Attack Trees, Multilateral and Multilevel Security

Software Security

Steffen Helke
Chair of Software Engineering

19th November 2018

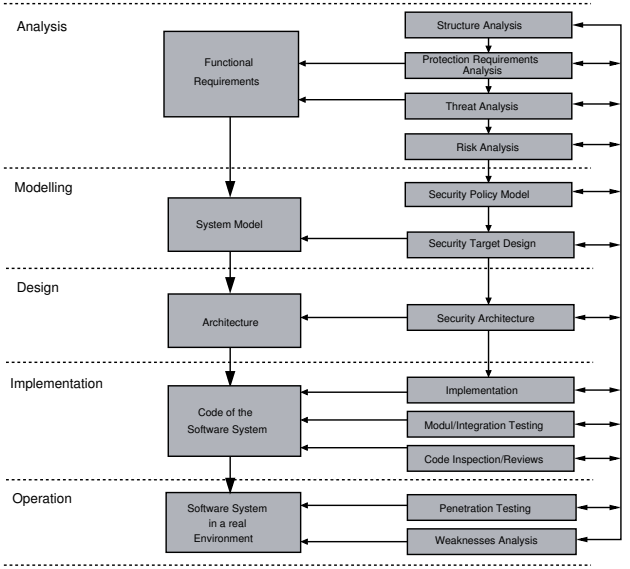
Brandenburgische
Technische Universität
Cottbus - Senftenberg

Repetition: Security Analyses

Objectives of today's lecture

- ➜ Repetition: Activities of Security Analyses
- ➜ Being able to use *Attack Trees* and *Risk Assessment Matrixes*
- ➜ Understanding differences between *Multilateral Security* and *Multilevel Security*
- ➜ Getting to know the characteristics of an IT security model and different *access control strategies*
- ➜ Being able to explain multilevel security using the *Bell-LaPadula model* as an example

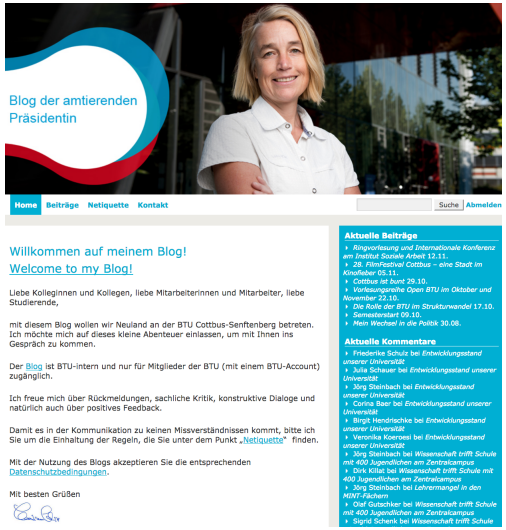
What are the most important activities of a security analysis?



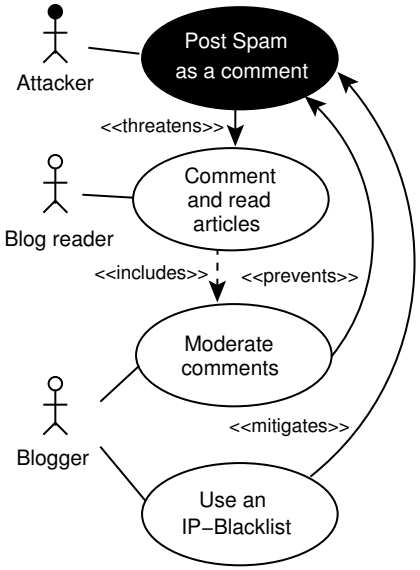
What are the most important artifacts?

1. **Structure Analysis**
   - Network *topology model*
   - Table with attributes for each system component
   - Initial requirements specification
2. **Protection Requirements Analysis**
   - *Use case model* to describe actors and system functionality
   - Identifiying *damage scenarios*, *protection goals* and conflicts
   - Evaluation of the required level of protection for scenarios
3. **Threat Analysis**
   - *Misuse case model* to decribe misactors, attacker behaviour and countermeasures
   - *Attack tree model* to refine attacker goals
4. **Risk Analysis**
   - *Risk assessment* to find out the required level of protection
   - *Annotated attack trees*, e.g. using costs and probabilities

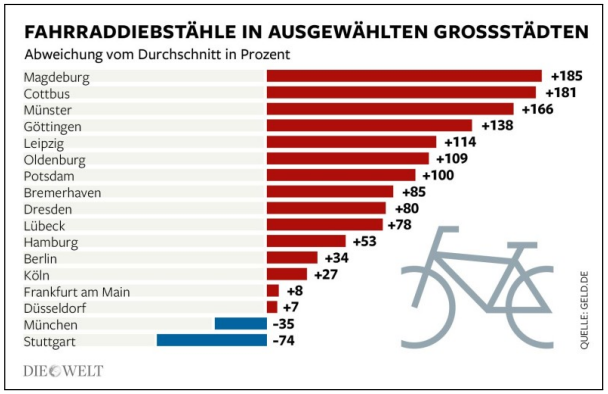
Exercise: Presidential Blog Threat Analysis (Misuse Case Model)



Example for a Misuse Case Model

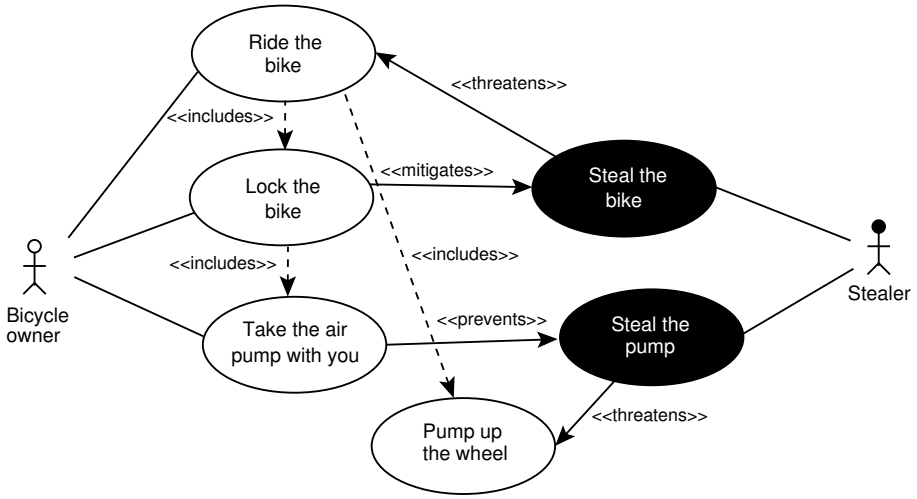


Example: Threat Analysis Bicycle Stealing



Source: *Die Welt* 26.6.2014

Example: Threat Analysis Bicycle Stealing



Evaluation of the Misuse Case Notation

Advantages

+ Provides a detailed analysis of attack scenarios
+ Is supported by a distinct methodology for describing functional and non-functional requirements, e.g. by dealing with external threats
+ Similar to the popular UML notation

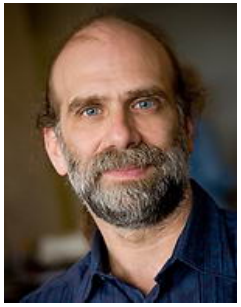
Disadvantages

– Trivialisation of security requirements
– Models can quickly become confusing

Attack Trees

General Remarks

- Developed by Bruce Schneier, an US security expert, in 1998
- Examples of similar modeling approaches
  - ➜ Fault Tree Analysis (1962, FTA)
  - ➜ Threat Trees (1994)

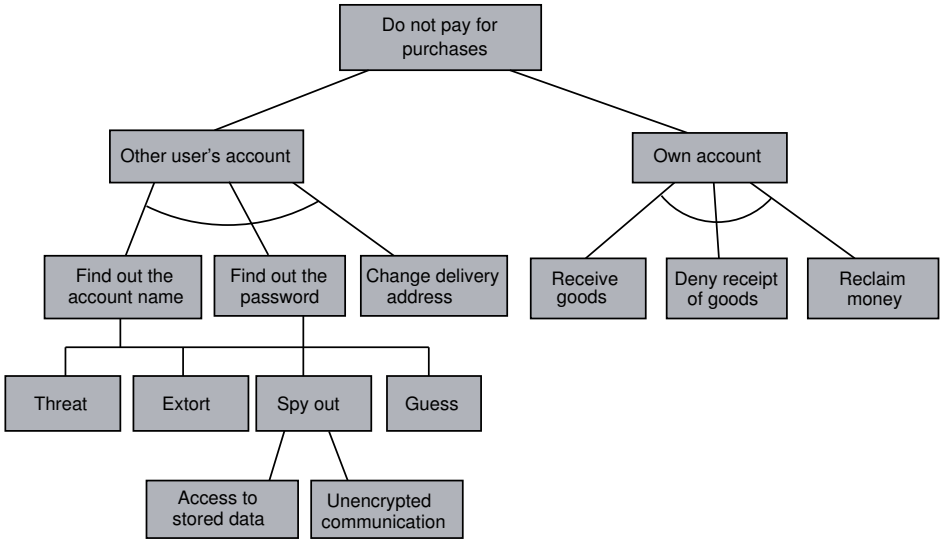


Quelle: http://www.schneier.com

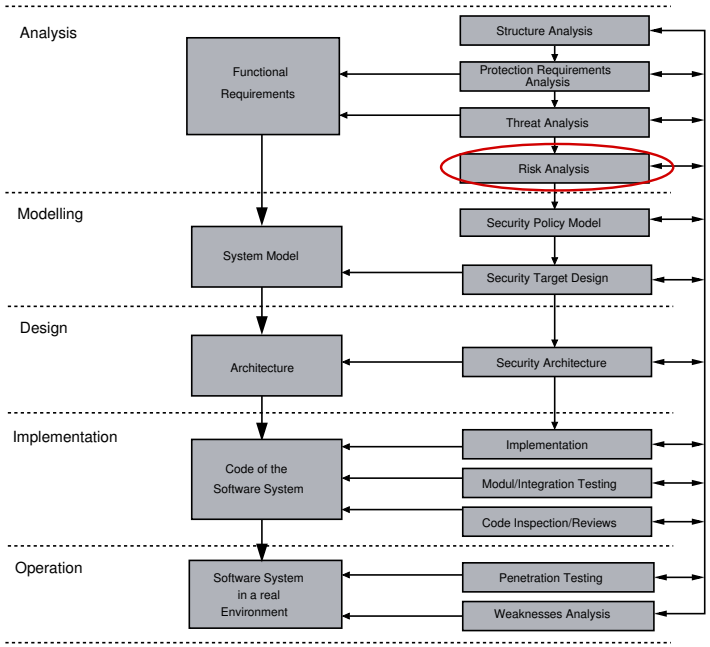
Objectives

- How can attacks be graphically modelled?
- What is the probability of a successful attack?
- How can an attack goal be refined by subgoals?

Attack Tree based on the Web Shop Example



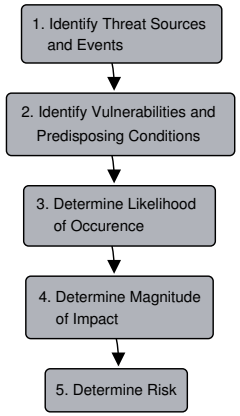
Activities of a Security Engineering Process



4. Risk Analysis

Remarks

- Risk is the likelihood of an unwanted incident and its consequence for a specific asset
- Can be modeled e.g. by *attack trees using attributes* (probabilities or costs)

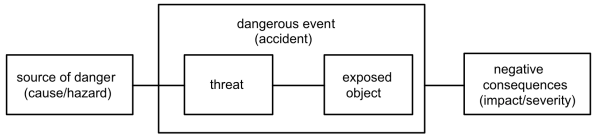


Risk Analysis of the BSI

- For low and medium security requirements there exist defaults classifications of the *IT-Grundschutz Catalogues*

Risk Analysis

➜ Analysis and evaluation of dangerous events, their sources (hazards) and impacts



Risk identification using qualitative methods

- scenario-based analysis
- simulation-based analysis

Risk evaluation using quantitative methods

- cardinal evaluation
- ordinal evaluation

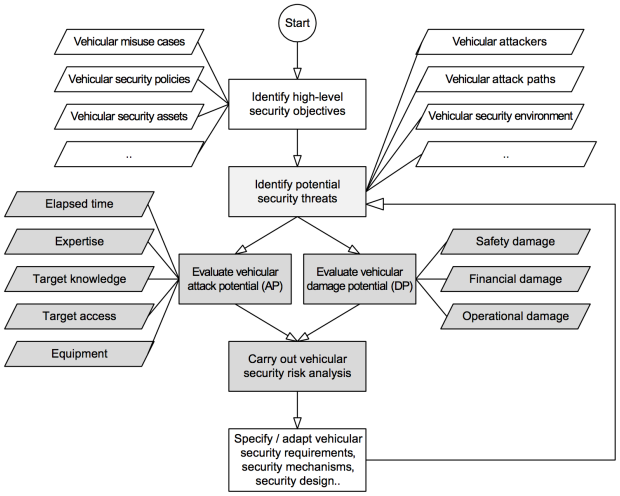
Risk Assessment Matrix

EXAMPLE RISK		Probability: Very High	High	Medium	Low	Very Low
Consequence	Very High	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

Source: http://diarmfs.com/risk-assessment-table/

Vehicular Security Design Process

➜ Gray boxes describe the activities for the risk analysis



Source: M. Wolf & M. Scheibel: *A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems, LNI, 2016.*

Exemplary Automotive IT Security Risk Matrix

AP↓	Probability reference	Risk assessment			
Basic	Certain	Undesirable	Inacceptable	Inacceptable	Inacceptable
Enhanced Basic	Likely	Tolerable	Undesirable	Inacceptable	Inacceptable
Moderate	Possibly	Tolerable	Undesirable	Inacceptable	Inacceptable
High	Unlikely	Negligible	Tolerable	Undesirable	Inacceptable
Beyond High	Rare	Negligible	Negligible	Tolerable	Inacceptable
	Practically infeasible	Negligible	Negligible	Negligible	Undesirable
DP →		Insignificant	Medium	Critical	Catastrophic

➜ Damage Potential Calculation

$$DP = DP_{safety} + DP_{financial} + DP_{operational}$$

➜ Attack Potential Calculation

$$AP = AP_{time} + AP_{expertise} + AP_{knowledge} + AP_{access} + AP_{equipment}$$

Source: M. Wolf & M. Scheibel: *A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems, LNI, 2016.*

Damage Potential Calculation

DP	Total damage potential classification
0 – 2	Insignificant
3 – 21	Medium
22 – 210	Critical
> 210	Catastrophic

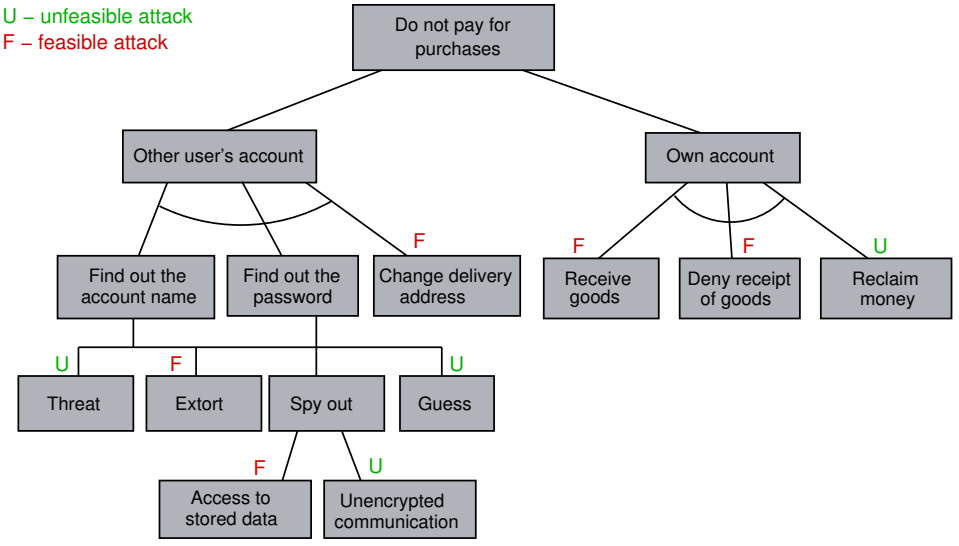
$$DP = DP_{safety} + DP_{financial} + DP_{operational}$$

Damage category	Damage reference	Factor
Safety severity classes	Life-threatening injuries (survival uncertain), fatal injuries	10,000
	Severe and life-threatening injuries (survival probable)	1,000
	Light and moderate injuries	100
	No injuries	0
Finance severity classes (global sum)	Existence-threatening financial damage (e.g., monetary damage is >30% of annual sales)	1,000
	Substantial financial damage, but yet not existence-threatening (e.g., monetary damage is 20% – 30% of annual sales)	100
	Undesirable financial damage (e.g., monetary damage is 5% – 20% of annual sales)	10
	No or tolerable financial damage (e.g., monetary damage is <5% of annual sales)	0
Operational functionality severity classes	Vehicles unusable, i.e., one or more fundamental functions are affected. The vehicle usage is infeasible. This can be compared with FMEA severity rating above 8.	100
	Service required, i.e., an important function is affected. The vehicle can be used only with massive restrictions. This can be compared with FMEA severity rating 6 to 8.	10

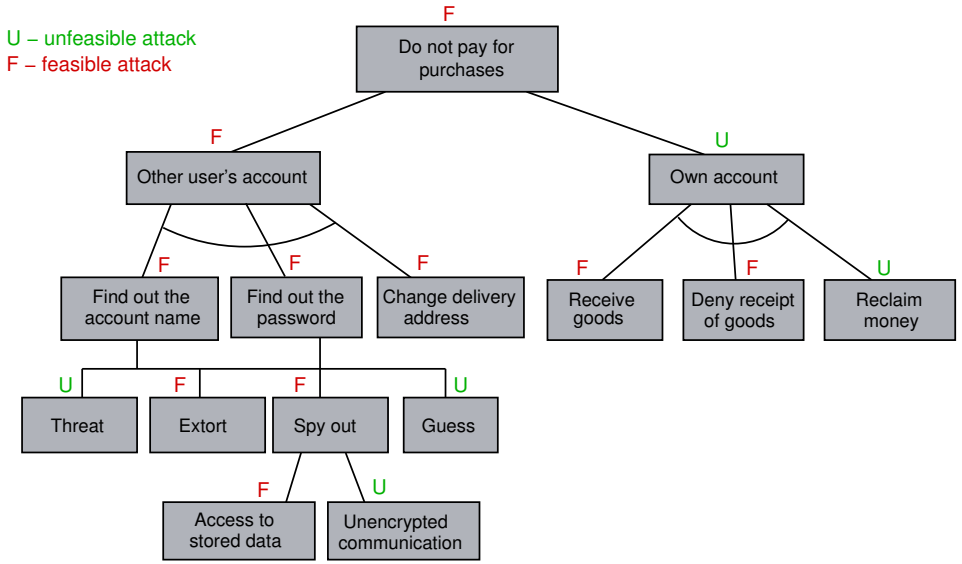
Source: M. Wolf & M. Scheibel: *A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems, LNI, 2016.*

How to attribute an Attack Tree?

U – unfeasible attack
F – feasible attack



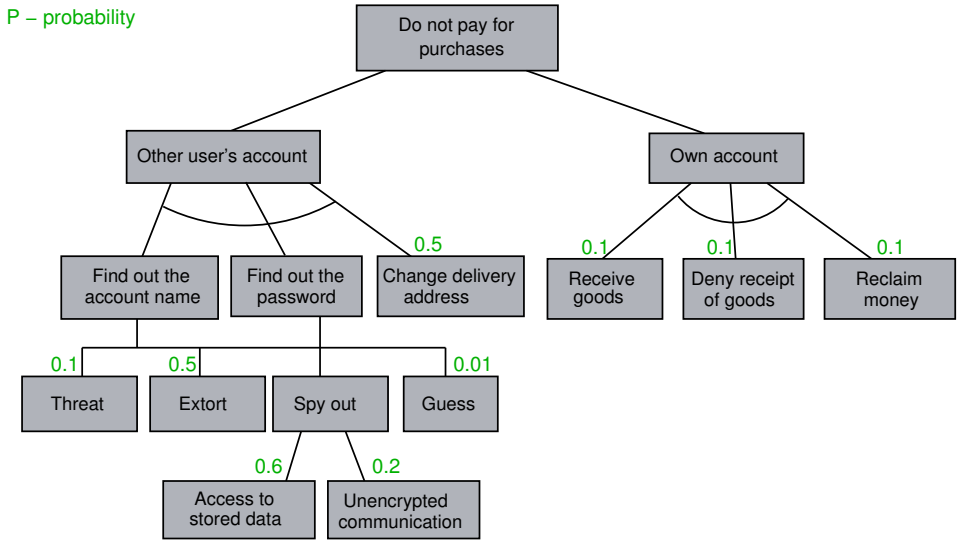
How to propagate the attributes?



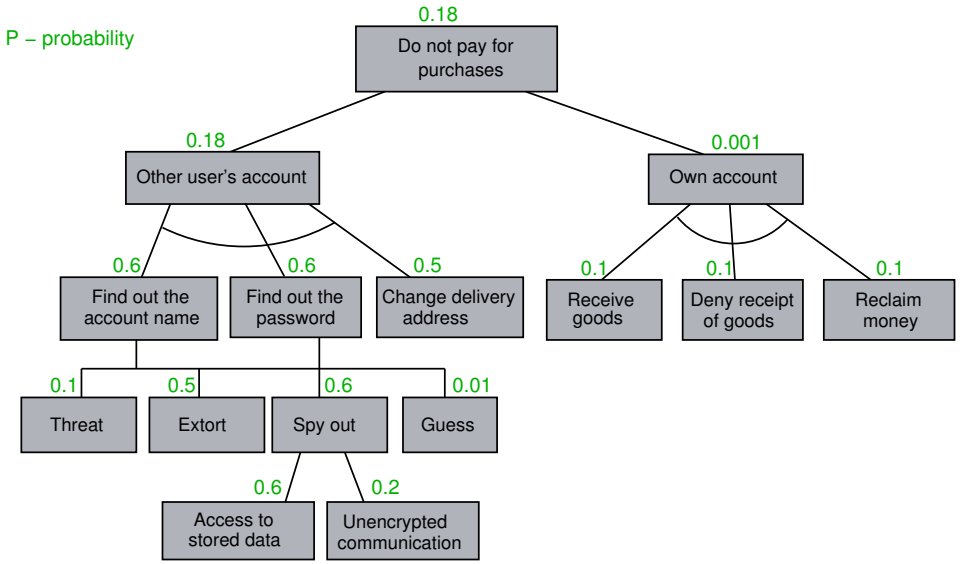
How to propagate attributes?

1. A parent node evaluates to FEASIBLE if ...
   - all its sub-nodes also evaluated to FEASIBLE for an *AND* relationship or
   - one of its sub-nodes is also evaluated to FEASIBLE for a *OR* relationship
2. The *costs* of a parent node are ...
   - the sum of the costs of all sub-nodes for an *AND* relationship or
   - the costs of the most cost-effective sub-node for a *OR* relationship
3. The *probability* of a parent node is ...
   - the product of the probabilities of all sub-nodes for an *AND* relationship or
   - the maximum of the probabilities of all sub-nodes for a *OR* relationship

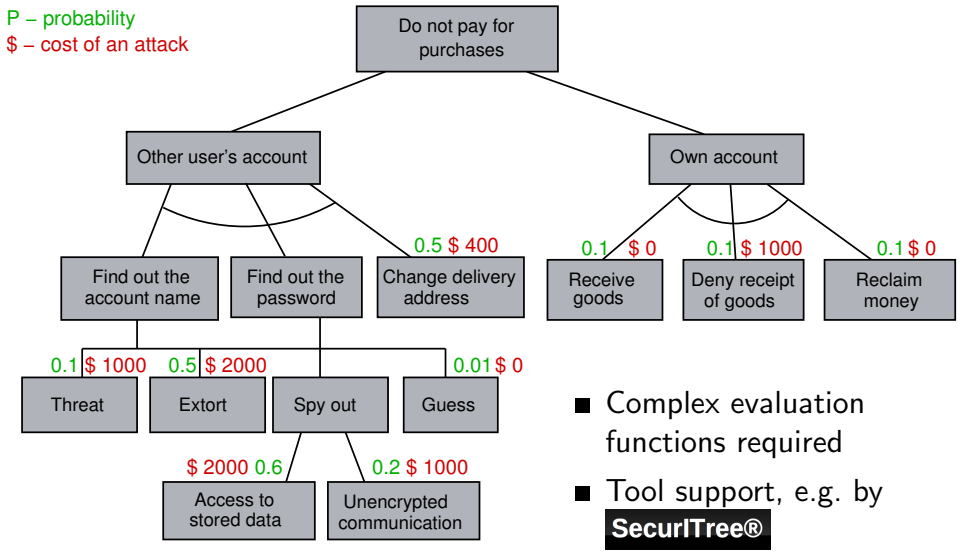
How to propagate probabilities?



How to propagate probabilities?



How to propagate combined values?



- Complex evaluation functions required
- Tool support, e.g. by **SecurITree®**

Risk Analysis Tool

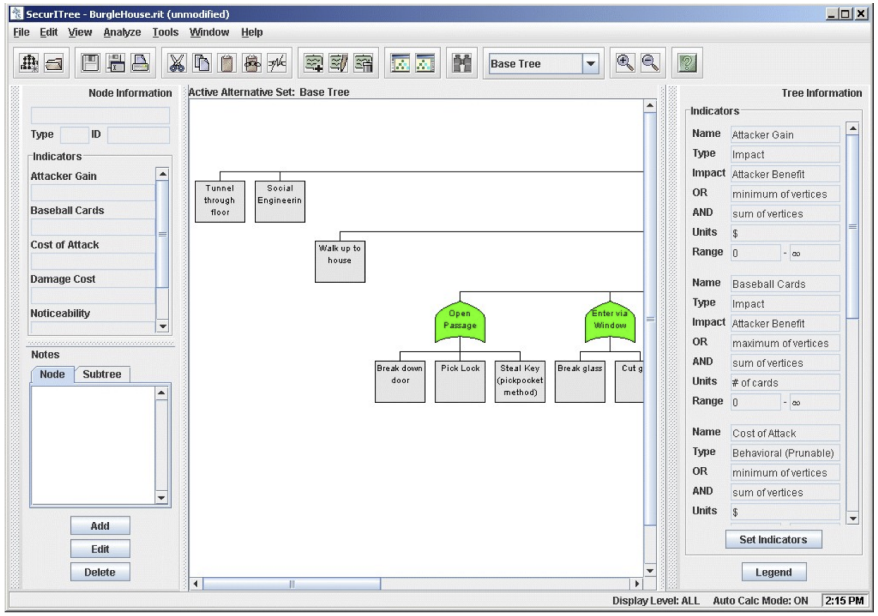
Remarks

- Software developed by Amaneza **SecurITree®**
- Basis: Attack trees

Features

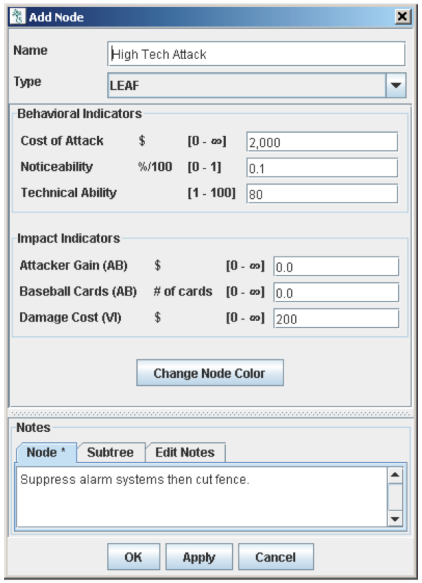
- Risk analysis for risk optimization
- Models for identifying attackers and vulnerabilities
- Adequate threat assessment
- Comprehensive libraries for standard components available
- Ability to create your own libraries

Attack Trees and Indicators of SecurITree

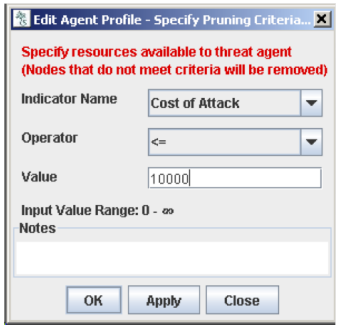


Quelle: http://www.amenaza.com/

Defining Nodes & Attacker Profiles



Source: http://www.amenaza.com/



Source: http://www.amenaza.com/

Assessment Procedure for SecurITree

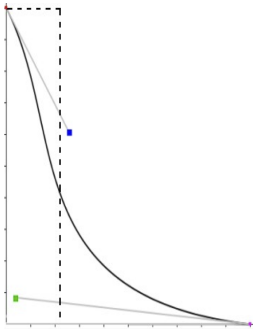
Problem

- Absolute values (e.g. costs) are not often reasonable

➜ Even small variations of the evaluation (e.g. $1) immediately lead to completely different results

Solution

- *Advanced Analysis Function*: Curve function maps the readiness of an attacker more appropriately
- Step function (dashed line) represents previous description with absolute values



Textual Representations of Attack Trees

➜ Graphical representation of realistic examples as trees can quickly become confusing

➜ Textual descriptions are more suitable

Numbered List Format

```
Goal: Open Safe (OR)
 1 Pick Lock
 2 Learn Combo
 3 Cut Open Safe
```

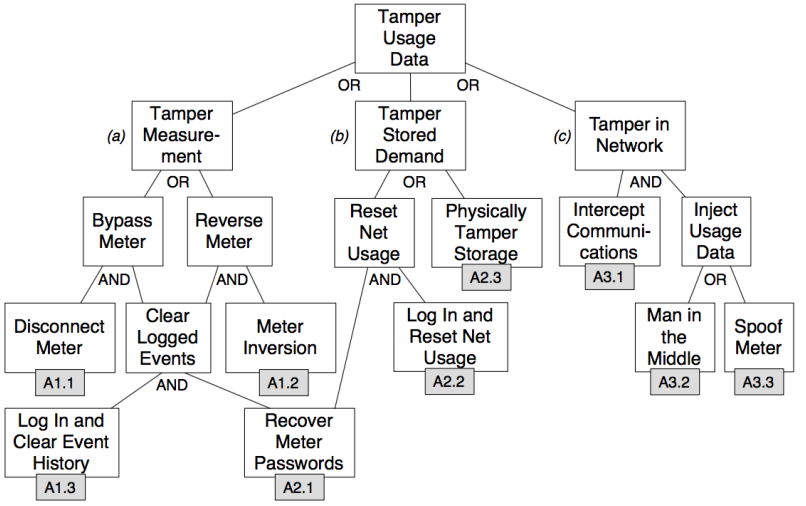
Alternative

```
Goal: Open Safe
OR 1 Pick Lock
   2 Learn Combo
   3 Cut Open Safe
```


Textual Representations of Attack Trees

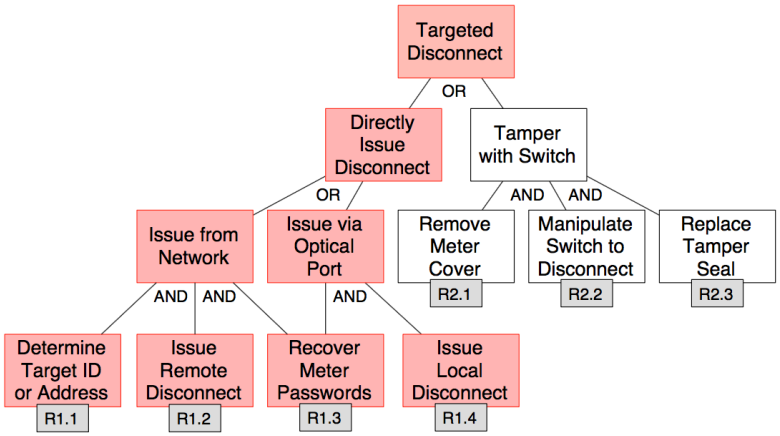
```
Goal: Open Safe
OR 1 Pick Lock
   2 Learn Combo
     OR 2.1 Find Written Combo
        2.2 Get Combo From Target
            OR 2.2.1 Threaten
               2.2.2 Eavesdrop
                     OR 2.2.2.1 Listen to Conversation
                        2.2.2.2 Get Target to State Combo
               2.2.3 Blackmail
   3 Cut Open Safe
```


Example: Attack Tree for Smart-Metering-System



Quelle: D. Podkuiko: Vulnerabilities in Advanced Metering Infrastructures, Pennsylvania State University, 2012.

Refinement of a Attack Tree for a Smart-Metering-System



Quelle: D. Podkuiko: Vulnerabilities in Advanced Metering Infrastructures, Pennsylvania State University, 2012.

Evaluation of the Attack Tree Notation

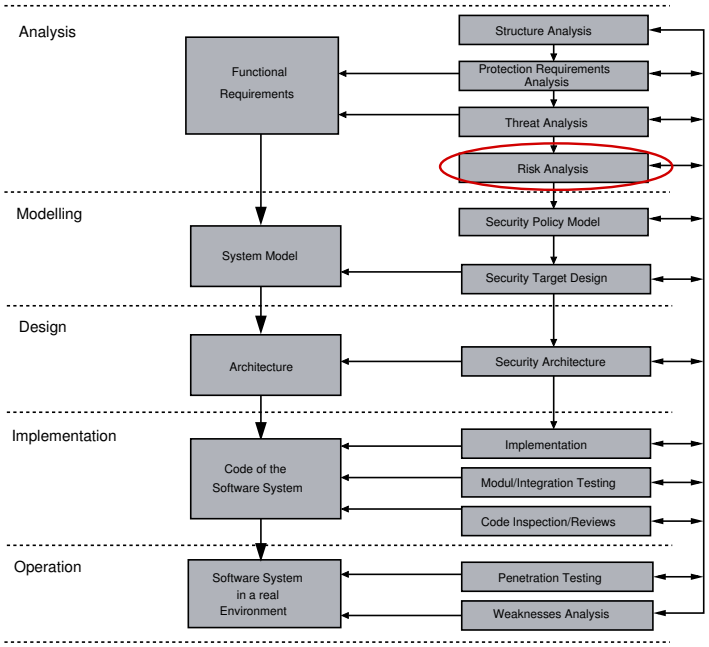
Advantages

+ Detailed analysis of attack scenarios is possible
+ Encapsulation & reuse of subtrees are supported
+ Analysis of threats leads to systematic design of countermeasures

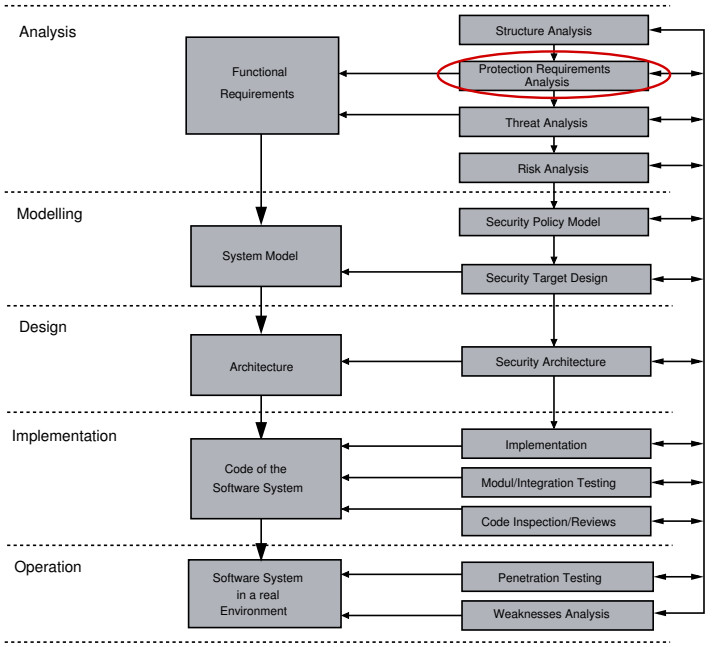
Disadvantages

– Defining a realistic assessment is often difficult
– Trees become too complex for real-world attacks
– Evaluation of the tree leaves can be context-dependent, therefore reuse is often not possible

Activities of a Security Engineering Process



Activities of a Security Engineering Process



Correlations between Protection Goals

Tasks for a Protection Requirement Analysis

➜ Check the feasibility of the collected protection goals

➜ Suggest possible compromises in case of conflicts (e.g. pseudonymity)

Basic Theory

➜ *Multilateral Security*

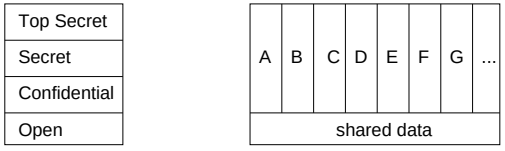
➜ Correlations and monotony behaviour of protection goals

Multilateral vs. Multilevel Security

Multilateral vs. Multilevel Security

Hierarchy vs. Coexistence

- Multilateral implements *no strictly hierarchical separation*, instead (equitable) coexistence of different protection areas
- Similar to the non-ordered security categories of multilevel security, however there are additionally strong hierarchical security levels



Democracy vs. Dictatorship

- No single party enforces protection goals against all other parties
- Multilateral security describes a democratic view on all communication partners, also called compartmented security

Multilateral Security

Definition

Multilateral security means the inclusion of *all* participants's protection interests as well as dealing with resulting conflicts, such as the development of a communication connection

Objectives

1. Each person has individual protection goals and should formulate them
2. Conflicts will be identified and compromises negotiated
3. Everyone can enforce their protection goals on the basis of the negotiated compromise

Protection Goals for Secure Communication

Potential threats	Protection of communication content	Protection of communication circumstances
Unauthorized access on information → Confidentiality goals	Confidentiality Hiding	Anonymity Unobservability
Unauthorized modification of information → Integrity goals	Integrity	Accountability
Unauthorized impairment of functionality → Availability goals	Availability	Reachability Legal Enforceability

Precise Definitions of Protection Goals (1)

Confidentiality ensures that nobody apart from the communicants can discover the content of the communication

Hiding ensures the confidentiality of the transfer of confidential user data. This means that nobody apart from the communicants can discover the existence of confidential communication

Anonymity ensures that a user can use a resource or service without disclosing his/her identity, not even the communicants can discover the identity of each other

Unobservability ensures that a user can use a resource or service without others being able to observe that the resource or service is being used. Parties not involved in the communication can observe neither the sending nor the receiving of messages

Integrity ensures that modifications of communicated content (including the sender's name, if one is provided) are detected by the recipient(s)

Precise Definitions of Protection Goals (2)

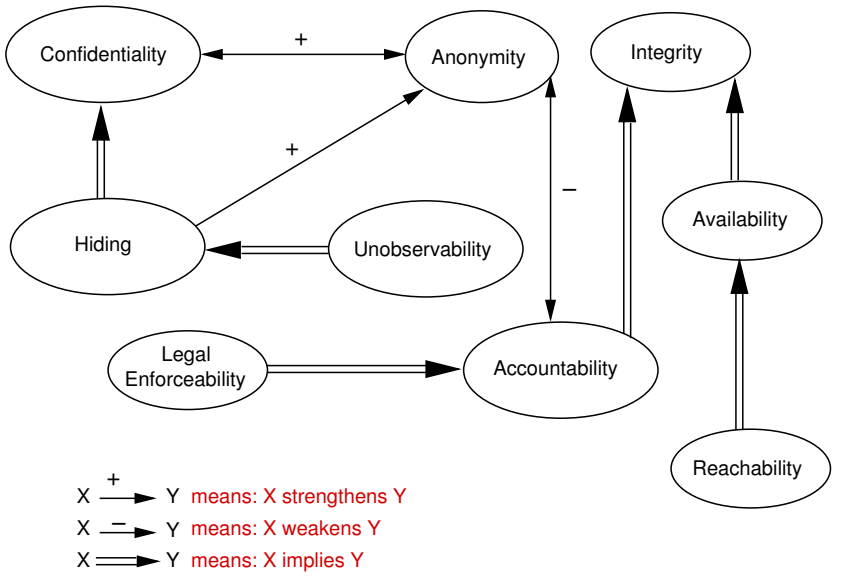
Accountability ensures that sender and recipients of information cannot successfully deny having sent or received the information. This means that communication takes place in a provable way

Availability ensures that communicated messages are available when the user wants to use them

Reachability ensures that a peer entity (user, machine, etc.) either can or cannot be contacted depending on user interests

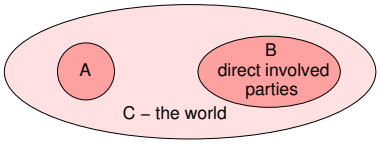
Legal Enforceability ensures that a user can be held liable to fulfill his/her legal responsibilities within a reasonable period of time

Correlations between Protection Goals

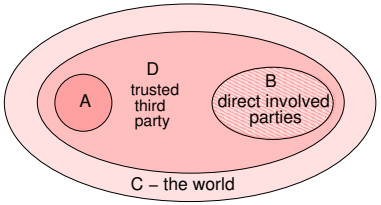


Against which parties are the protection goals to be enforced?

1. *Common* perspective against the rest of the world



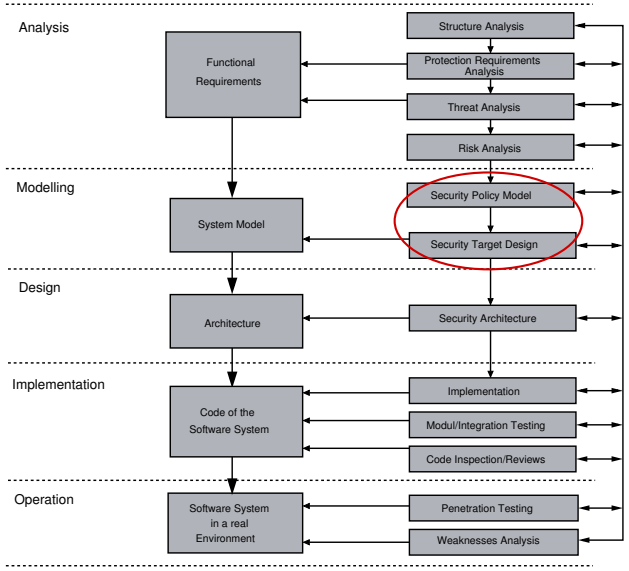
2. *Individual* perspective from *A* against *B* and the rest of the world sometimes with the help of a trusted third party



Protection goal	Who against	Whom?	Common or individual perspective
Confidentiality	A & B	C	*We* want to enforce confidentiality of the message content
Hiding	A & B	C	*We* want to hide the existence of the message
Anonymity	A B	B(+C) A(+C)	*I* want to remain anonymous *He* or *she* wants to remain anonymous
Unobservability	A(&D) B(&D)	B(+C) A(+C)	*I* want to stay unobservable *He* or *she* wants to stay unobservable
Integrity	A & B	C	*We* want integrity of the message content
Accountability	A(&D) B(&D)	B(+C) A(+C)	*I* agree to be accountable *He* or *she* wants me to be accountable for communicating
Availability	A&B(&D)	C	*We* want to access or receive messages in time
Reachability	A B	B A	*I* want to reach him *He* or *she* wants to be reachable
Legal Enforceability	A(&D)	B(+C)	*I* want his promises to be legally enforceable

Properties of a Security Policy Model

A security policy model is a design artifact



Security Policy Model

Definition

A document that describes precisely and concisely which protection mechanisms are to be implemented

➜ based on attacker model

➜ is the basis for the system design

Characteristic Properties

1. Approved by the management
2. Rules are valid for all employees
3. Only required data is made available
4. All policy violations are reported

Important Documents of the Security Design

1. **Security Policy Model**
   - Security/protection properties that a system or a type of system should have
2. **Security Target**
   - Protection mechanisms provided by a concrete implementation to achieve certain objectives related to the properties of (**1.**)
3. **Protection Profile**
   - similar to (**2.**), but independent of the implementation, e.g. to enable the comparability of different products

Classification

There are *two types* of security policy models at the design level with the following properties.

➜ It provides a general security framework,

➜ and it has to be instantiated for specific applications

Models

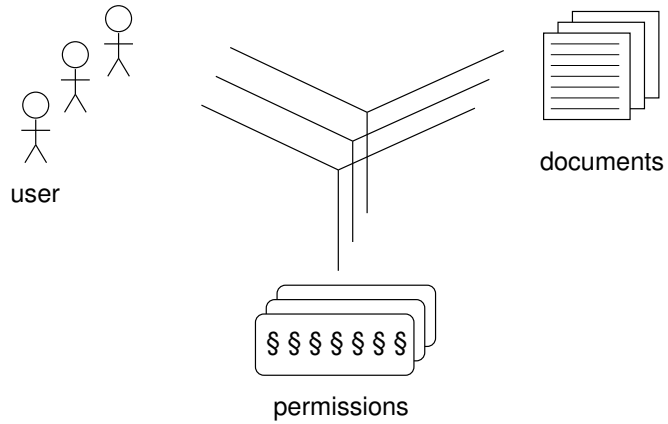
1. Multilevel Security
2. Multilateral Security

Access Control Strategies

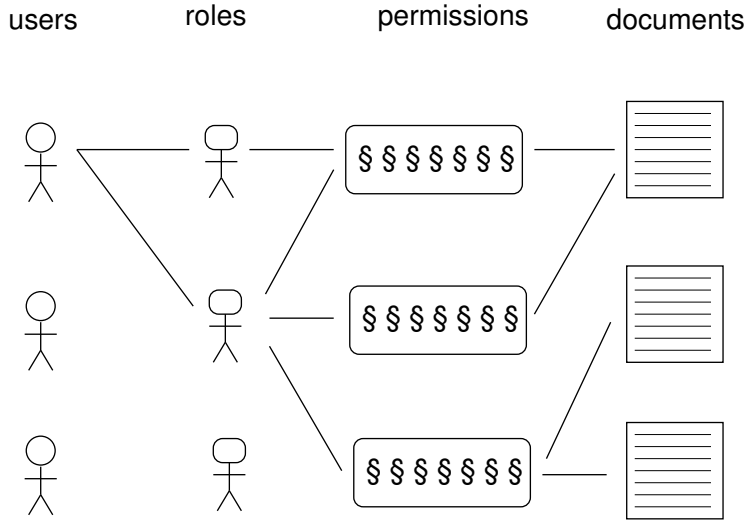
... are the core of a security policy model

1. **Discretionary Access Control (DAC)**
   - restricting access to objects based on the identity of subjects
2. **Role Based Access Control (RBAC)**
   - access control mechanism defined around roles and privileges
3. **Mandatory Access Control (MAC)**
   - the operating system constrains the ability of a subject to access to an object

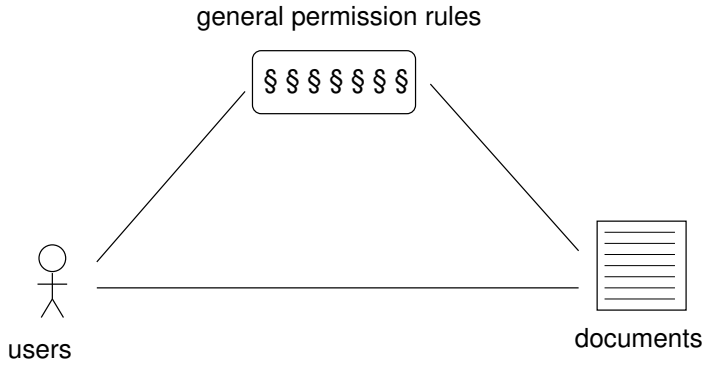
Discretionary Access Control (DAC)



Role Based Access Control (RBAC)



Mandatory Access Control (MAC)



Multilevel Security

Which type of access control is required for Multilevel Security?

Problem

- User-based Access Control is often not sufficient for security-critical applications, e.g. in the military domain

Solution

- Implementation of multilevel security concepts
- *System-based Access Control* (Mandatory Access Control, MAC)
- *Confidentiality* can be implemented using the Bell-LaPadula model (BLP)

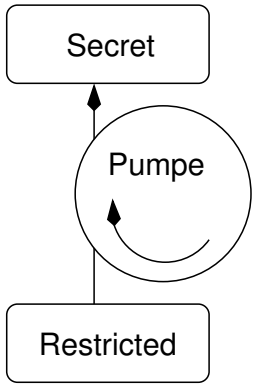
Bell-LaPadula Security Model (BLP)

- Developed by David Elliott Bell and Len J. LaPadula
- Late 1960s / early 1970s
- 1969: First practical implementation with the operating system MULTICS (predecessor of UNIX)
- 1973: Bell-LaPadula model was designed for the U.S. Air Force

  $\Rightarrow$ U.S. Air Force had increased security interest in its software (especially confidentiality)

How would a hardware design for BLP look like?

- Idea: Use of an *information pump* [Anderson01]
- Copy all data permanently from lower to higher security levels
- Benefit: Approach guarantees confidentiality
- Drawback: High costs



➜ Based on this simple idea, software solutions were developed

The most important elements of BLP are Security Classes

... **Security classes** are represented as pairs (A, C), where

A: Sensitivity level (security label)
C: Compartments (set of security categories)

Sensitivity level

0 unclassified
1 confidential
2 secret
3 top secret

Compartments (e.g.)

D doctor
N nurse
P patient
A admin staff

How to compare security classes?

Determinations for BLP

1. Sensitivity levels are *totally ordered*
   top secret (3) > secret (2) > confidential (1) > unclassified (0)
2. Compartments are sets which can only be *partially ordered*
   $\{\} \subseteq \{D\} \subseteq \{D, N\} \subseteq \ldots$

➜ Security classes form a lattice structure and are only partially ordered

Example

- Assuming there are three labels given
  $L_1 = (3, \{D, N, P\})$, $L_2 = (2, \{N\})$, $L_3 = (3, \{N, P, A\})$
- Is $L_1 \leq L_2$? no
- Is $L_2 \leq L_3$? yes
- Is $L_1 \leq L_3$? L_1 and L_3 are not comparable

How does access control work in BLP?

... Information from (A, C) to (A', C') shall flow if and only if

1. $A \leq A'$ and
2. $C \subseteq C'$

Two Rules for Confidentiality

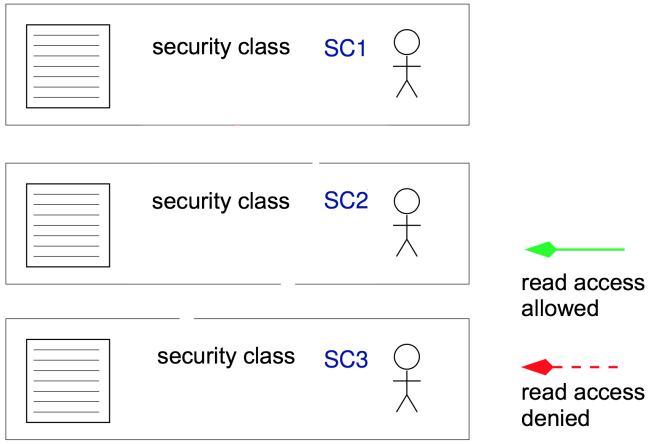
- No Read Up: Subjects are not allowed to read an object (data) from a higher security class
- No Write Down: Subjects are not allowed to write an object (data) of a lower security class

Determinations for BLP

- Security class of a subject is also called security *clearance*
- Security class of an object is also called security *classification*

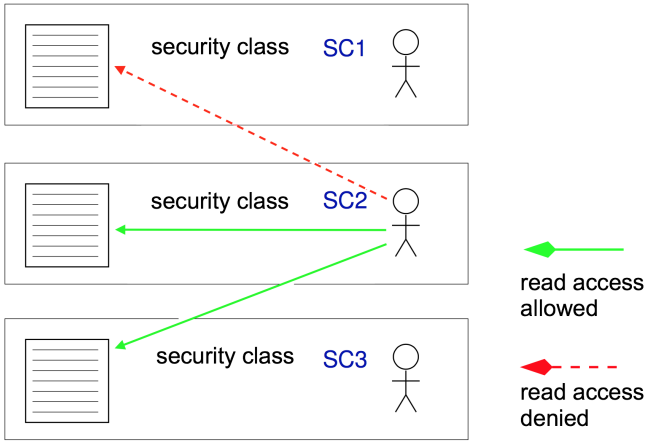
No Read Up (Simple Security Property)

... assumed if SC3 $\leq$ SC2 $<$ SC1, then what is allowed?



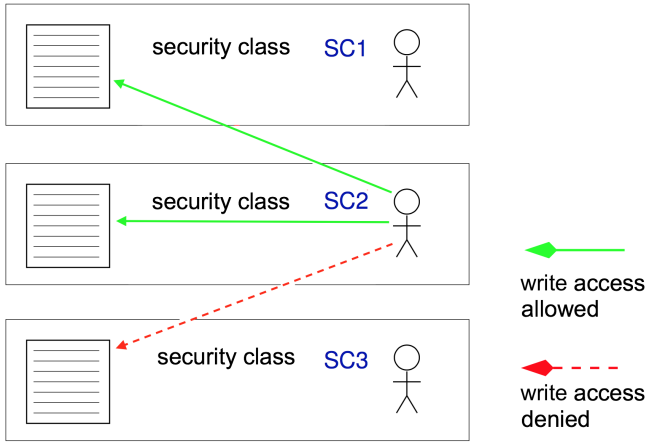
No Read Up (Simple Security Property)

... assumed if SC3 $\leq$ SC2 $<$ SC1, then what is allowed?

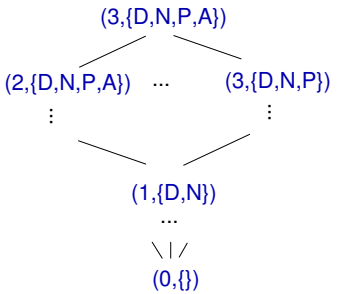


No Write Down (*-Property)

... assumed if $SC3 < SC2 \leq SC1$, then what is allowed?



Example: Hospital Scenario



Note:

- all compartments of a security class must be linked by conjunction
- e.g. $(\_, \{D, N\})$ means, reading is only allowed if the subject is authorized for both compartments doctor and nurse

1. Will it be possible for a person or process P with $SC = (1, \{D\})$ to read a document with $SC = (0, \{D\})$? yes
2. Is it possible for P to expand/write a document with $SC = (2, \{D, N\})$? yes
3. Are there documents that P is allowed to read and write at the same time? yes, documents with $SC = (1, \{D\})$!