Non-technical parts of security

Security is the lack of insecurity!

But how do we measure security?

I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it;

but when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind;

it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be.

Lord Kelvin, May 3, 1883, lecture on "Electrical Units of Measurement"
(*Popular Lectures*, Vol. 1, page 73)

Measurements – Requirements

- Operations of measurement involve **collecting and recording data** from observation
- It means **identifying the class of entities** to which the measurement relates
- Measurements must be **independent of the views** and preferences of the measurerer
- Measurements **must not be corrupted** by an incidental, unrecorded circumstance, which might influence the outcome

Measurements – Meaningfulness

- **Meaningfulness** means that the scale measurement should be appropriate to the type of property measured, such that once measurement has been performed – and data expressed on some scale - sensible conclusions can be drawn from it
  - Example 1:
    "point A is twice as far as point B"

    meaningless: distance is a ratio scale, but position is not
  - Example 2:
    "point A is twice as far from point X as point B

    meaningful: distance is a ratio scale

Measurements -- Scales

Nominal scale	denotes membership of a class for purposes such as labelling or color matching
Ordinal scale	when measurement expresses comparative judgement
Interval scale	when measuring ”distance” between pairs of items of a class according to the chosen attribute
Ratio scale	denotes the degree in relation to a standard, i.e. a ratio. It must preserve the origin.
Absolute scale	used for counting the number of elements in an entity set

Security?

- Security is **not well-defined**. There are different interpretations in different areas
  - CIA-model
  - Absence of vulnerabilities (rather than presence of “security”)
  - Set of “authorized” and “unauthorized” states (policy)
    - secure as long as only transitions to authorized states
  - Is Adam’s password secure?
    - Long enough? Complex enough? Not related to personal details?
    - → secure enough as long as password guessers cannot crack it

Methods for measuring security

- Evaluation/Certification (according to some standard)
  - Common Criteria
- Risk Analysis
  - Estimate probability of certain events, consequences and their costs
- Penetration tests
  - Find vulnerabilities using red teams
  - What does it mean if a team does not find anything?
- Vulnerability assessments
  - Fuzzers, scanners, etc.
- Effort-based
  - How much effort is required to break system
- Weakest adversary
  - Weakest adv to break system
- Mean-Time-To-Compromise
  - Borrowed from reliability
- Cryptographic strength
  - “computational efforts”
- Privacy-measures
  - leaking personal information
- Fault trees, worst case analysis, …

A selection of different methods

CVSS

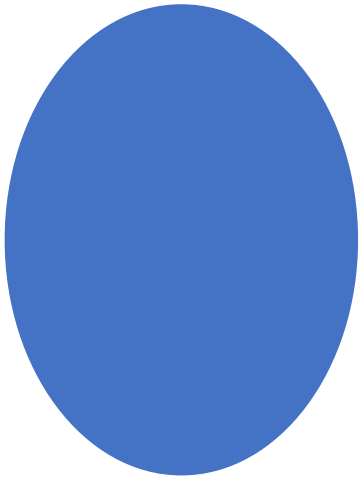
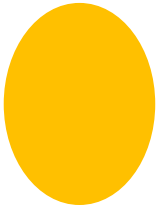
Common Criteria

Risk Analysis

CVSS

- CVSS is an industry standard for assessing the severity of computer system security vulnerabilities

- The **Common Vulnerability Scoring System (CVSS)** provides a way to
  - capture the principal characteristics of a vulnerability and
  - produce a numerical score reflecting its severity.
  - The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

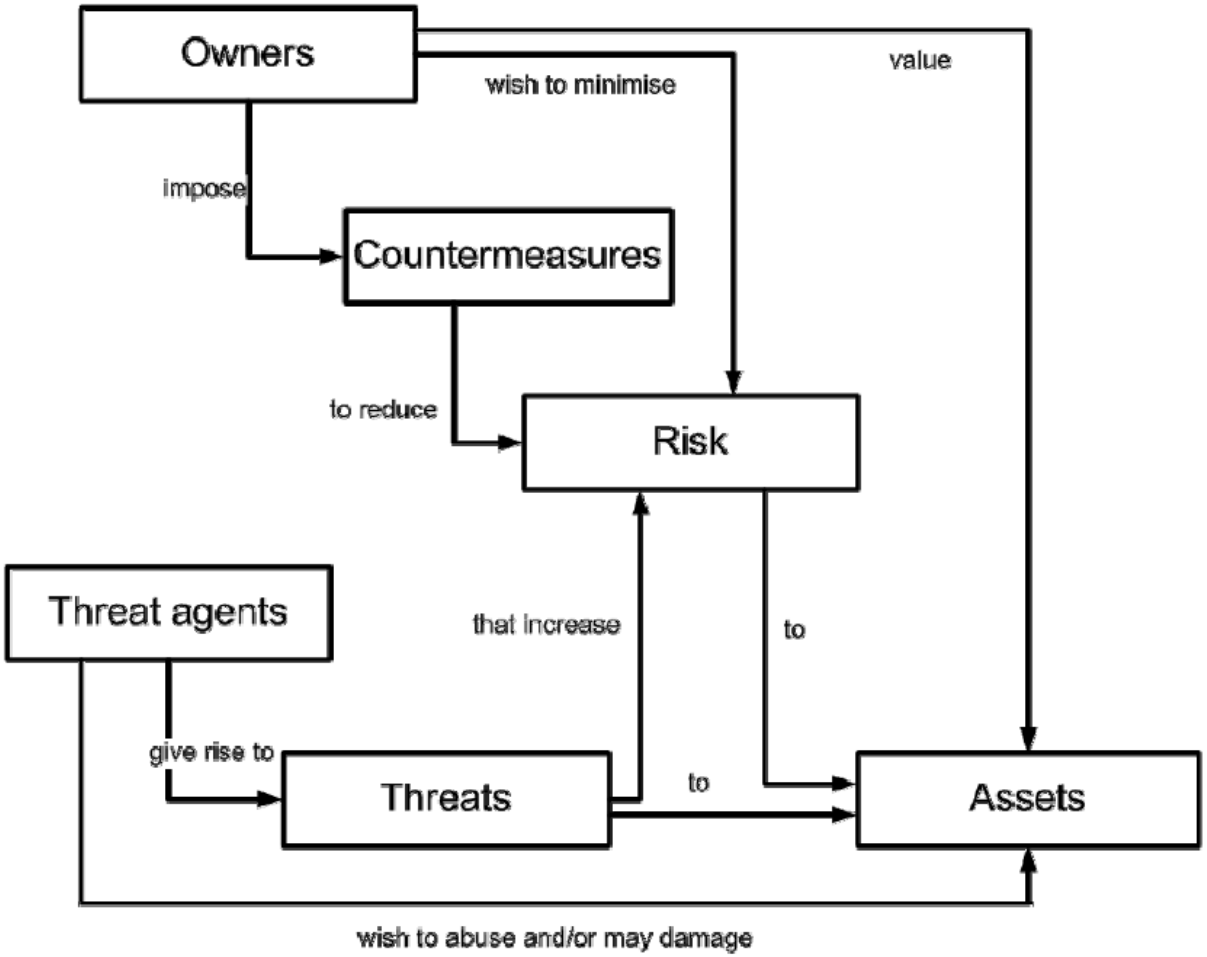



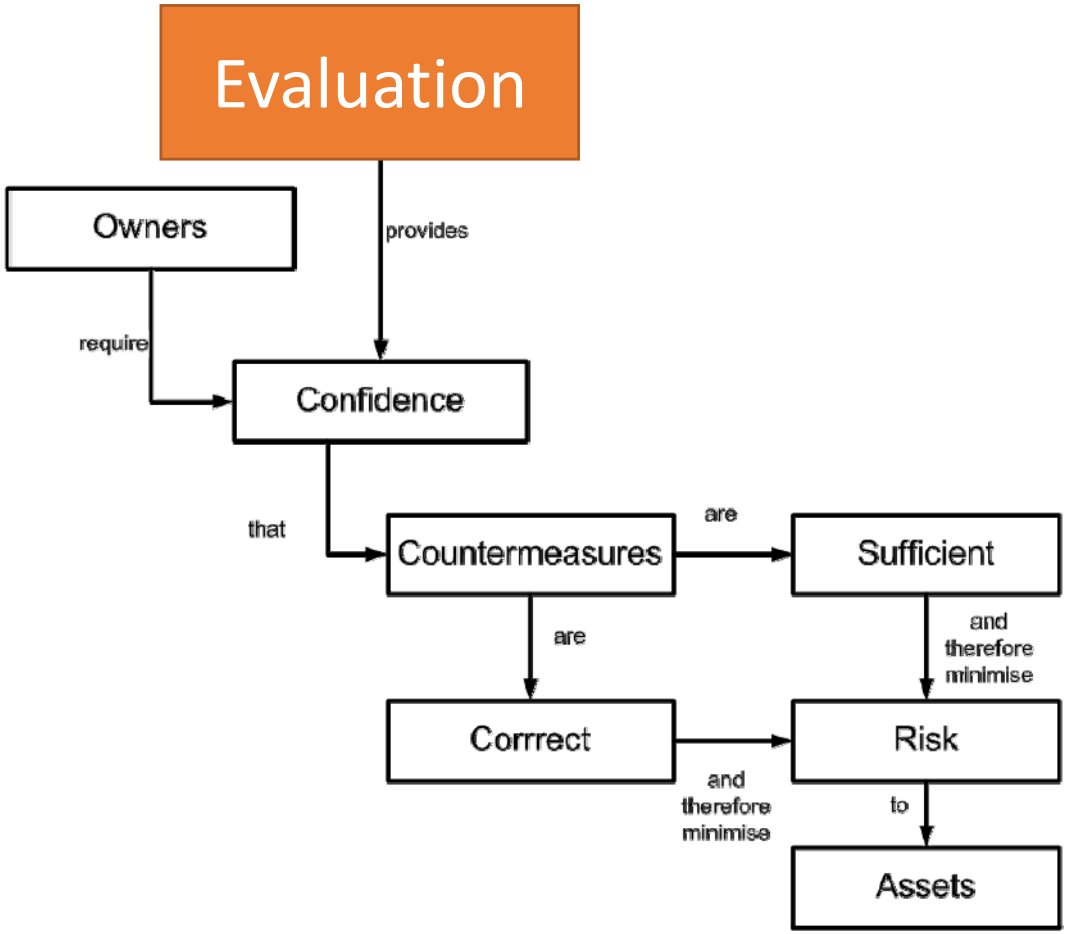
Common Criteria

Questions

- Does it work as intended?
- ”Security Assurance” = degree of confidence that security controls works as intended and protects the system

Trustworthy system?


Owners
value
wish to minimise
impose
Countermeasures
to reduce
Risk
Threat agents
that increase
to
give rise to
Threats
to
Assets
wish to abuse and/or may damage



HOW?

- Threat-/Risk analysis
- Architectural analysis
- Static analysis
  - Code reviews
- Dynamic analysis
  - Test in operational environment
- Penetration tests
- Fuzzing
- Analysis of development environments

Trustworthy system?

Questions

- Does it work as intended?
- ”Security Assurance” = degree of confidence that security controls works as intended and protects the system

We need evaluation criteria

- 80’s: TCSEC (”Orange Book”)
- 90’s: Common Criteria
  - ISO Standard that …
    - specifies security requirements, and then
    - defines evaluation criteria (*”yes, product meets these sec req”*)

The **evaluation process** establishes a **level of confidence** that the **security functionality** of these IT products and the assurance measures applied to these IT products **meet these requirements**. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

- 90's: Common Criteria
  - ISO Standard that …
    - specifies security requirements, and then
    - defines evaluation criteria (*"yes, product meets these sec req"*)

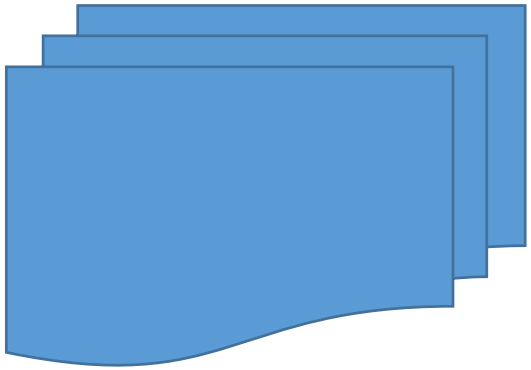
Trustworthy system?

The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the CC in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, **may result in meaningless evaluation results.**

- defines evaluation criteria (*"yes, product meets these sec req"*)

Trustworthy system?

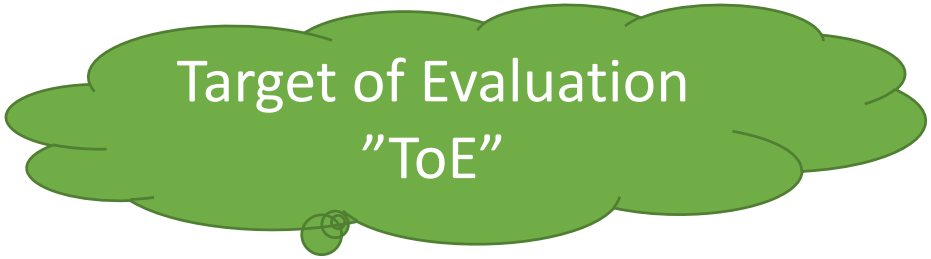
Target groups

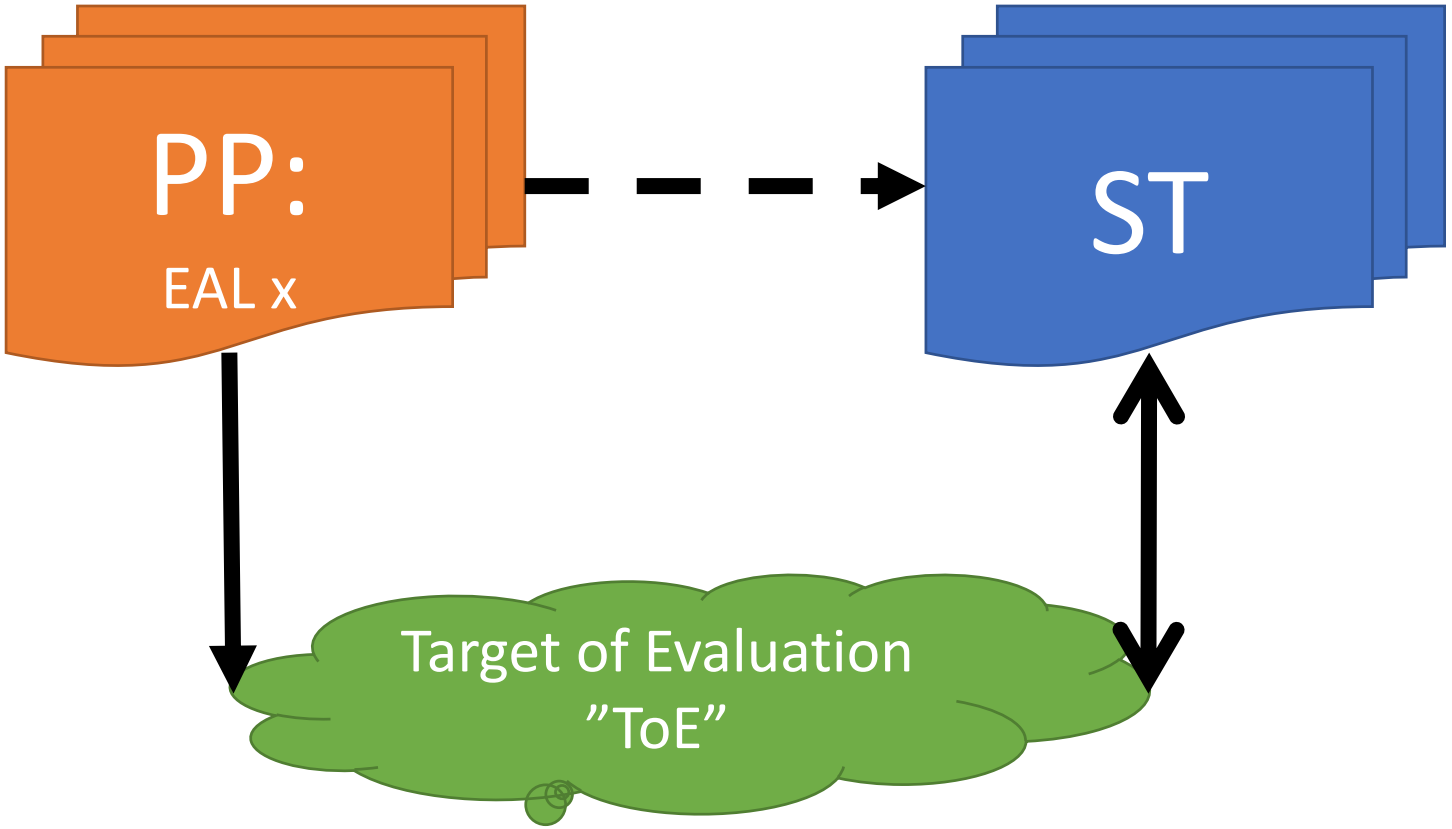


- Consumers
  - an implementation-independent structure, termed the **Protection Profile (PP)**, in which to express their security requirements in an unambiguous manner.
- Developers
  - implementation-dependent construct termed the **Security Target (ST)**.
- Evaluators

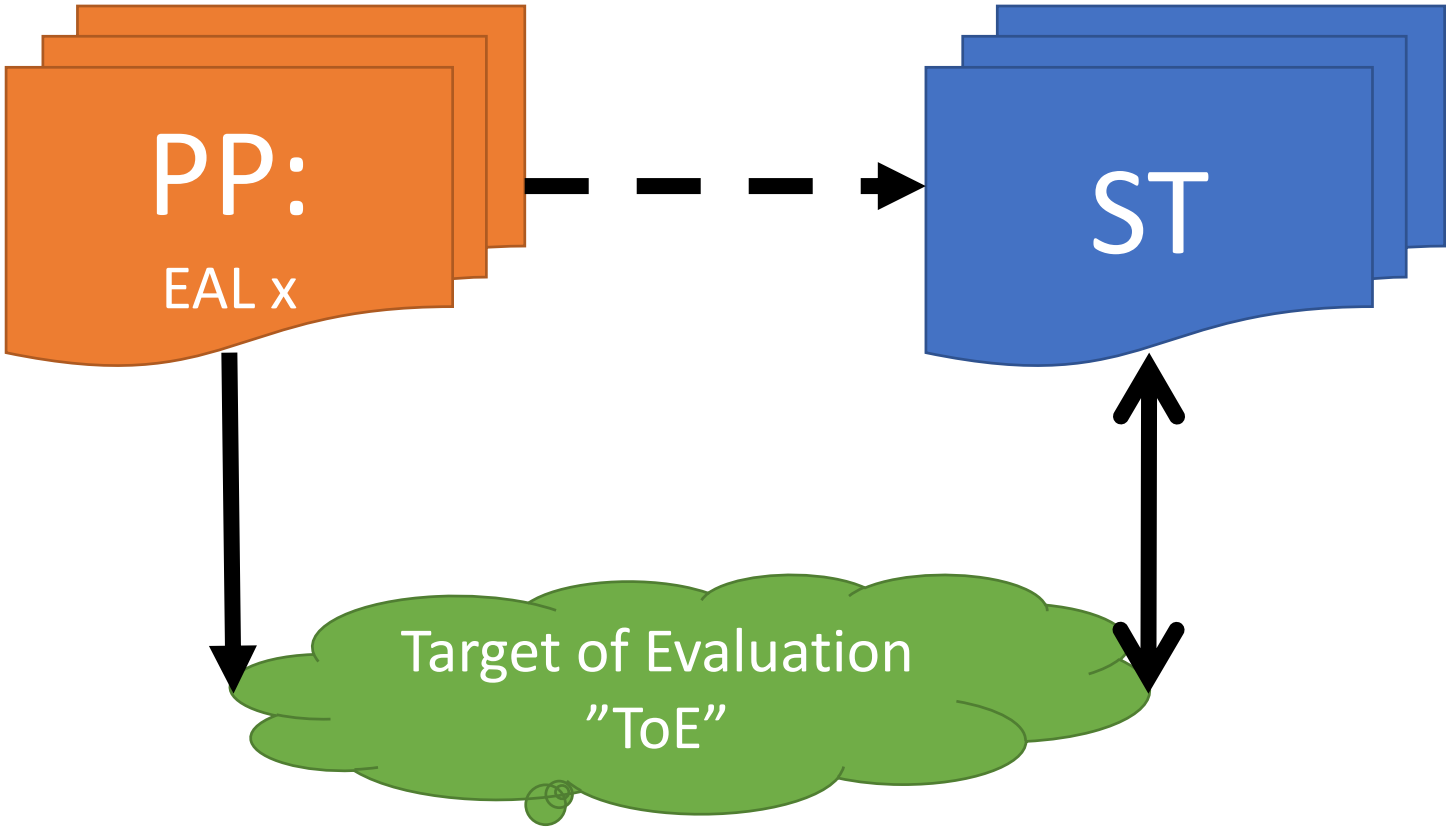
Evaluation criteria for PPs and STs:
7 pre-defined assurance packages **“EALs” (Evaluation Assurance Levels)**

- A software application;
- An operating system;
  - A software application in combination with an operating system;
- A smart card integrated circuit;
  - The cryptographic co-processor of a smart card integrated circuit;

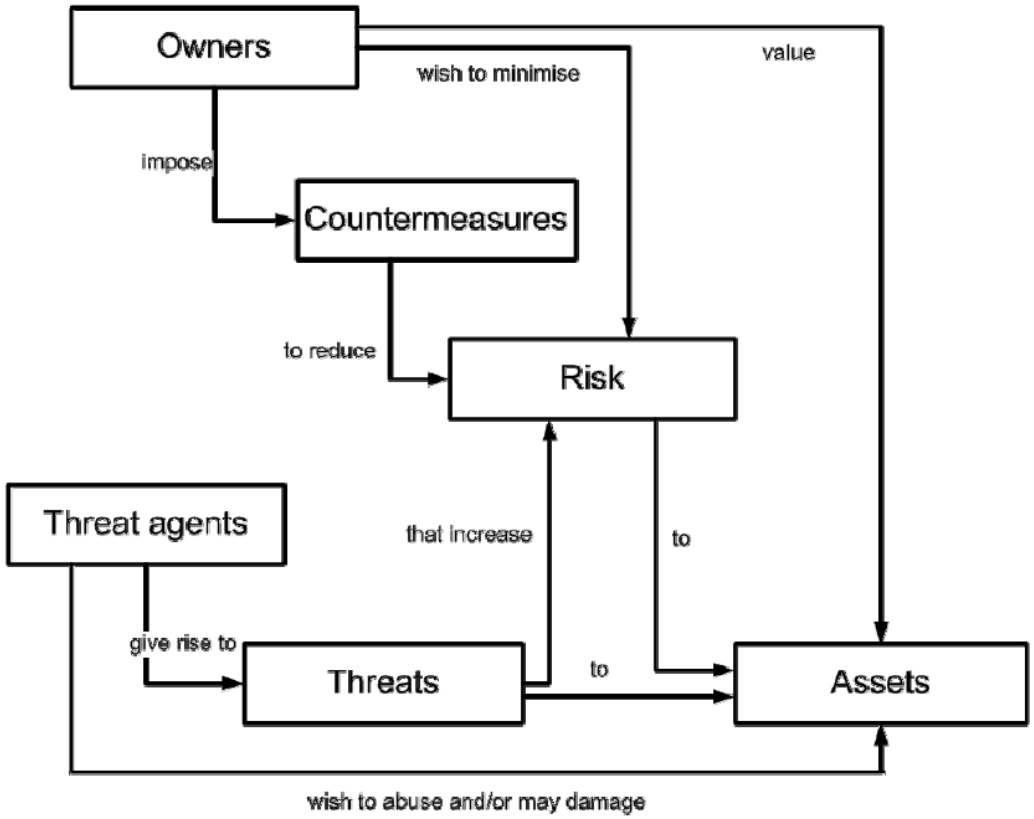



PP:
EAL x
ST
Target of Evaluation
”ToE”

- Sponsor: Customer/vendor
- Developer: provide evidence for evaluation
- Evaluator: evidence + testing + … =?= ST
- Certifier: government agency

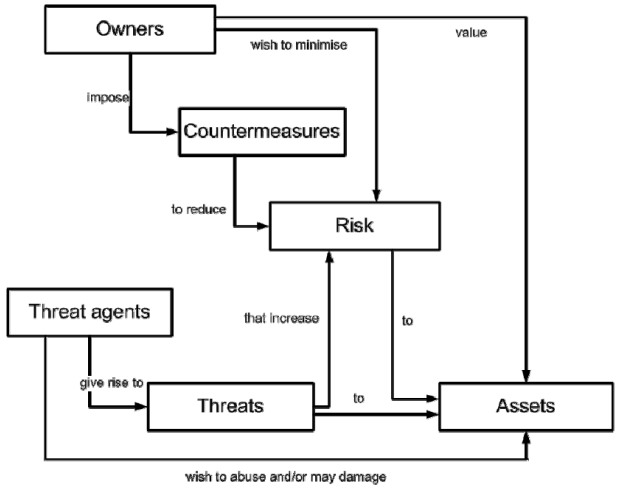


Risk Analysis



Risk Analysis

- What assets do we need to protect?
- How are these assets threatened?
- What can we do to counter these threats?

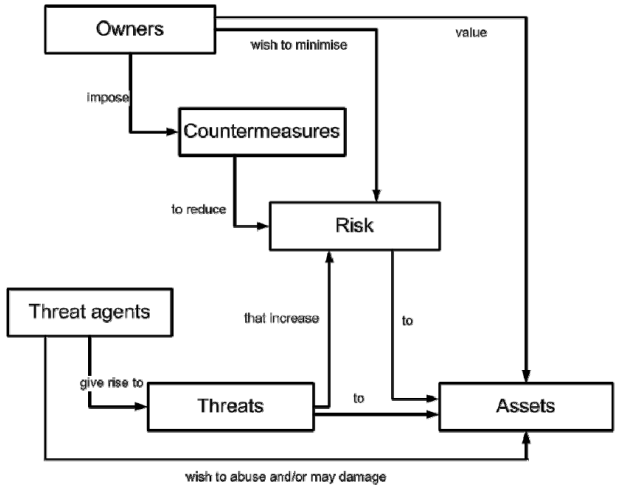


Detailed Risk Analysis Process

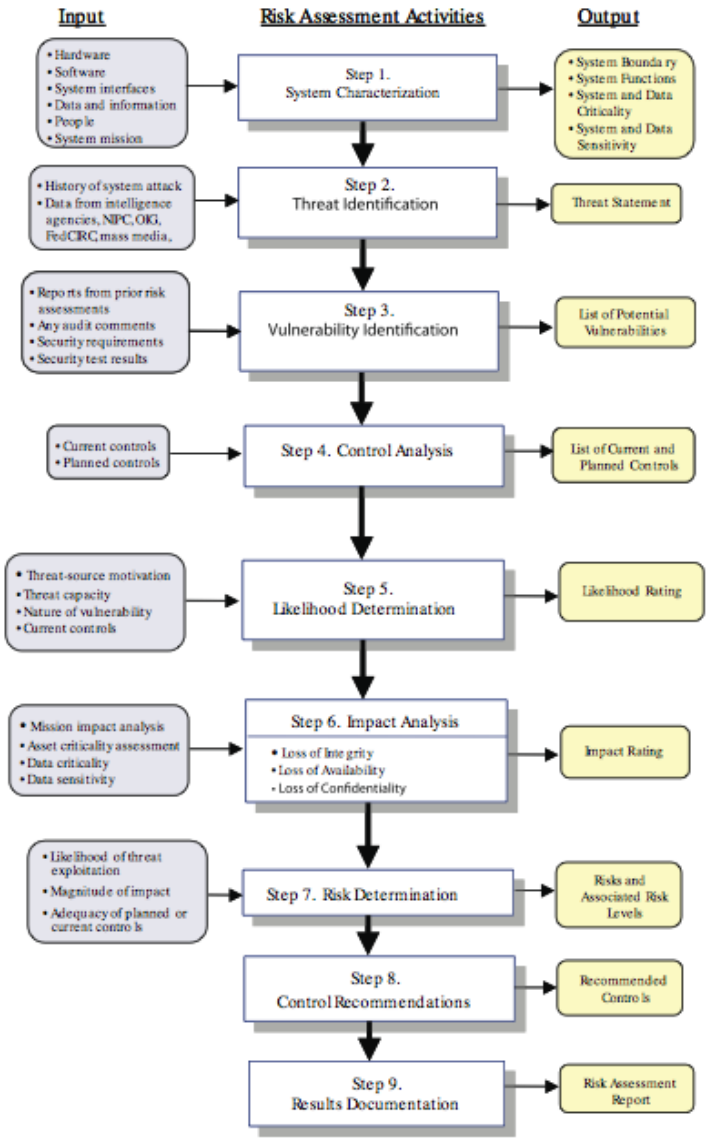
- Prepare/check status

- Identify threat sources
- Identify vulnerabilities
- Determine likelihood
- Determine impact (consequences)
- Determine risk

- Take action



Risk Analysis Process



Analyse Risks

- specify **likelihood of occurrence** of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce risk exposure
- specify **consequence** should the threat occur
- hence **derive overall risk rating** for each threat:
  risk = probability threat occurs x cost to organization
- in practice very hard to determine probabilities exactly, thus you may need to use qualitative
  (rather than quantitative) ratings for each
- aim to **order resulting risks** in order to treat them

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Determine Consequence

Rating	Consequence	Expanded Definition.
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last up to 2 weeks and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last 4-8 weeks and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for 3 months or more and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be de termined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

	Consequences					
Likelihood	**Doomsday**	**Catastrophic**	**Major**	**Moderate**	**Minor**	**Insignificant**
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

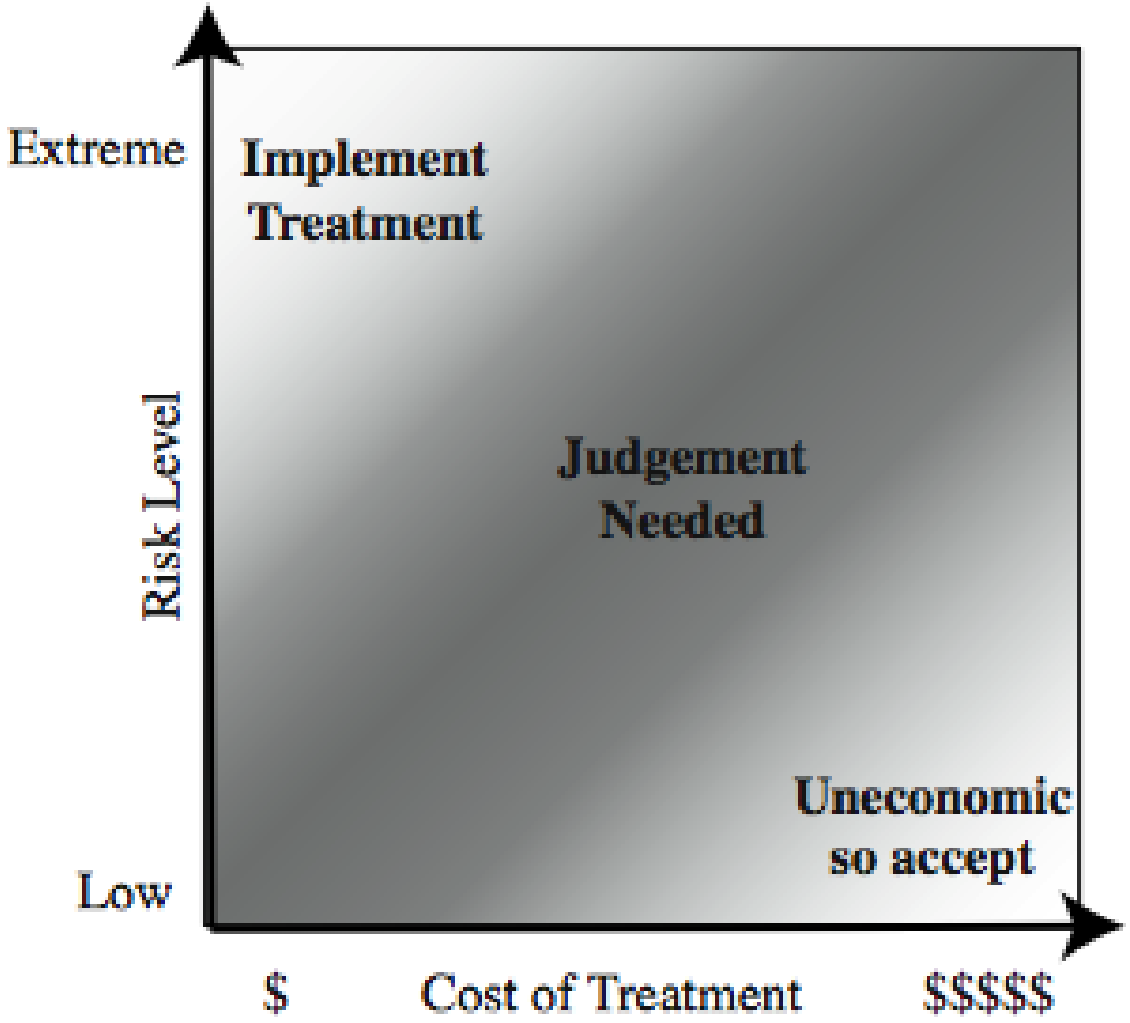
Risk Level	Description
Extreme (E)	Will require detailed research and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources.
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Document in Risk Register and Evaluate Risks

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment Alternatives

- Three major alternatives for risk treatment:
  - risk acceptance – "take the risk"
  - risk avoidance – "do not do it"
  - risk transferal – "insure yourself"
    – "look for partners"
- Plus two alternatives that are really "normal" security measures:
  - reduce consequence – "back-ups, recovery plans"
  - reduce likelihood – "better security mechanisms
    – and controls"


Extreme
Implement
Treatment
Risk Level
Judgement
Needed
Uneconomic
so accept
Low
$
Cost of Treatment
$$$$$

Summary

- **risk assessment** is an **important part of** the IT security management process
- detailed risk assessment process involves
  - **context** including asset identification
  - **identify threats, vulnerabilities,** risks
  - **analyse and evaluate** risks
- deal with the risk assessment correctly

Summary

Each letter of STRIDE maps to an adversaries and/or the defender's goals. Of course the primary goals can also be useful during the initial compromise to open the door.

Goal	Defender	Attacker	Threat Category
Open the Door	Prevent door opening	Compromise	**S**poofing
Integrity	Preserve	Violate	**T**ampering
Hide Activity	Preserve visibility	Hide Activity	**R**epudiation
Confidentiality	Preserve	Violate	**I**nformation Disclosure
Availability	Preserve	Deny	**D**enial of Service
Open the Door	Prevent door opening	Compromise	**E**levation of Privilege

Links

- To learn more about STRIDE and threat modeling: http://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx
- SDL Process https://www.microsoft.com/en-us/sdl/process/design.aspx
- Microsoft's Free Threat Modeling Tool: https://www.microsoft.com/en-us/download/details.aspx?id=49168

Acknowledgements

A special thank you goes to my colleagues Michael Howard, John Rodriguez and Walter Dominguez for their valuable feedback.

Back to top

Tags #Cybersecurity #SDL #STRIDE

Join the conversation

Add Comment

The student is invited to read the corresponding material by him/herself in the textbook. Thus, the slides can be regarded as a reading template.

Human and Organisational factors

- The greatest threat?
  - Human in the system?
    - Forgetful, unsuspecting, negligent, egoistic, open to bribery, …

Example: Use of passwords

- Intrusion method:
  Guess passwords/Exhaustive search
  (e.g. using the Crack software)

- Where is the vulnerability/Who is to blame?
  - system designer: who constructs the system?
    (password length insufficient, password file readable)
  - customer: who bought insecure software?
  - users:
    - who are choosing bad passwords?
    - who write them down/who give them away?
  - system administrator: for not checking the passwords?
  - the boss: who does not inform/educate his employees?

Ex: Use of passwords
How to fix the problem (1)

- Possible countermeasure 1
  - Generate passwords that could be **pronounced** and that are **easy to memorize**!
    But still being “random”.
  - Result
    - The sample space was significantly reduced, so it became much easier to guess the password with Crack!!
      (human-deficient conclusions)

Ex: Use of passwords
How to fix the problem (2)

- Possible countermeasure 2
  - password aging: the system enforces a change after a certain predefined time
  - RESULT
    - Users change between two different passwords all the time or “change/change back” immediately.
- CM3
  - The system “remembers” old passwords and does not accept re-use of a password that has already been in use
    (the last n times).
  - RESULT
    - Users change passwords n+1 times
      each time a password change is enforced!
      (human laziness/inability to adhere to rules)

Terms and documents

- Organizational Security Policy
  - “formal statement of rules by which people given access to organization's technology and information assets must abide”
  - Topics: Principles, organizational reporting structure, physical security, hiring, management, and firing, data protection, communications security, hardware, software, operating systems, etc.
- IT Security Plan
  - What will be done, who is responsible, what resources needed?
- Incident Handling
- Change management, configuration management, personnel security
  - Personnel Security
    - Hiring
    - Employment agreements: should agree and sign terms (remember forensics)
    - During employment
    - Termination