CORPORATE TECHNOLOGY

Formal Security Analysis

Dr. David von Oheimb

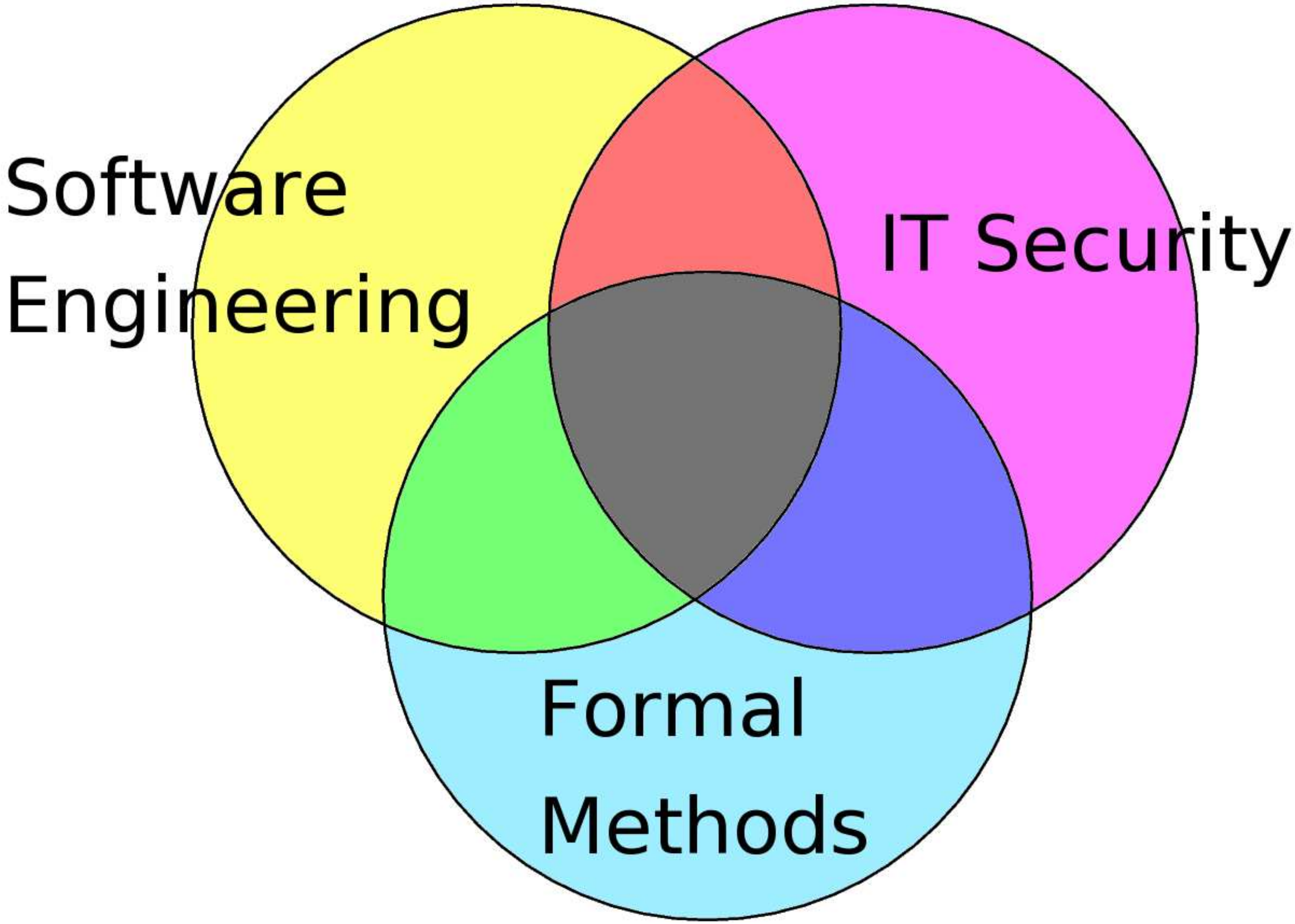
Munich, May 2005

Information &
Communications
Security

Overview

- What is Formal Security Analysis?
  - IT Security
  - Formal Modeling
  - Practical Considerations
  - Relation to Common Criteria

Formal Security Analysis: Areas



CORPORATE TECHNOLOGY

Overview

- What is Formal Security Analysis?

☞ **IT Security**

  – Formal Modeling

  – Practical Considerations

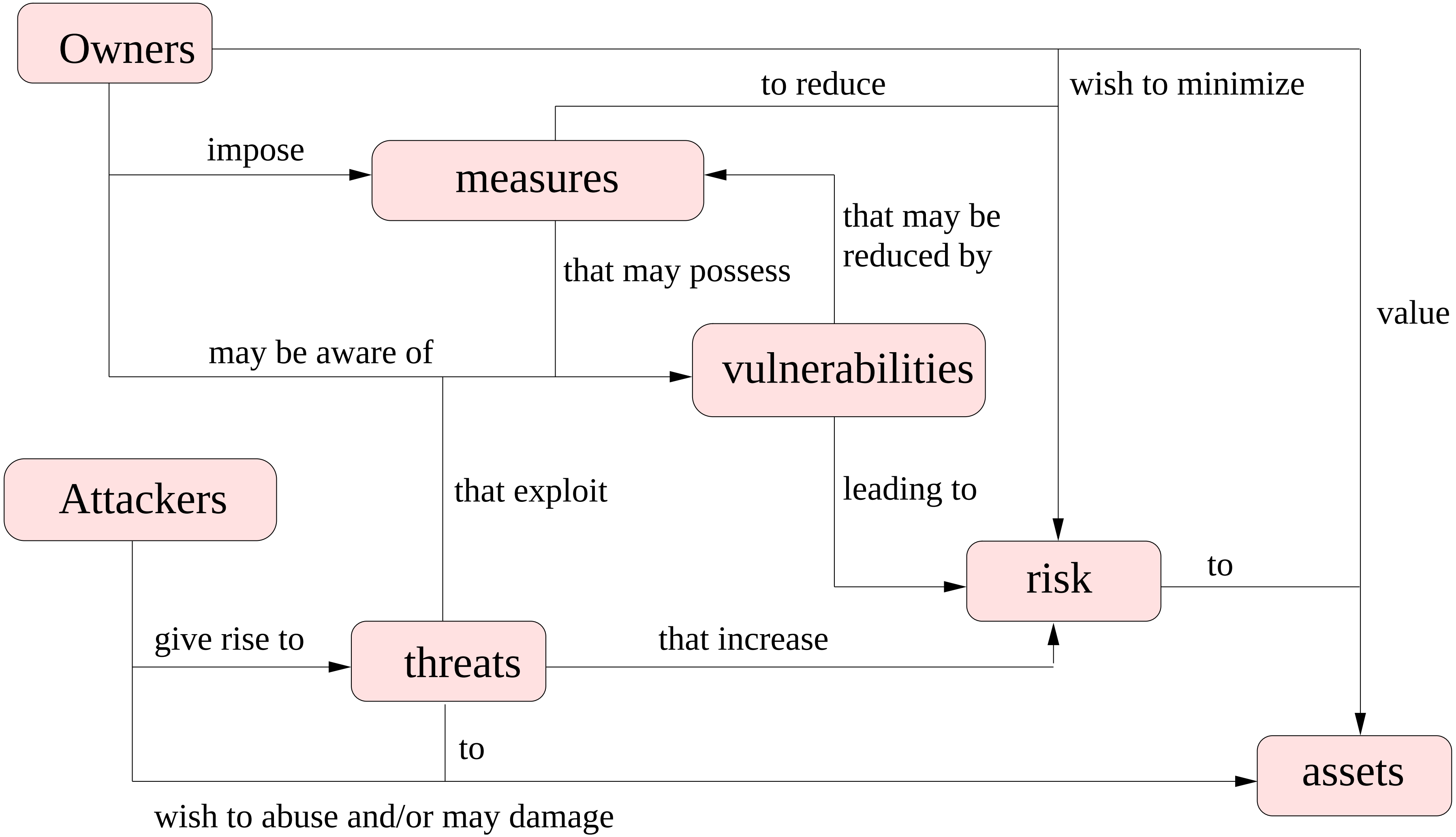
  – Relation to Common Criteria

IT Security

- IT/Computer security deals with the prevention, or at least detection, of unauthorized actions by users of a computer system.
  - Authorization is central to definition.
  - Sensible only relative to a security policy, stating who (or what) may perform which actions.
- Complements safety: prevent damage through errors or malfunction

CORPORATE TECHNOLOGY

Security Concepts and Relationships



Policy (here implicit) defines authorized actions on assets,

i.e., what constitutes legal use (or abuse/damage, respectively).

Information & Communications Security

Security as a Software Engineering Problem

Situation: security loopholes in IT systems will be actively exploited

— in this sense even worse than safety problems!

Goal: achieve absence of attacks by absence of vulnerabilities

— and convince yourself/contractors/customers of this!

Problem: IT systems are very complex, security flaws hard to find.

Security cannot be added on, but must be co-designed with the system.

Remedy: address security in all development phases.

Reviews supported by formal security modeling/analysis.

During ...

- **requirements analysis:** helps understanding the security issues
- **design, documentation:** helps improving the quality of specifications
- **implementation:** acts as correctness reference for testing/verification

Goals, Threats, and Mechanisms

Standard breakdown in security engineering:

Goals/Objectives: What to achieve

Threats: Which attacks to counter

Mechanisms How to achieve goals

Required for certification according to e.g. ITSEC and Common Criteria

Security Goals

- Goals: **CIA**

  Confidentiality No unauthorized disclosure/leakage of information

  Integrity: No unauthorized modification of information

  Availability: No unauthorized impairment of functionality

  All these require authorization = authentication + access control.

- Other goals

  Privacy: User data is only exposed in permitted ways.

  Nonrepudiation: One cannot deny responsibility for actions.

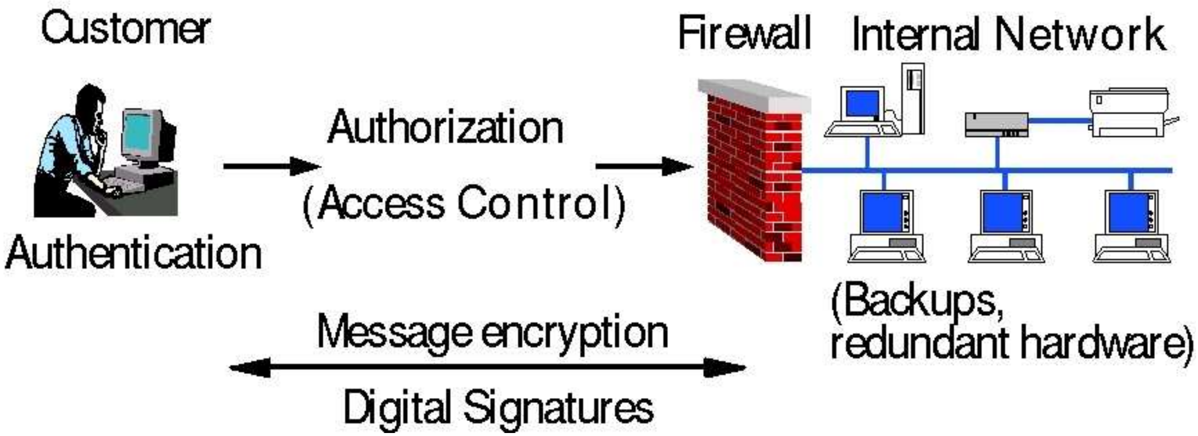
  Also called **accountability**

  Application specific requirements and combinations, e.g. e-voting

Threats

Confidentiality	Interception	Unauthorized party gains access to information
Integrity	Fabrication	Generation of additional data or activities
Integrity	Modification	Unauthorized tampering of data or services
Integrity, Availability	Interruption	Service or data becomes unavailable or unusable

Security Mechanisms



- Various mechanisms are used to achieve goals.
- Designing adequate mechanisms is challenging.
- One must be cognizant of the tradeoffs and costs involved.

Overview

- What is Formal Security Analysis?
  - IT Security
  - ☞ **Formal Modeling**
  - Practical Considerations
  - Relation to Common Criteria

Security Policies and Models

- A security policy defines what is allowed (actions, data flow, etc.) typically by a relationship between subjects and objects.
- A security model is a (+/- formal) description of a policy and mechanisms, usually in terms of system state or sequences of states (traces).
- Security verification proves wrt. model that mechanisms enforce policy
- Models usually focus on specific characteristics of the reality (policies).
- Types of (formal) security models
  - Access Control models
  - Information Flow models
  - Cryptoprotocol models

What are Formal Methods?

- A language is formal if it has a well-defined syntax and semantics.

  Examples: Predicate logic, automata, λ-calculus, process algebra, ...

- A model is formal if it is specified with a formal language.

  Example:

$$\forall x.\ bird(x) \rightarrow flies(x) \qquad bird(tweety)$$

- A proof is formal if it is done using a deductive system (i.e., a set of precise rules governing each proof step).

  Examples: Tableau calculus, axiomatic calculus, term rewriting, ...

- A formal proof is machine-assisted if it is performed, or at least checked, by an IT system.

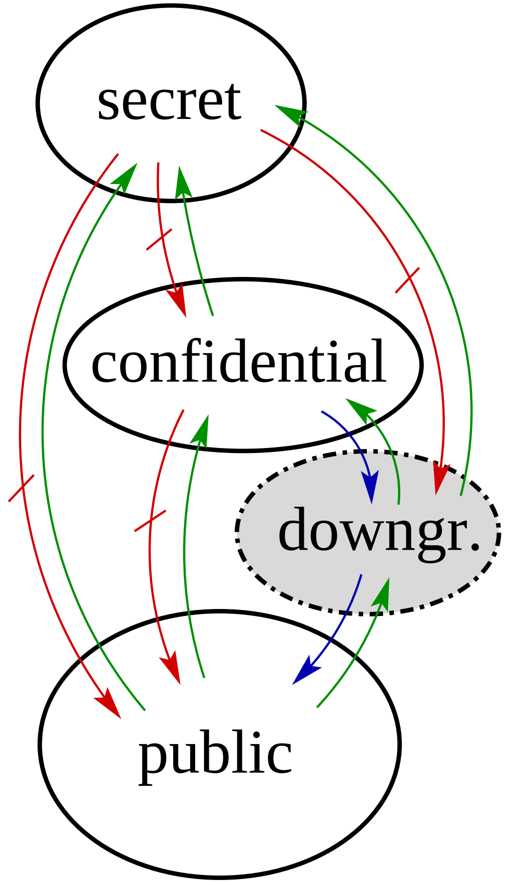
  Examples: OFMC (model checker), Isabelle (theorem prover)

Access Control models

- Discretionary vs. mandatory AC models.
- Various types of models:
  - Models can capture policies
    for confidentiality (Bell-LaPadula)
    or for integrity (Biba, Clark-Wilson).
  - Some models apply to static policies (Bell-LaPadula),
    others consider dynamic changes of access rights (Chinese Wall).
  - Security models can be informal (Clark-Wilson), semi-formal,
    or formal (Bell-LaPadula, Harrison-Ruzzo-Ullman).

Information Flow models

- Identify domains holding information
- Specify allowed flow between domains
- Check the observations that can be made about state and/or actions
- Consider also indirect and partial flow



- Classical model: Noninterference (Goguen & Meseguer)
- Many variants: Non-deducability, Restrictiveness, Non-leakage, ...

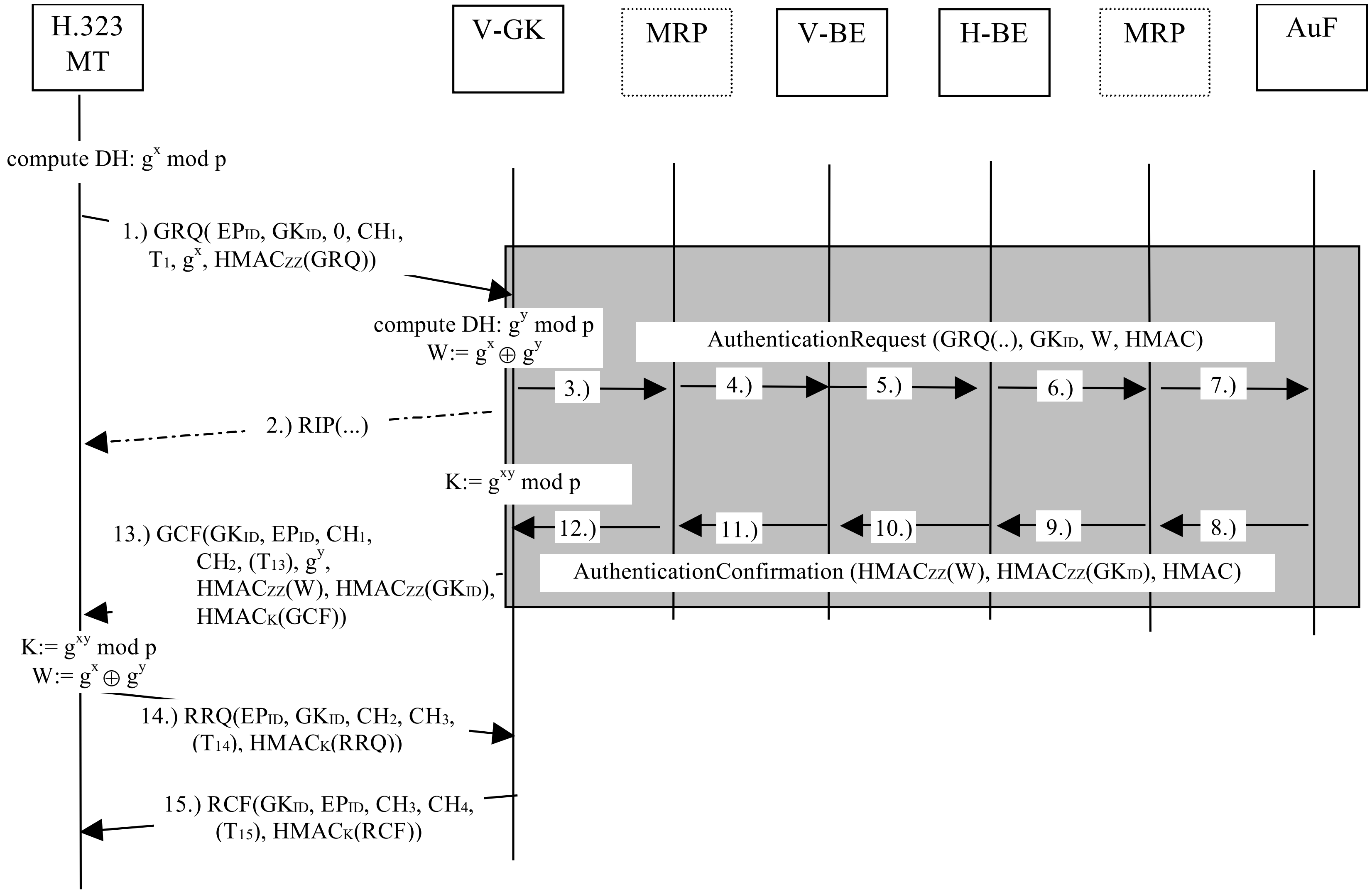
Cryptoprotocol models

- Describe message traffic between processes or principals

- Take cryptographic operations as perfect primitives
- Specified with by domain-specific languages
- Describe secrecy, authentication, . . . goals
- Are typically verified automatically using model-checkers

CORPORATE TECHNOLOGY

H.530: Authentication for Mobile Roaming



Two vulnerabilities found and corrected. Solution patented.

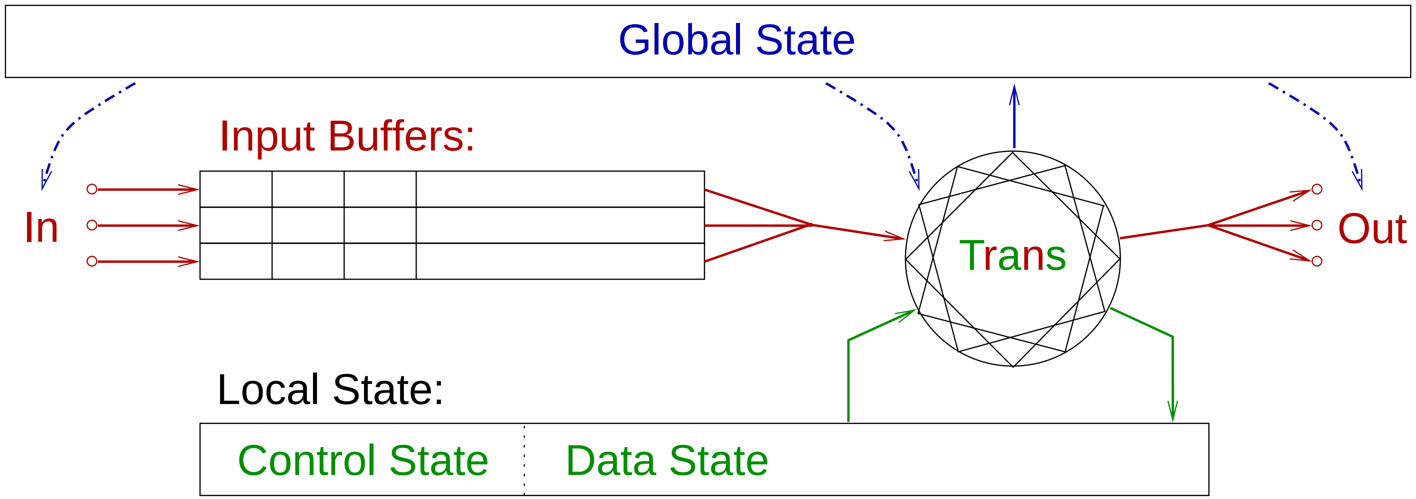
Information & Communications Security

Interacting State Machines (ISMs)

Automata with (nondeterministic) state transitions +

buffered i/o simultaneously on multiple connections

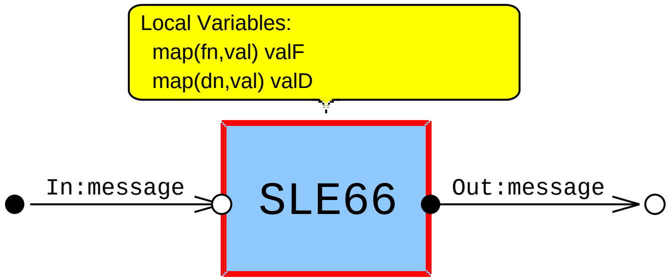
ISM system may depend on global state



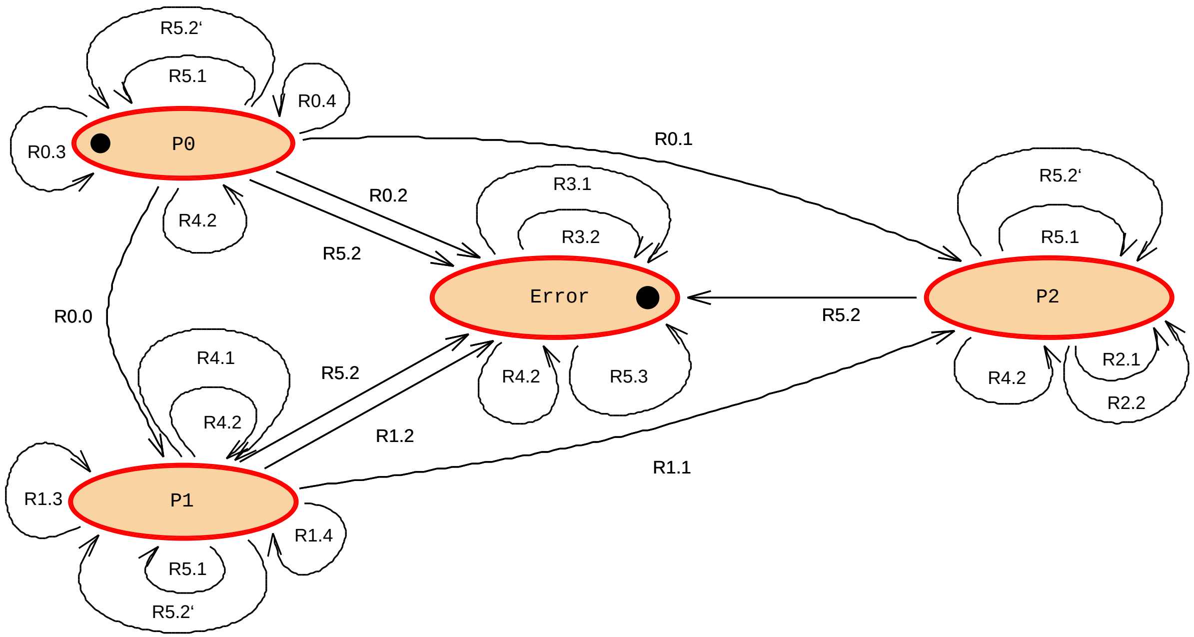
Applicable to a large variety of reactive systems

LKW Model of Infineon SLE 66 Smart Card

System Structure Diagram:



State Transition Diagram (abstracted):



First higher-level (EAL5) certification for a smart card processor!

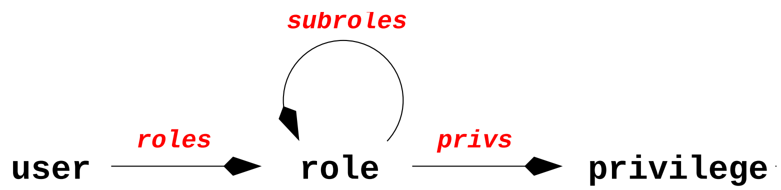
RBAC of Complex Information System

Privileges:

$\textit{roles} \subseteq \texttt{user} \times \texttt{role}$

$\textit{subroles} \subseteq \texttt{role} \times \texttt{role}$

$\textit{privs} \subseteq \texttt{role} \times \texttt{privilege}$



$$(u, p) \in \textit{roles} \circ \textit{subroles}^* \circ \textit{privs}$$

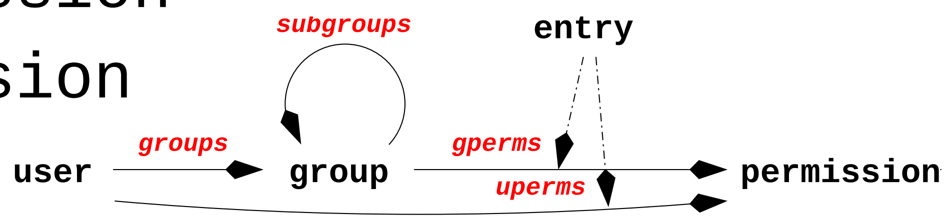
Permissions:

$\textit{groups} \subseteq \texttt{user} \times \texttt{group}$

$\textit{subgroups} \subseteq \texttt{group} \times \texttt{group}$

$\textit{gperms} \subseteq \texttt{group} \times \texttt{permission}$

$\textit{uperms} \subseteq \texttt{user} \times \texttt{permission}$



$$(u, p) \in (\textit{groups} \circ \textit{subgroups}^* \circ \textit{gperms}(e)) \cup \textit{uperms}(e)$$

“nagging questions” $\rightsquigarrow$ clarification improving specification quality

Overview

- What is Formal Security Analysis?
  - IT Security
  - Formal Modeling
  - ☞ **Practical Considerations**
  - Relation to Common Criteria

Shaping a Formal Model

Choice of Formalism: dependent on ...

- application domain, modeler's experience, tool availability, ...
- formalism should be simple, expressive, flexible, mature

Formality Level: should be adequate:

- the more formal, the more precise,
- but requires deeper mastering of formal methods

Abstraction Level: should be ...

- high enough to achieve clarity
- low enough not to loose important detail

refinement allows for both high-level and detailed description

Information Necessary

Overview: architecture and components, e.g. authentication services, PKI

Security-related concepts: actors, objects, states, messages, . . .

Threats/security goals/objectives: which attacks shall be countered.

Described in detail such that concrete verification goals can be set up,

e.g. integrity: which contents shall only be generated/modified by whom

from when to when, or on transit from where to where

Security mechanisms: their relation to goals and how they are applied,

e.g. who signs which contents for what purpose and where checked.

Described precisely but at high level (no implementation details required),

e.g. abstract message contents/format but not concrete syntax

CORPORATE TECHNOLOGY

Overview

- What is Formal Security Analysis?
  - IT Security
  - Formal Modeling
  - Practical Considerations

☞ **Relation to Common Criteria**

CC: Goals & General Approach

Common Criteria
...the standard for Information Security

Goal: Gaining confidence in the security of a system

- What are the goals to be achieved?
- Are the measures employed appropriate to achieve the goals?
- Are the measures implemented correctly?

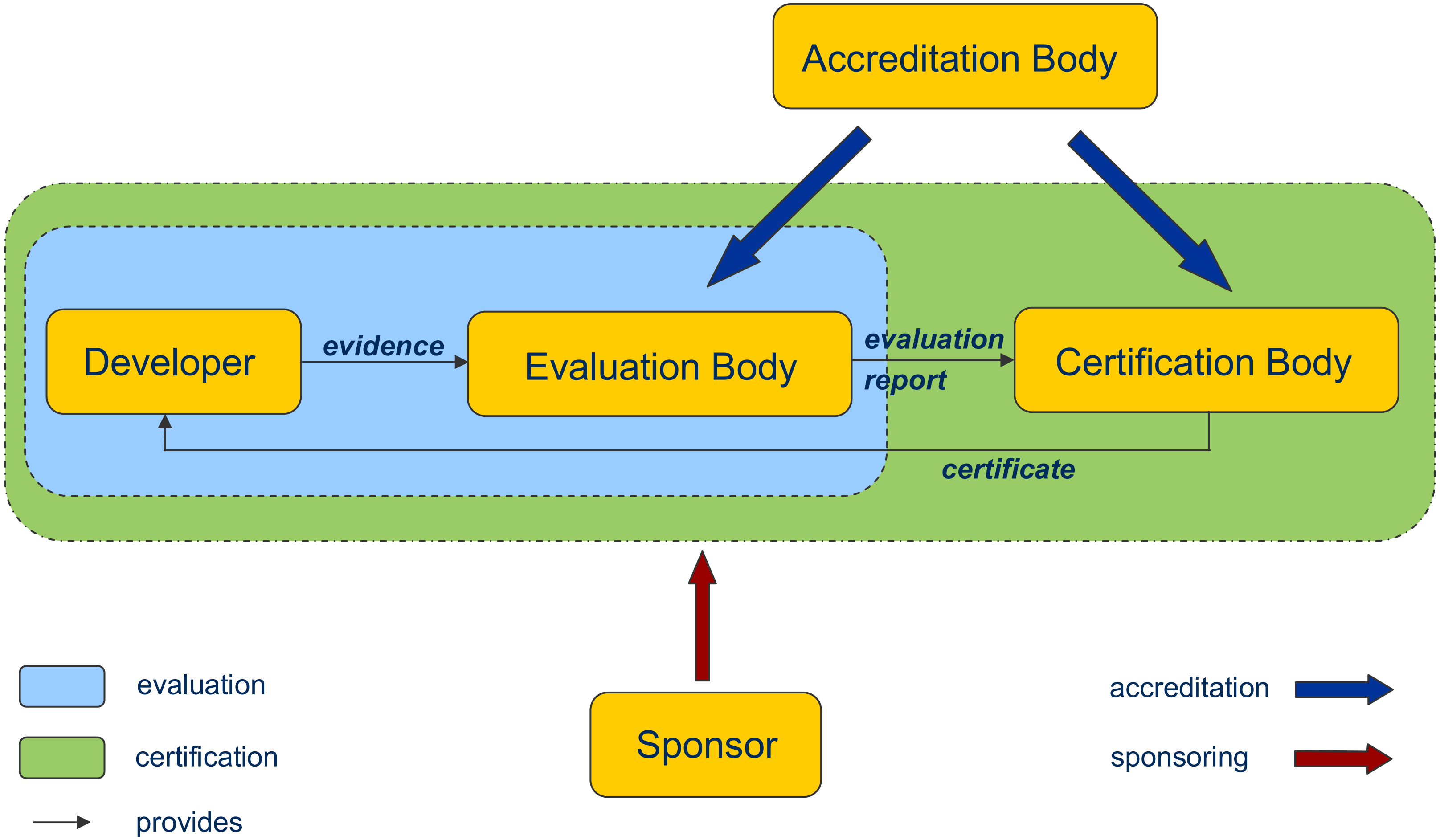
Approach: assessment (evaluation) of system security by neutral experts

- Understanding how the system's security functionality works
- Gaining evidence that security functionality is correctly implemented
- Gaining evidence that the integrity of the system is kept

Result: Successful evaluation is awarded a certificate

CORPORATE TECHNOLOGY

CC: Process Scheme



Information & Communications Security

CC: Security Target

- Definition of the Target of Evaluation (TOE) and separation from its environment
- Definition of the TOE's security threats, objectives and requirements
- Introduction of TOE Security Functions (TSF): measures intended to counter the threats
- Determination of Evaluation Assurance Level (EAL)

$\Rightarrow$ The Security Target is the document to which all subsequent evaluation activities and results refer!

$\Rightarrow$ Interpretation of results is only reasonable if referring to the ST context

CC: Evaluation Assurance Levels

EAL1: functionally tested

EAL2: structurally tested

EAL3: methodically tested and checked

EAL4: methodically designed, tested, and reviewed,
including security policy model

EAL5: semiformally designed and tested
including formal security policy model

EAL6: semiformally verified design and tested

EAL7: formally verified design and tested

Increasing requirements on scope, depth and rigor

CC: EAL example: EAL5

In red: additional requirements compared to EAL4

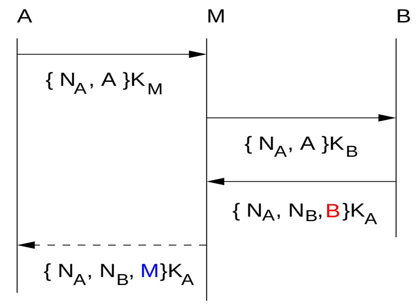
- Complete source code is subject to analysis
- Formal security policy model
- Semiformal description techniques
- Modular design
- Documentation of developer's tests up to low-level design
- Vulnerability analysis refers to moderate attack potential
- Covert channel analysis
- Comprehensive configuration management

CC: How to scale an Evaluation

- Separation of TOE and TOE environment
- Detail level of TOE summary specification
- Definition of security objectives
- Definition of security functional requirements
- Strength-of-function claims
- EAL selection

Why are Formal Security Models so useful?

A formal security model is an abstract formal description of a system (and its environment) that focuses on the relevant security issues.



- improves understanding of security issues by
  - abstraction: concentration on the essentials helps to keep overview
  - systematic approach: generic patterns simplify the analysis
- prevents ambiguities, incompleteness, and inconsistencies

  and thus enhances quality of specifications
- provides basis for systematic testing or even formal verification

  and thus validates correctness of implementations