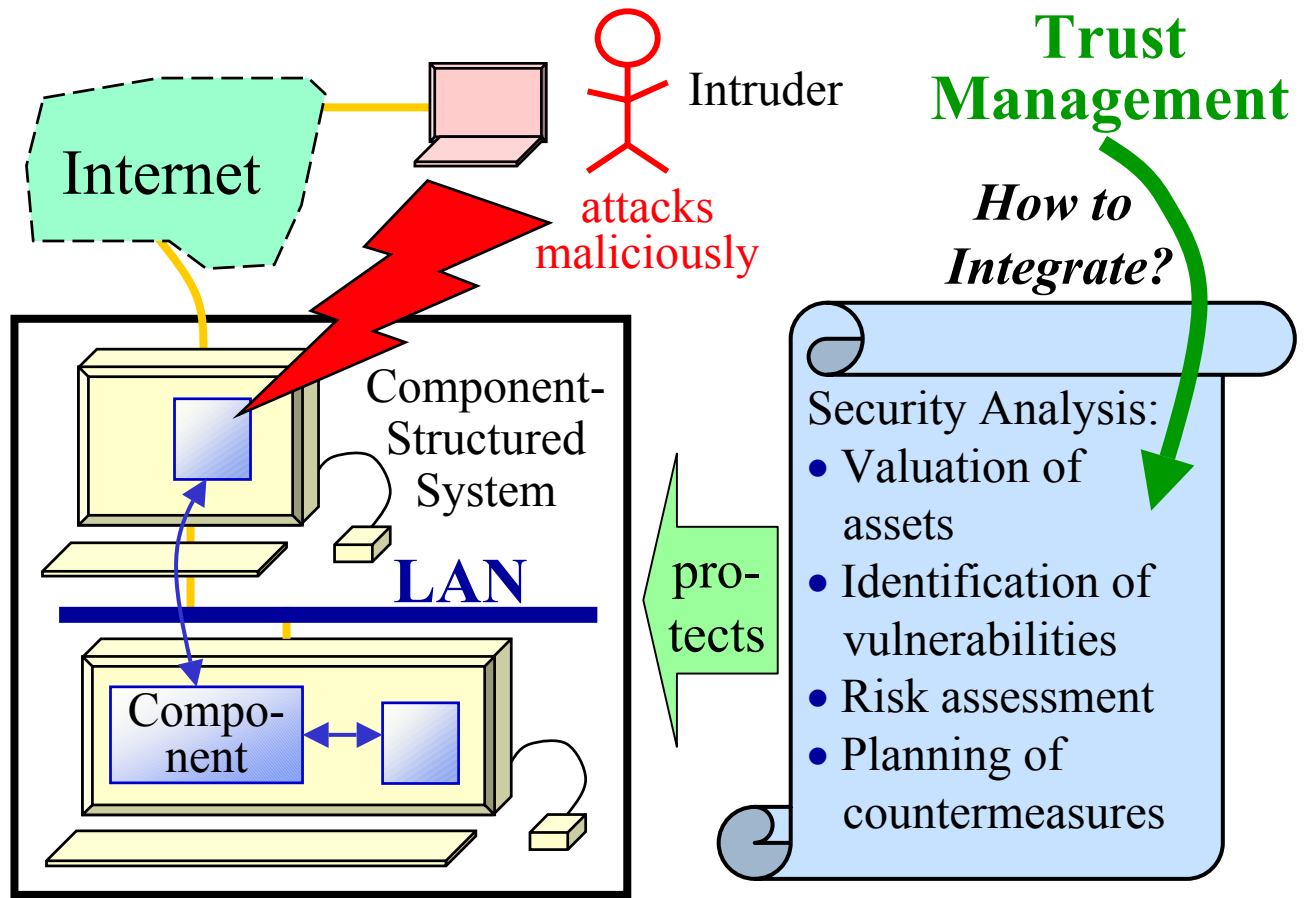




How to Integrate Trust Management into a Risk Analysis Process



*Peter Herrmann,
RvS, Informatik IV
Universität Dortmund*

Contents:

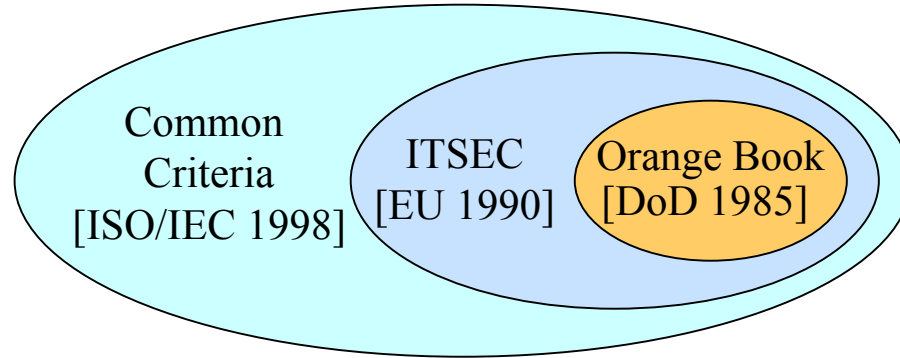
- ◆ Security Analysis
- ◆ Trust Modeling
- ◆ Integration of Trust Values
(Two approaches)



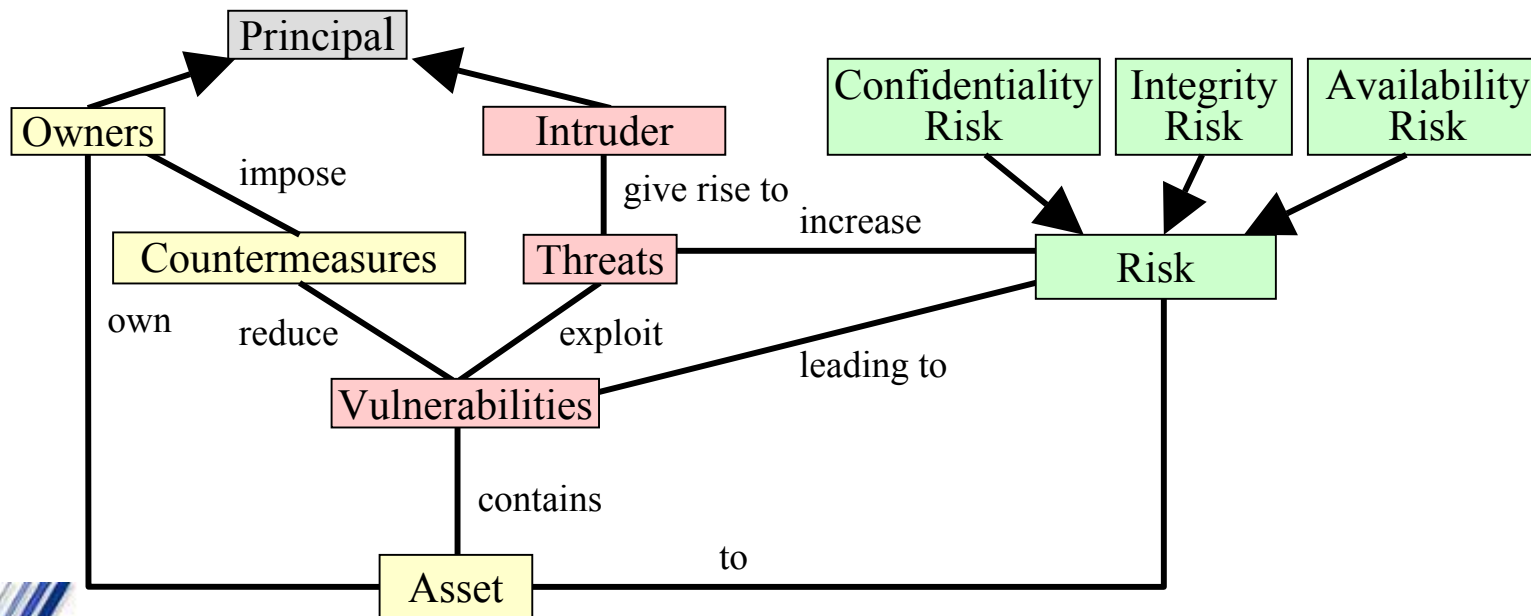


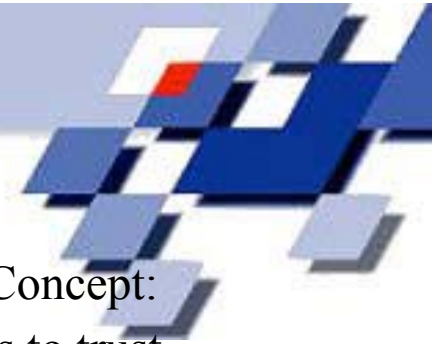
Security Analysis

- ◆ Standards:



- ◆ Common Criteria: Security classes and associations





Security Analysis

Phases:

- ◆ Identification of the system and its assets
- ◆ Valuation of the assets
 - security levels
- ◆ Identification of vulnerabilities and threats
- ◆ Valuation of vulnerabilities and threats
- ◆ Assessment of risks on assets
 - depending on security levels and misuse likelihoods
 - stop, if all risks are bearable
- ◆ Planning and design of countermeasures
- ◆ Analysis of the extended system
 - countermeasures are also vulnerable



Common Criteria Trust Concept:

- ◆ Owner of an asset has to trust countermeasures built up by audits
- ➔ concept is insufficient since it does not concentrate on parts of the audited system!

Potentially Trusted System Parts:

- ◆ Principals with access to an asset
 - all principals may be benevolent
- ◆ Asset itself
 - free of vulnerabilities
- ◆ Countermeasures
 - sufficient protection
 - immune against attacks on itself

➔ Reduction of the analysis process by considering trust in system parts

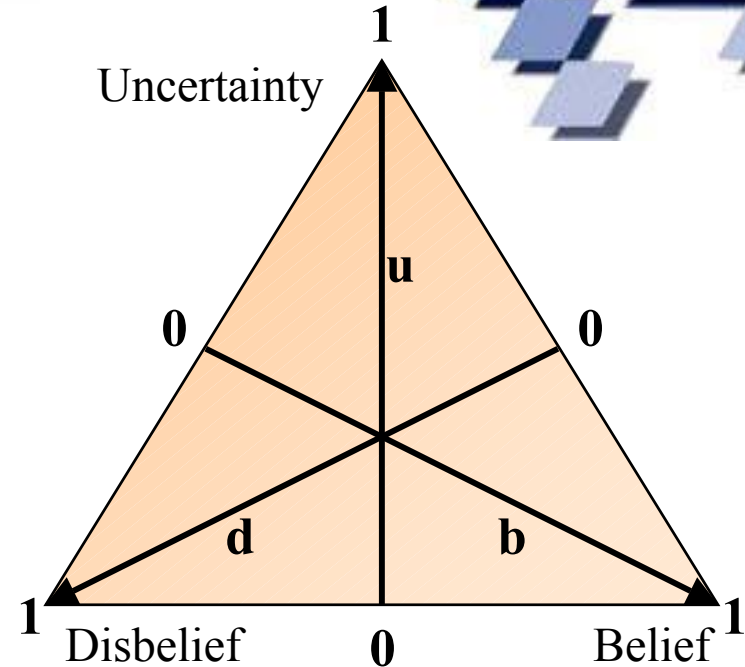




Trust Modeling

- ◆ Trust values:
 - Interval [0,1]
 - Triple <b, d, u>
 - b: belief
 - d: disbelief
 - u: uncertainty
 - ➔ $b + d + u = 1$
- ◆ Trust value determination:
 - Calculation from the number of
 - positive experiences p
 - negative experiences n
 - Metrics:
 - Jøsang, Knapskog: liberal philosophy
 - Beth, Borchering, Klein: unforgiving philosophy

◆ Opinion triangle (Jøsang)



◆ Metric of Jøsang, Knapskog:

$$b = \frac{p}{p+n+1} \quad d = \frac{n}{p+n+1} \quad u = \frac{1}{p+n+1}$$

◆ Metric of Beth, Borchering, Klein:

$$b = \begin{cases} 1 - \alpha^p; & n = 0 \\ 0; & n > 0 \end{cases}$$





Integration of Trust Values

Adaption of the risk level computation:

- ◆ Risk levels depend on security levels, misuse likelihoods, and trust values
 - ➔ as higher the belief value b is, as lower the computed risk level will be!

Misuse Likelihood	max	high	mod	low	no
Security Level					
max	max	max	high	mod	no
high	max	high	mod	low	no
mod	high	mod	low	low	no
low	mod	low	low	no	no
no	no	no	no	no	no

$b \leq 0.999$

Misuse Likelihood	max	high	mod	low	no
Security Level					
max	max	high	mod	low	no
high	high	mod	low	no	no
mod	mod	low	low	no	no
low	low	low	no	no	no
no	no	no	no	no	no

$b > 0.999$

- ◆ Disadvantage:
 - Perceived risks instead of real risks as intended by the CC

Phases:

- ◆ Identification of the system and its assets
- ◆ Valuation of the assets
 - security levels
- ◆ Identification of vulnerabilities and threats
- ◆ Valuation of vulnerabilities and threats
- ◆ Assessment of risks on assets
 - depending on security levels and misuse likelihoods
 - stop, if all risks are bearable
- ◆ Planning and design of countermeasures
- ◆ Analysis of the extended system
 - countermeasures are also vulnerable





Integration of Trust Values

Decision about bearable risks based on trust values:

- ◆ Valuation of the risks considers current trust values
 - as higher the belief value b is, as higher the level of a bearable risk will be!
- ◆ Example mapping:
 - if $b \leq 0.999$, we will accept a low confidentiality risk
 - if $b > 0.999$, we will also accept a moderate confidentiality risk
- ◆ Disadvantage:
 - Selection of risk acceptance policy should only depend on the preference and personality of the asset owner and not on statistical parameters!

Phases:

- ◆ Identification of the system and its assets
- ◆ Valuation of the assets
 - security levels
- ◆ Identification of vulnerabilities and threats
- ◆ Valuation of vulnerabilities and threats
- ◆ Assessment of risks on assets
 - depending on security levels and misuse likelihoods
 - stop, if all risks are bearable
- ◆ Planning and design of countermeasures
- ◆ Analysis of the extended system
 - countermeasures are also vulnerable

