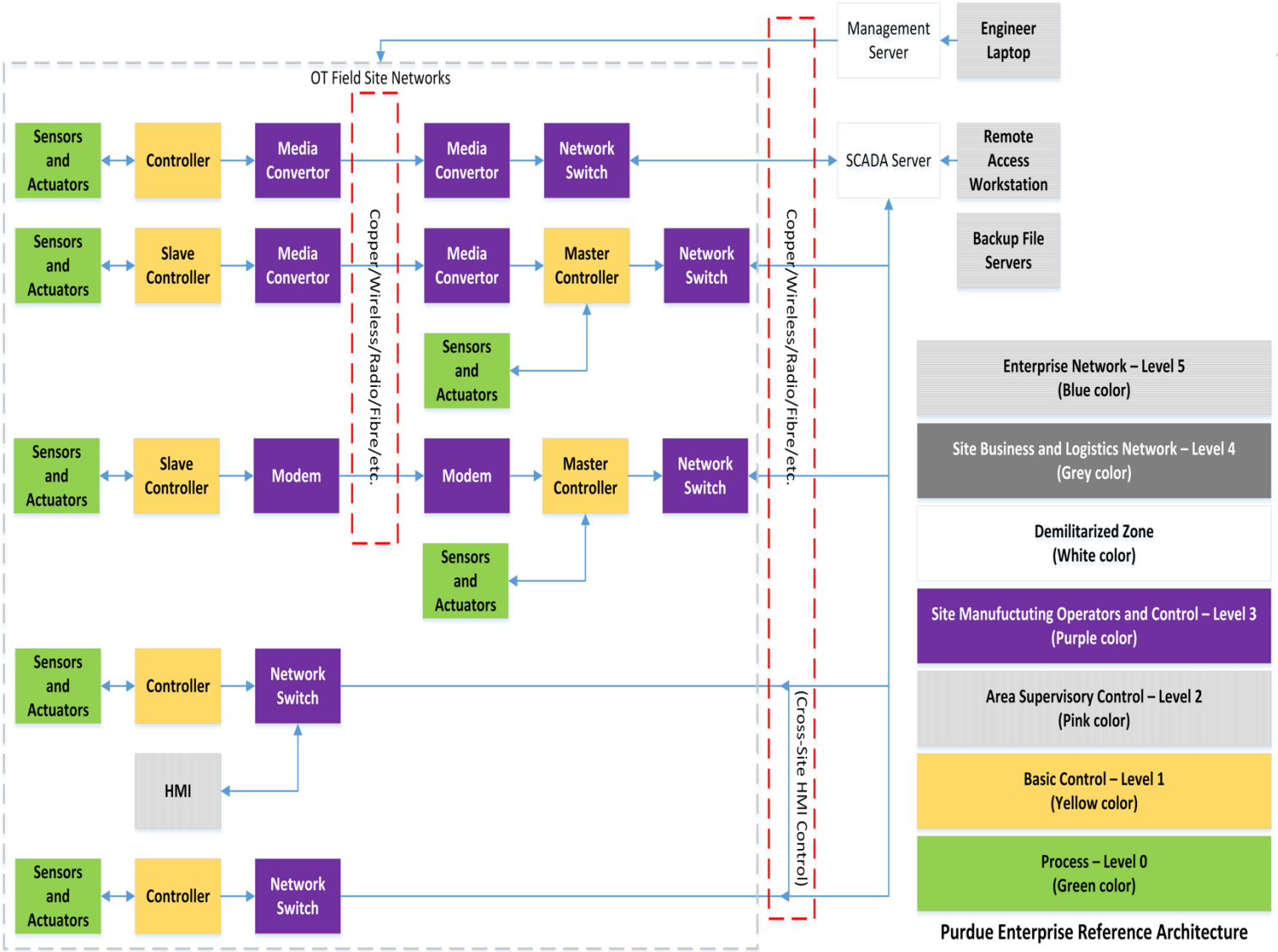


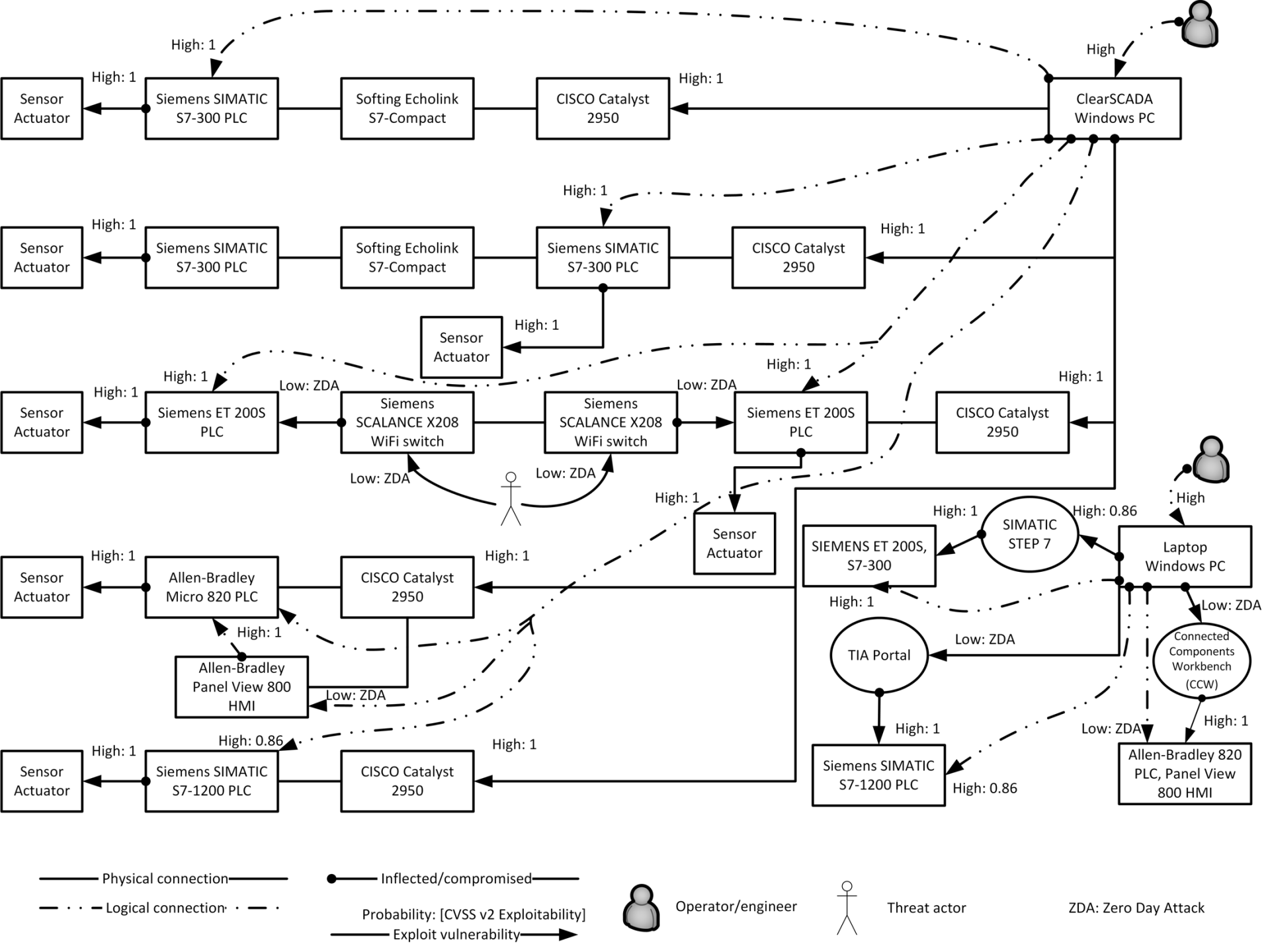
Security policies

- Security requirement analysis
  - Identify assets and their values
  - Identify vulnerabilities, threats and risk priorities
  - Identify legal and contractual requirements
- Define security policies
- Security policy document
- Selection and implementation of controls

Markus Kuhn, Introduction to security,
https://www.cl.cam.ac.uk/teaching/0708/IntroSec/slides.pdf

Identify assets and values




Sensor Actuator
Siemens SIMATIC S7-300 PLC
Softing Echolink S7-Compact
CISCO Catalyst 2950
ClearSCADA Windows PC
Siemens ET 200S PLC
Siemens SCALANCE X208 WiFi switch
Allen-Bradley Micro 820 PLC
Allen-Bradley Panel View 800 HMI
Siemens SIMATIC S7-1200 PLC
SIEMENS ET 200S, S7-300
SIMATIC STEP 7
Laptop Windows PC
TIA Portal
Connected Components Workbench (CCW)
Allen-Bradley 820 PLC, Panel View 800 HMI
High: 1
High: 0.86
Low: ZDA
High
Physical connection
Logical connection
Inflected/compromised
Probability: [CVSS v2 Exploitability]
Exploit vulnerability
Operator/engineer
Threat actor
ZDA: Zero Day Attack

Example: Risk identification and vulnerabilities

- Examples of threats on main assets
  - Radio jamming/data manipulation
  - Becoming an HMI
  - Backup server
  - …
- Examples of vulnerabilities
  - ClearSCADA server: CVE-2014-5411, CVE-2014-5412, CVE-2014-5413
  - Network switches: CVE-2001-0895, CVE-2014-5412
  - Controllers: Siemens SIMATIC S7-300 , S7-1200, ET 200S PLC, …
  - Management server: SIMATIC STEP 7, Connecter Components Workbench, TIA Portal, …

Gouglidis, Antonios and König, Sandra and Green, Benjamin and Rossegger, Karl and Hutchison, David (2018) *Protecting Water Utility Networks from Advanced Persistent Threats : A Case Study.* In: Game Theory for Security and Risk Management : From Theory to Practice. Static & Dynamic Game Theory: Foundations and Applications . Springer Birkhäuser, Basel.

Define suitable security policies

- The security requirements identified can be complex and may have to be abstracted first into high-level security policy

- A set of rules that clarifies which are and are not authorised, required, and prohibited activities, states and information flows

Markus Kuhn, Introduction to security,
https://www.cl.cam.ac.uk/teaching/0708/IntroSec/slides.pdf

Security policy document

- Understand what exactly security means for an organisation and what needs to be protected or enforced.
- Document high-level security policies as a reference for anyone involved in implementing controls
- Lay out the overall objectives, principles, and the underlying threat model that are to guide the choice of mechanisms in the next step.

Markus Kuhn, Introduction to security,
https://www.cl.cam.ac.uk/teaching/0708/IntroSec/slides.pdf

Selection and implementation of controls

- Issues addressed in a typical low-level organisation security policy
  - General (affecting everyone) and specific responsibilities for security
  - Name manager who ‘owns’ the overall policy and is in charge of its continued enforcement, maintenance, review, and evaluation of effectiveness
  - Name individual managers who ‘own’ individual information assets and are responsible for their day-to-day security
  - Reporting responsibilities for security incidents, vulnerabilities, software malfunctions

Markus Kuhn, Introduction to security,
https://www.cl.cam.ac.uk/teaching/0708/IntroSec/slides.pdf

… continued

- Mechanism for learning from incidents
- User training, documentation, and revision of procedures
- Physical security
  - Authorisation procedure for removal of property
  - Clear desk policy
  - Define security perimeter
  - …
- …

Markus Kuhn, Introduction to security,
https://www.cl.cam.ac.uk/teaching/0708/IntroSec/slides.pdf

Questions?

References

[1] *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Edition, By Ross Anderson, Chapter ,1 https://www.cl.cam.ac.uk/~rja14/book.html
[2] *Security in Computing*, 5th Edition, By Charles P. Pfleeger, Shari Lawrence Pfleeger, Prentice Hall, Chapter 1, https://ptgmedia.pearsoncmg.com/images/9780134085043/samplepages/9780134085043.pdf
[3] *All In One – CISSP Exam Guide*, 5th Edition by Shon Harris. ISBN 978-0-07-160217-4
[4] *Systems Engineering Fundamentals*, DoD, January 2001, https://ocw.mit.edu/courses/aeronautics-and-astronautics/16-885j-aircraft-systems-engineering-fall-2005/readings/sefguide_01_01.pdf
[5] The Protection of Information in Computer Systems, J. Saltzer and M. Schroeder, Proceedings of the IEEE, Vol. 63, No. 9, September 1975.
[6] William Stallings, Network and Internetwork Security: Principles and Practice. Englewood Cliffs, NJ: Prentice-Hall International, 1999.
[7] British Standard 7799 “Code of practice for information security management”
[8] German Information Security Agency’s “IT Baseline Protection Manual” http://www.bsi.bund.de/gshb/english/etc/
[9] US DoD National Computer Security Center Rainbow Series, for military policy guidelines http://www.radium.ncsc.mil/tpep/library/rainbow/