Assessment of IT Security in Networked Information Systems

Jonas Hallberg and Amund Hunstad

Dept. of Systems Development and IT security
Swedish Defence Research Agency (FOI)

www.itsecurity.foi.se/dfs
jonas.hallberg@foi.se

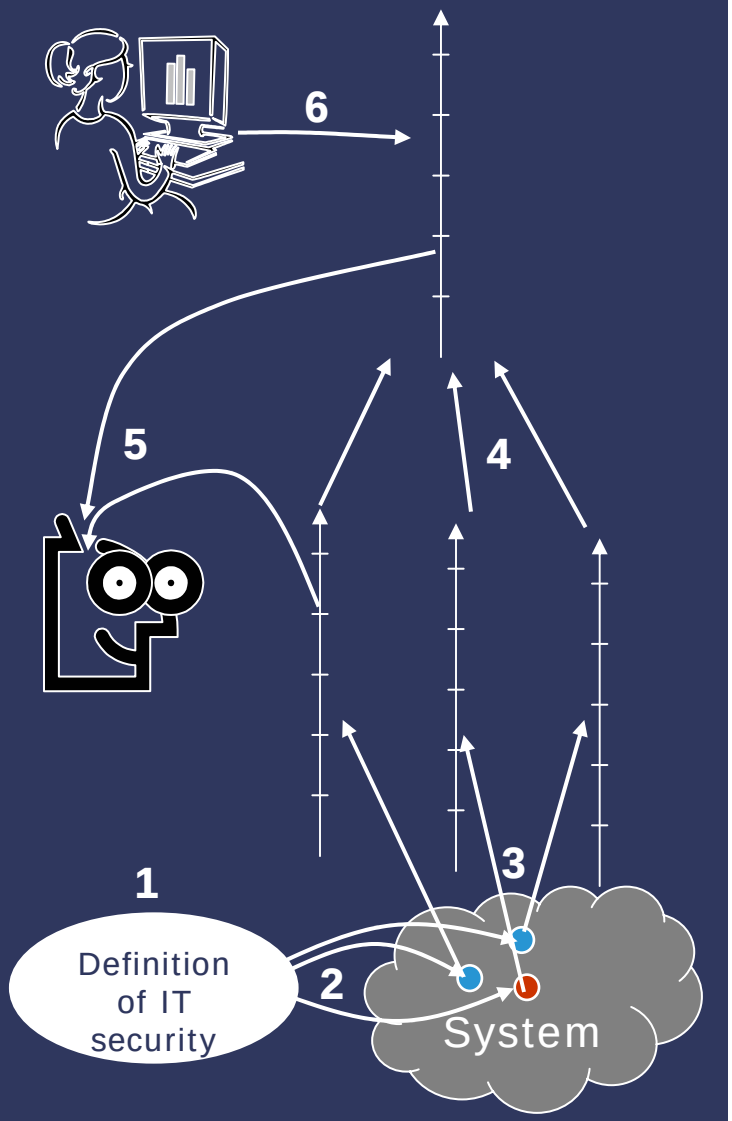
FOI

Security assessment

- Assessment process outline
  1. Define IT security
  2. Transform definition of IT security into measurable entities
  3. Measure selected entities
  4. Combine basic values into compound values
  5. Interpret values
  6. Establish user needs

Security metrics

Security metrics



Security metrics are the basis for assessment

FOI

How to find basic security metrics?

Possible approaches:

- Start from high-level security attributes, e.g. CIA
- Use set of security-relevant system properties, e.g. based on CC SFRs
- …

FOI

How to combine security metrics?

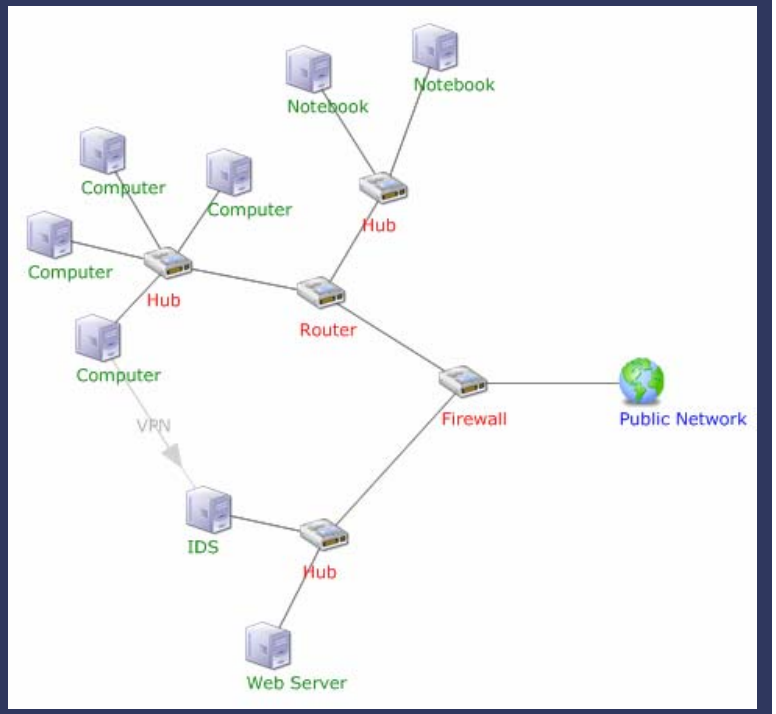
- One approach is to use Analytic hierarchy process to combine values
- Is this approach viable?

Security property	# low-level properties	Example	Value for gen. comp.
access control	20	Users uniquely identified	0.62
security logging	12	Correct time	0.615
protection against intrusions	17	Administration solemnly by authorized personnel	0.564
intrusion detection	12	Automatic detection of violation of specified rules	0
protection against malware	16	Block malware accessing system resources	0.554

FOI

MASS – systems modeling

- Systems are modeled as interconnected components
  - Two main classes of components:
    1. Traffic generators, e.g. PCs and PDAs
    2. Traffic mediators, e.g. firewalls and hubs
  - Two types of relations:
    1. Physical, e.g. network and IR connections
    2. Logical, e.g. node dependencies and trust relationships
- The abstraction level is not fixed
- Hierarchical models are supported

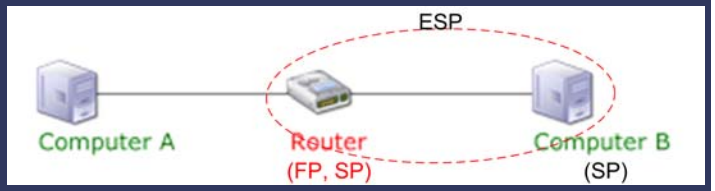


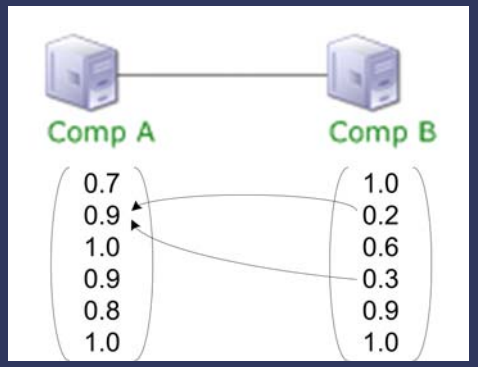
FOI

MASS – security values

- Component profiles
  - Security profiles are sets of *security features* with corresponding *elementary security values* from 0 to 1
  - Filtering profiles describes the ability of traffic mediators to block malicious traffic
- Component relations
  - Inter-component relations are modeled with a set of functions, e.g. min, max, and average
- System-dependent security profiles
  - calculated for each component based on component security profiles and relations
- System security values
  - based on the system-dependent security profiles

$$\begin{pmatrix} \text{Audit} \\ \text{Access Control} \\ \text{Authentication} \end{pmatrix} = \begin{pmatrix} 0.8 \\ 0.5 \\ 0.7 \end{pmatrix}$$





FOI