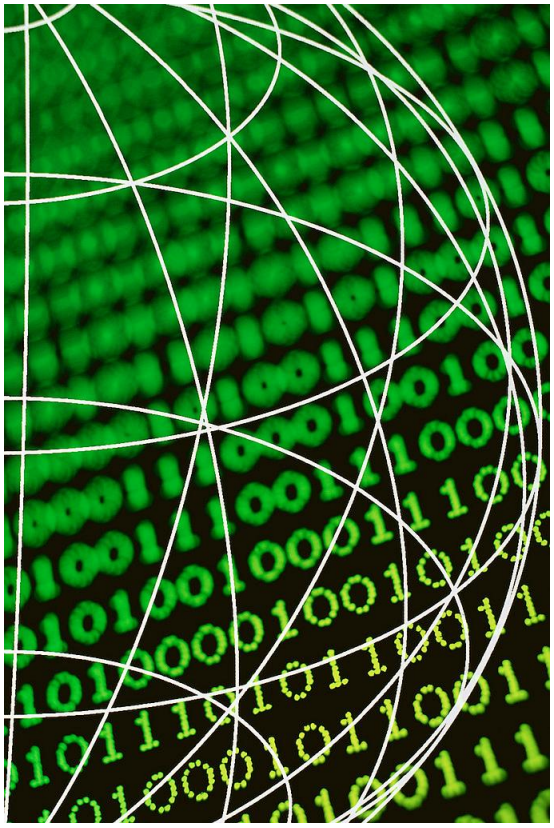
Measuring Information Security

Reijo Savola, VTT Technical Research Centre of Finland

IPLU Workshop, May 18, 2006

Contents

- Introduction: Measuring Information Security
- Key Concepts
- Use of Measurements
- Definition of Security Metrics
- Discussion
- Conclusions



Measuring information security

Measurements vs. Metrics

Measurements

- a one-time view of specific measurable parameters

Metrics

- measurements over time
- means of interpretation for the collected data

"An activity cannot be managed well if it cannot be measured."

Introduction

Key Concepts: Security Requirements, Measurement Methods and the Objects of Measurement

Security Requirements

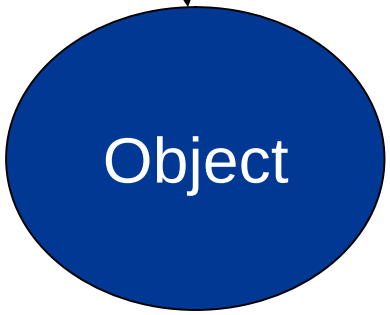
Measurement methods

Object can be e.g.:

- *Organisation*
- *Product*
- *Technical system*

(e.g. a certain IP network)

- *Human behaviour, or*
- *SECURITY AS A WHOLE*



Introduction

Security Requirements – the Core of Measurements

Basis

- security risk analysis (threats, probabilities, impacts)
- knowledge about technological selections,
- vulnerabilities
- use scenarios
- quality attributes

> Security Requirements

References

- Security requirements, e.g. Common Criteria (CC)
- Best practices,
- Security base lines,
- Maturity models like SSE-CMM.

Common Criteria

SSE-CMM
SYSTEMS SECURITY ENGINEERING - CAPABILITY MATURITY MODEL

Key Concepts

Security Requirements are based on Security and Dependability Main Attributes

Dependability

- Confidentiality
- Integrity
- Availability
- Reliability
- Safety
- Maintainability

Information Security

- Confidentiality
- Integrity
- Availability
- (Non-repudiation)
- (Authenticity)

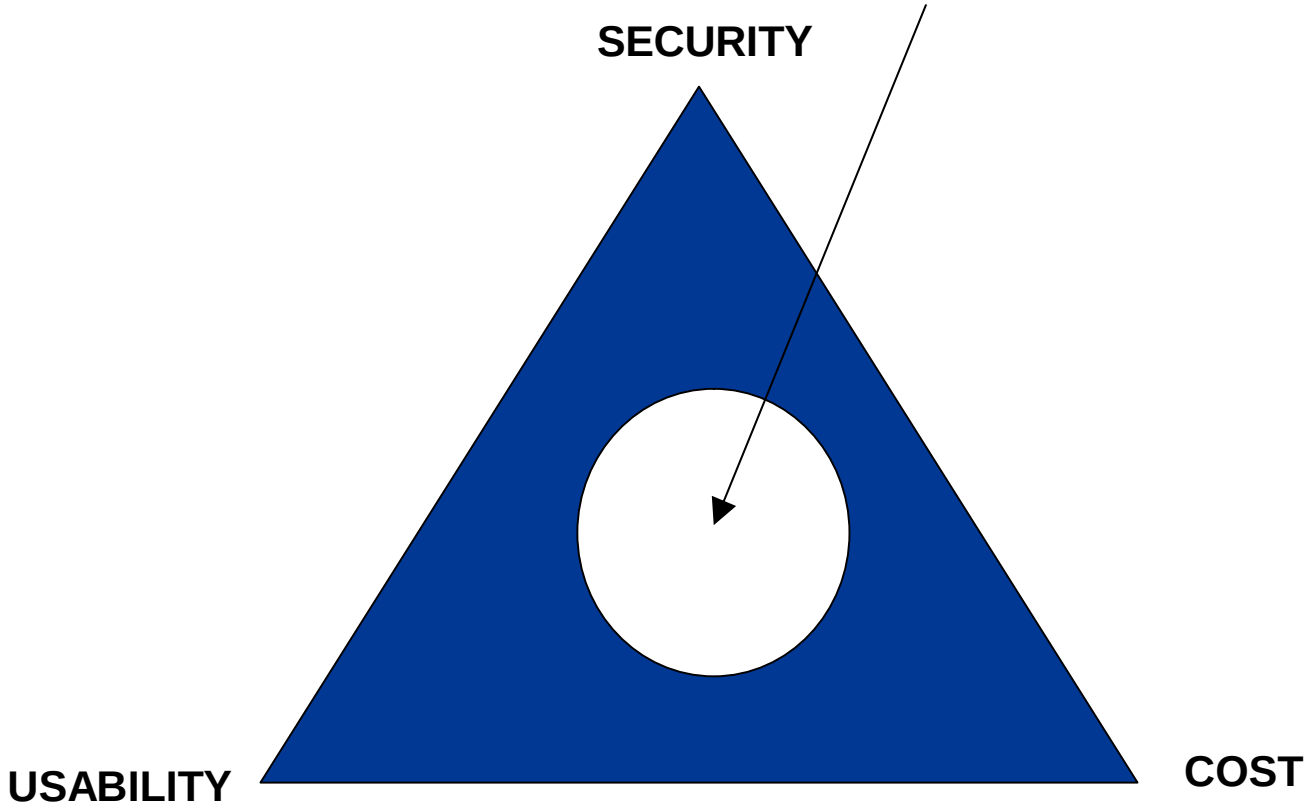
Dimensions of Attributes

- **Probability [0,1]**
- **Impact [-1,+1]**

$$I = \sum_{t=0}^{T} w_t \cdot p(a_r, v)_t \cdot i(a_r, u)_t$$

Key Concepts

Goal? Desired / Adequate level of Security.



Key Concepts

Methods of Measurement

Methods of Measurement:

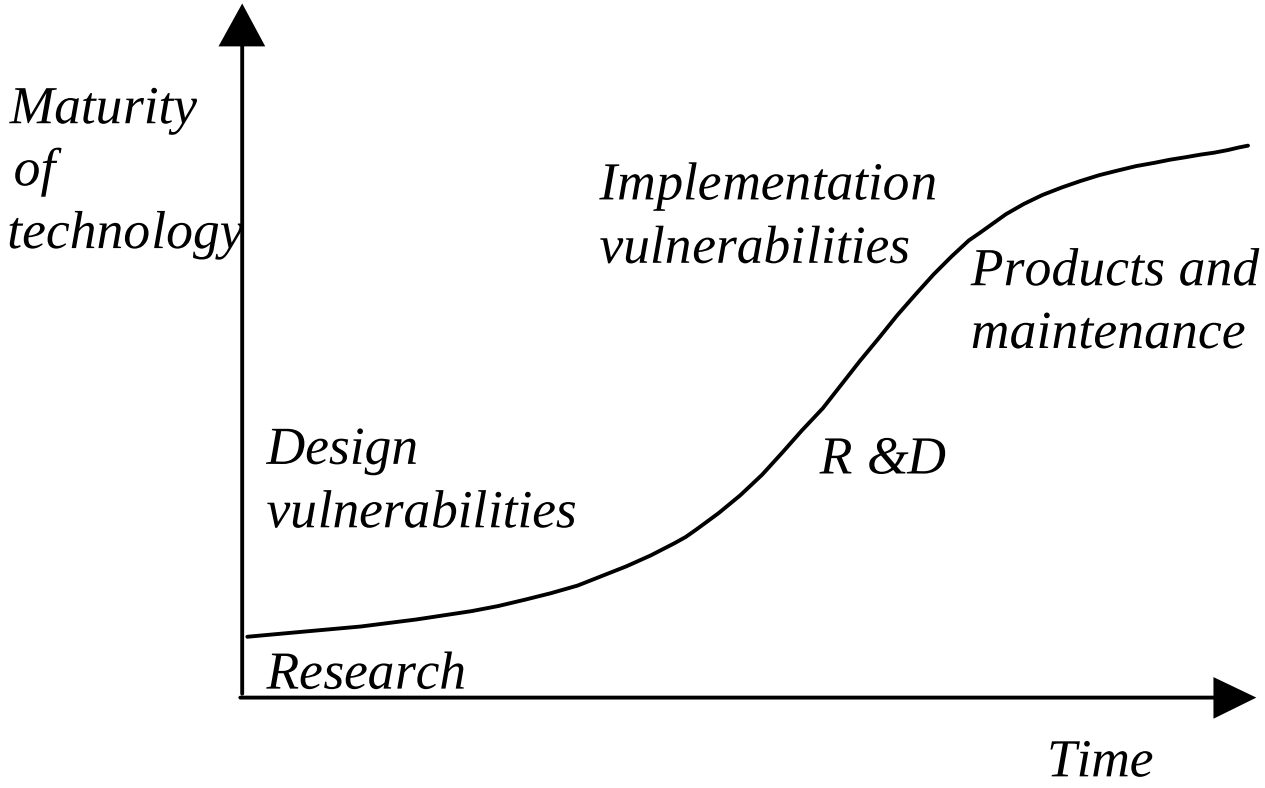
- Risk analysis
- Certification or auditing
- Measures of the intrusion process
- Observation of system security performance
- Testing (tiger teams etc.)
- Analytical model-based methods

Industrial practices, information for research

R&D

Key Concepts

Effect of Technological Maturity in Products to the Selection of Security Metrics



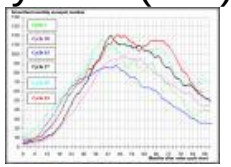
Key Concepts

Use of Technical Security Metrics

Technical security metrics can be applied in, e.g.

Goal establishment: to establish goal and measure how well the object achieves the goal

Prediction: to predict security level before implementation or in an implemented system, to predict possible intrusion using an Intrusion Prevention System (IPS)



Comparison: to compare the security level of objects

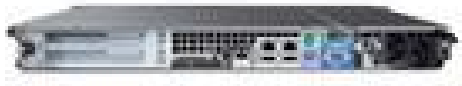
Monitoring: to monitor or scan the security level of an object (e.g. Intrusion Detection System IDS)

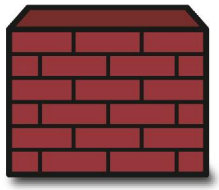
Enabling analysis: in the case of fault injection methods metrics enable analysis.

Use of Measurements

Examples of Technical Equipment and Software for Industrial Security Measurements

- IDS/IPS (Intrusion Detection and Prevention Systems)
- Other kinds of Network Security Monitoring devices
- Antivirus systems
- Antispyware systems
- Firewalls



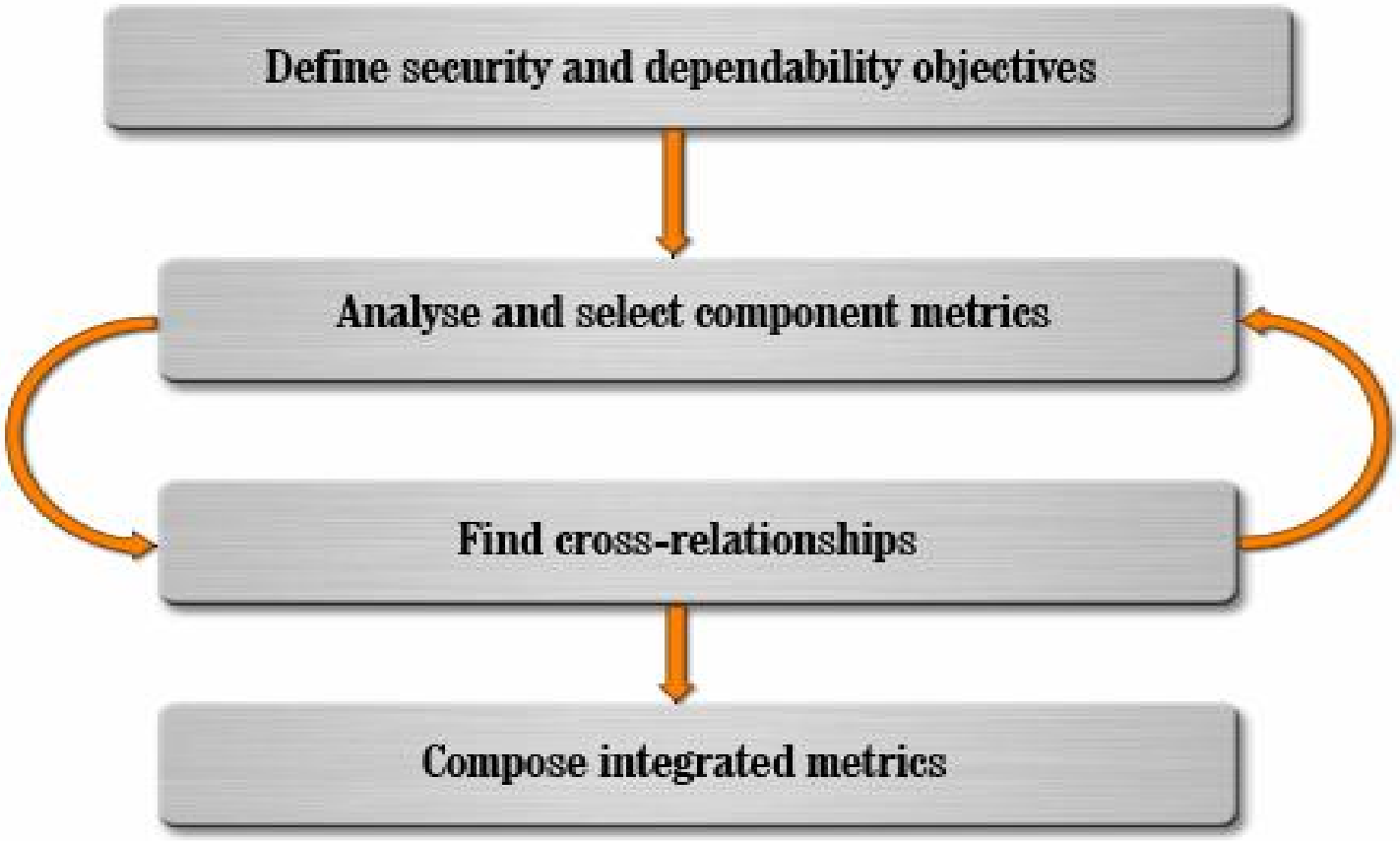


All of them generate measurement results – technical logs

The trend: **Beyond IDS ?**

Use of Measurements

A Compositional Approach to Define Security Metrics



Definition of Security Metrics

Some Examples of Security Metrics

Some examples of security metrics

Technical metrics

- Cryptographic strength
- Mean time to attack
- Anomaly detection (IDS/IPS)
- Attack tree probabilities
- Software engineering metrics

Quality and business oriented metrics

- Product quality and general quality m
- ROI (return of invest)
- Business process metrics

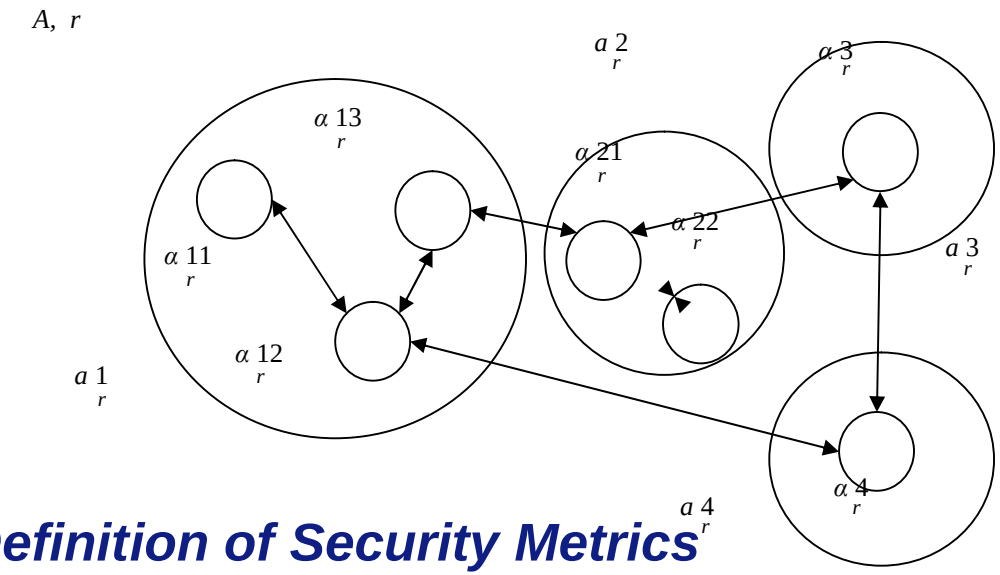
Process oriented / audit metrics

- Interview techniques
- Security audit metrics
- Capability model metrics

Definition of Security Metrics

A Model-Based Approach*

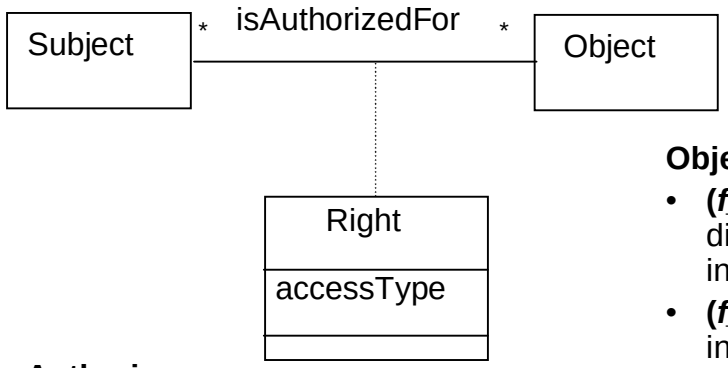
- The security behaviour of the system could be modelled e.g. using *atomic security actions* and their cross-relationships.
- Each atomic action has *probability* and *impact* -- an effect to a security requirement (e.g. confidentiality)



Definition of Security Metrics

*Savola R and Röning J.: *Towards Security Evaluation based on Evidence Collection and Impact Analysis*. To appear in the Proc. Of Workshop of Empirical Evaluation of Dependability and Security (WEEDS) 2006, June 28, 2006, Philadelphia, PA, 6 p.

A Model-Based Approach: Example of Security Actions



Subject:

- (***req1***) request from an authenticated process authorized to access the file,
- (***req2***) request from an authenticated process not authorized to access the file,
- (***req3***) request from an impersonating process that has been able to go through the authentication,
- (***req4***) request from an unauthenticated process authorized to access the file, and
- (***req5***) request from an unauthenticated process not authorized to access the file.

Authorizer:

- (***check_read_right***) check the read right of the process requesting a read access,
- (***authorize_req***) authorize the process to read from the file,
- (***not_authorize_req***) forbid the process to read from the file,
- (***upd_rd_r***) update read rights, and
- (***authenticate_right_change***) authenticate the party asking for right change.

Object:

- (***f_access1***) access to a file with no directly or indirectly confidential information,
- (***f_access2***) access to a file with indirectly confidential but no directly confidential,
- (***f_access3***) access to a file with directly confidential but no indirectly confidential information, and
- (***f_access4***) access to a file with directly and indirectly confidential information.

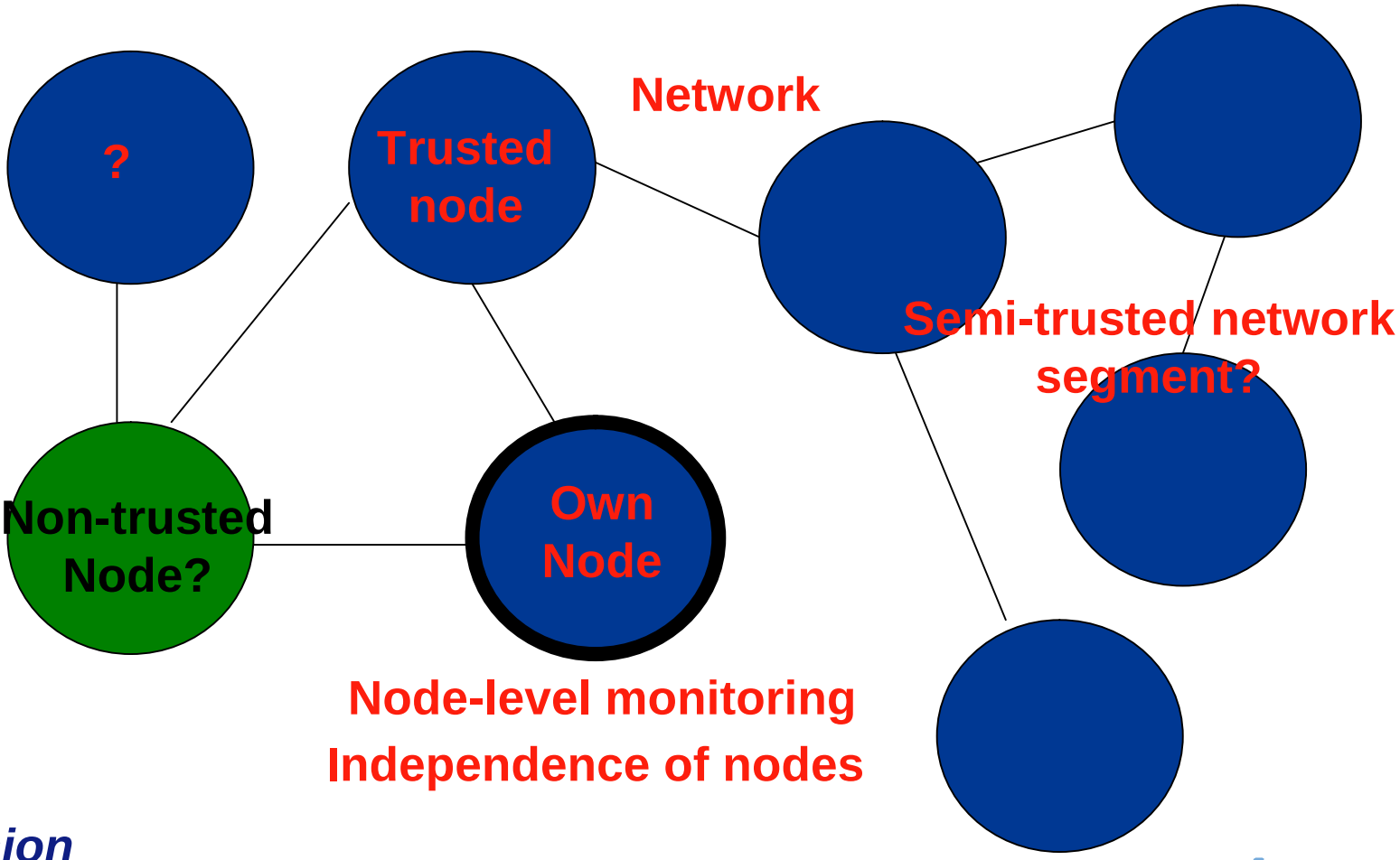
Definition of Security Metrics

Security Evaluation Process

- **Risk and threat analysis**. Carry out risk and threat analysis of the system and its use environment if not carried out before. These are lacking in many practical systems.
- **Define and prioritize security requirements** in a way that they can be compared with the security actions of the system. Based on the threat analysis, define the security requirements for the system, if not yet defined. The most critical and security requirements should be paid the most attention. Remember that the weakest links of the system are critical too.
- **Model the security behaviour.** Based on the prioritized security requirements, identify the functionality of the system that forms the security actions and their dependencies in a priority order.
- **Gather evidence** from measured, reputation and tacit security information. Use suitable evidence collection tools like vulnerability identification and assessment tools.
- **Estimate the probabilities and impacts of security actions** based on the evidence. Aggregate the results to form a clear picture of whether or not the system fulfils the security requirements.

Definition of Security Metrics

Responsibility of Security in Self-Organizing networks?



Discussion

Conclusions

- Measuring security includes: security requirements, measuring method and the object to be measured
- It is very challenging to try to measure security (or dependability) solely based on general quality attribute information – tailored security or dependability requirements are required
- Metrics used might be different depending on the technological maturity
- Compositional, iterative methods can be used to define an aggregate metrics framework
- Analytical model-based methods can be used to construct security requirements and define security metrics based on them.

Conclusions

Kiitoksia! Thank you!

REIJO SAVOLA

Network and Information Security
Research Coordinator

Tel. +358 20 722 2138

GSM +358 40 569 6380

Fax +358 20 722 2320

Email Reijo.Savola@vtt.fi

VTT TECHNICAL RESEARCH CENTRE OF FINLAND
Network and Information Security Research Coordination Group
Kaitoväylä 1, Oulu, FINLAND
PL 1100, 90571 Oulu, FINLAND
www.vtt.fi