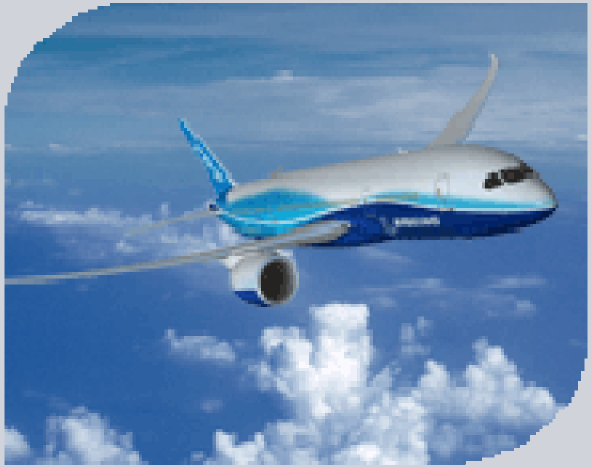
Corporate Technology

Product certification and formal security analysis at industrial examples



Dr. David von Oheimb
Siemens Corporate Technology, IT Security

Guest lecture in the System Security series on invitation by Prof. Posegga, University of Passau, Germany, 8 Jul 2013

http://web.sec.uni-passau.de/teaching/ »Software-Sicherheit«

Overview

- **IT Security at Siemens Corporate Technology**
- Software distribution systems
- Common Criteria certification
- Smart Metering security requirements
- Formal security analysis
- Research project AVANTSSAR
- Conclusion on formal security analysis

Siemens Corporate Technology (CT)

Networking the integrated technology company

SIEMENS

Customers

Chief Technology Officer (CTO)

- Review innovation strategies
- Drive technology based synergies
- Secure the innovation power
- Technology assessments
- Governance and guidance

Sectors / Divisions

Energy

Healthcare

Industry

Infrastructure & Cities

Regions

Chief Technology Office (CT O)
- Direct support of CTO

Corporate Research and Technology Center (CT RTC)
- Technology Fields with multiple impact
- Pictures of the Future
- Accelerators

Corporate Development Center (CT DC)
- Software development partner for the Sectors

Corporate Intellectual Property and Functions (CT IP)
- Intellectual property
- Standardization and regulation
- Information research

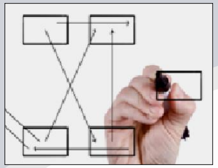
Corporate Technology (CT)

Siemens corporate RTC: some 1,800 researchers

Present in all leading markets and technology hot spots

SIEMENS

IT Security topics at Siemens Corporate Technology



Security lifecycle
Sustainable integration of IT security topics into product lifecycle processes

Security assessment
"Friendly" hacking and assessments of products, solutions, applications and processes

Security architectures
Domain specific security architectures, certification, and best practice use of COTS and Open Source security

Siemens product CERT
Incident handling and vulnerability management for Siemens products & solutions

IT Security @ Siemens CT

Embedded systems security
Optimized and adequate security for embedded systems

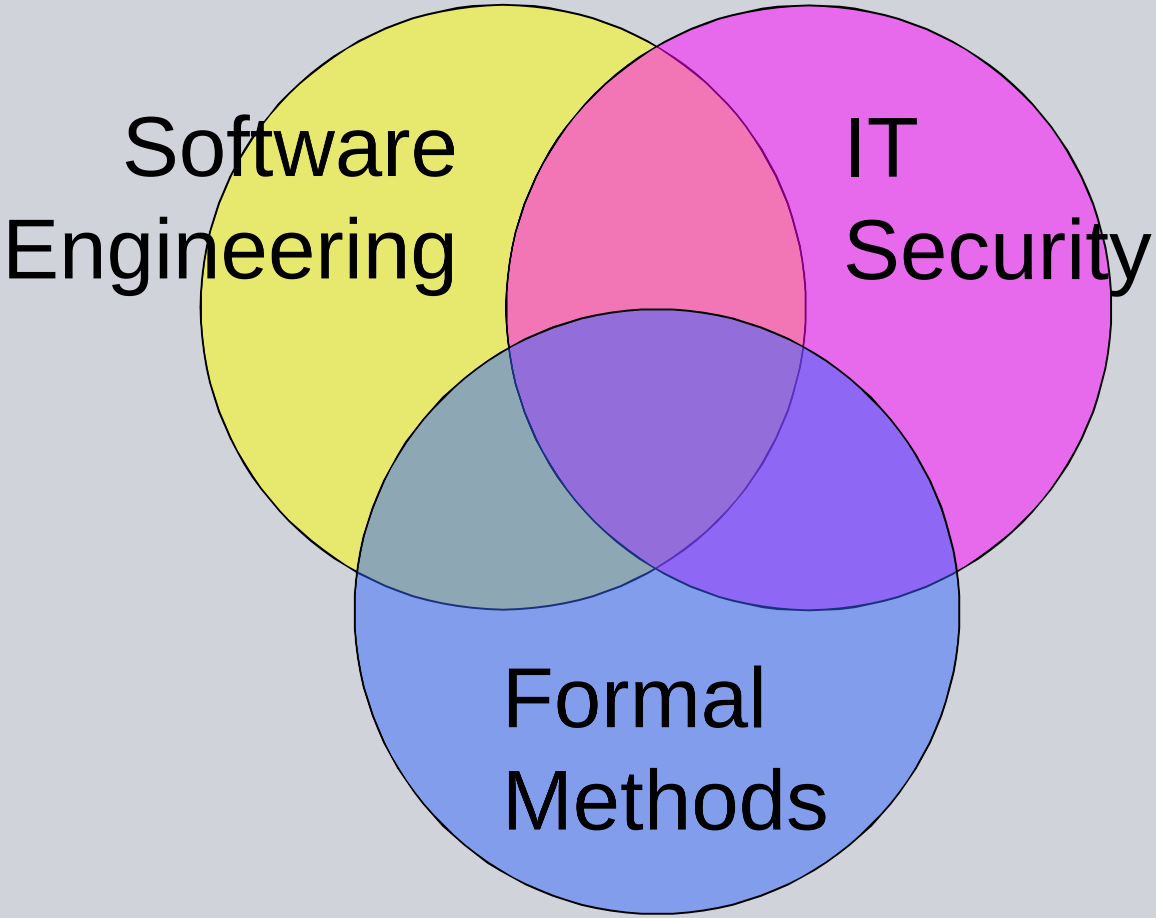
Computer Emergency Response Team (CERT)
Corporate incident handling and technical policies

Cyber Security for specific regions

Regional Support focusing on specific security regulations and application topics like NERC-CIP, HIPAA, DIACAP (USA) or industrial control system security (Asia)

SIEMENS

Fields

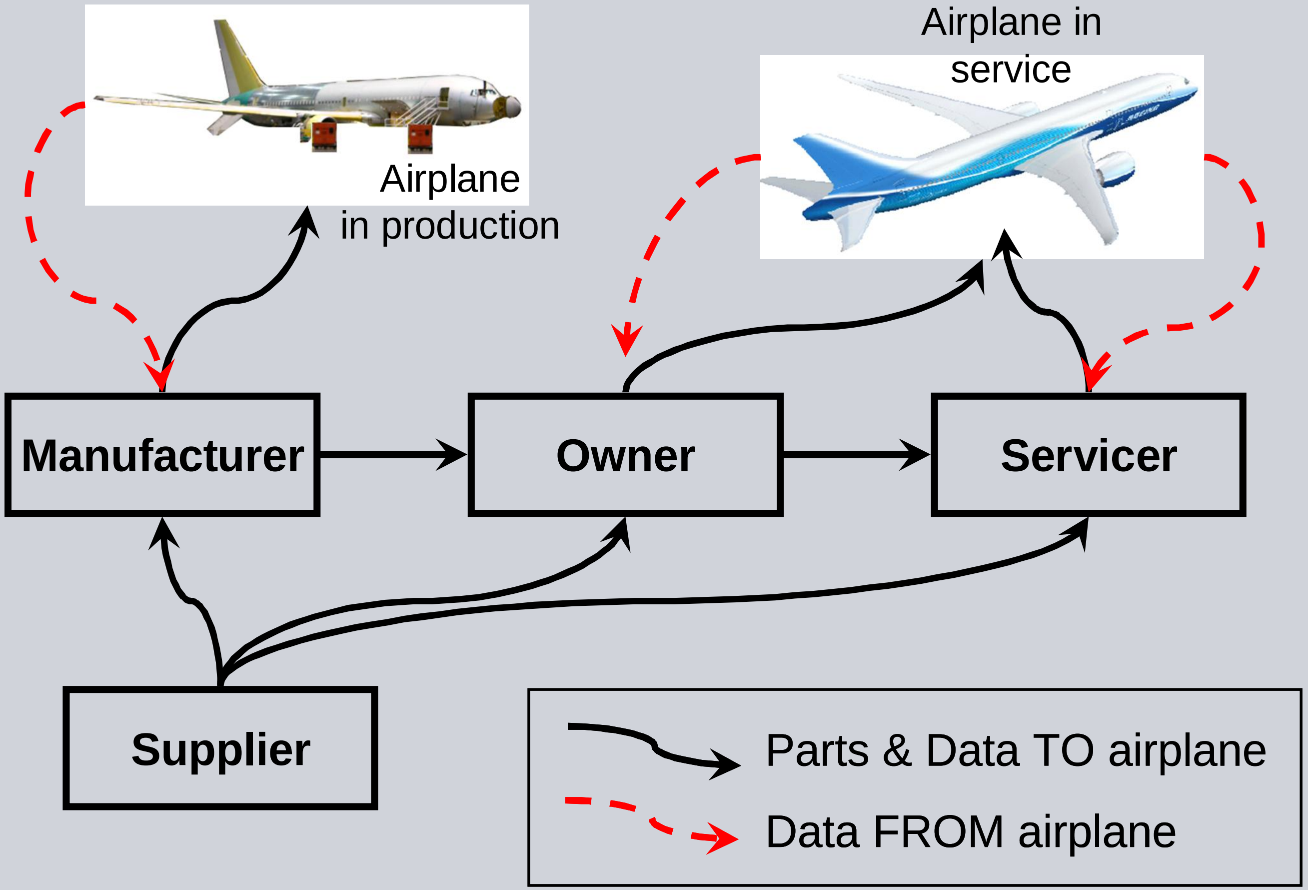


Overview

- IT Security at Siemens Corporate Technology
- **Software distribution systems**
- Common Criteria certification
- Smart Metering security requirements
- Formal security analysis
- Research project AVANTSSAR
- Conclusion on formal security analysis

Airplane Assets Distribution System (AADS)

AADS is a system for storage and distribution of airplane assets, including *Loadable Software Airplane Parts* (LSAP) and airplane health data



Airplane Assets Distribution System architecture

A complex distributed store-and-forward middleware with OSS components

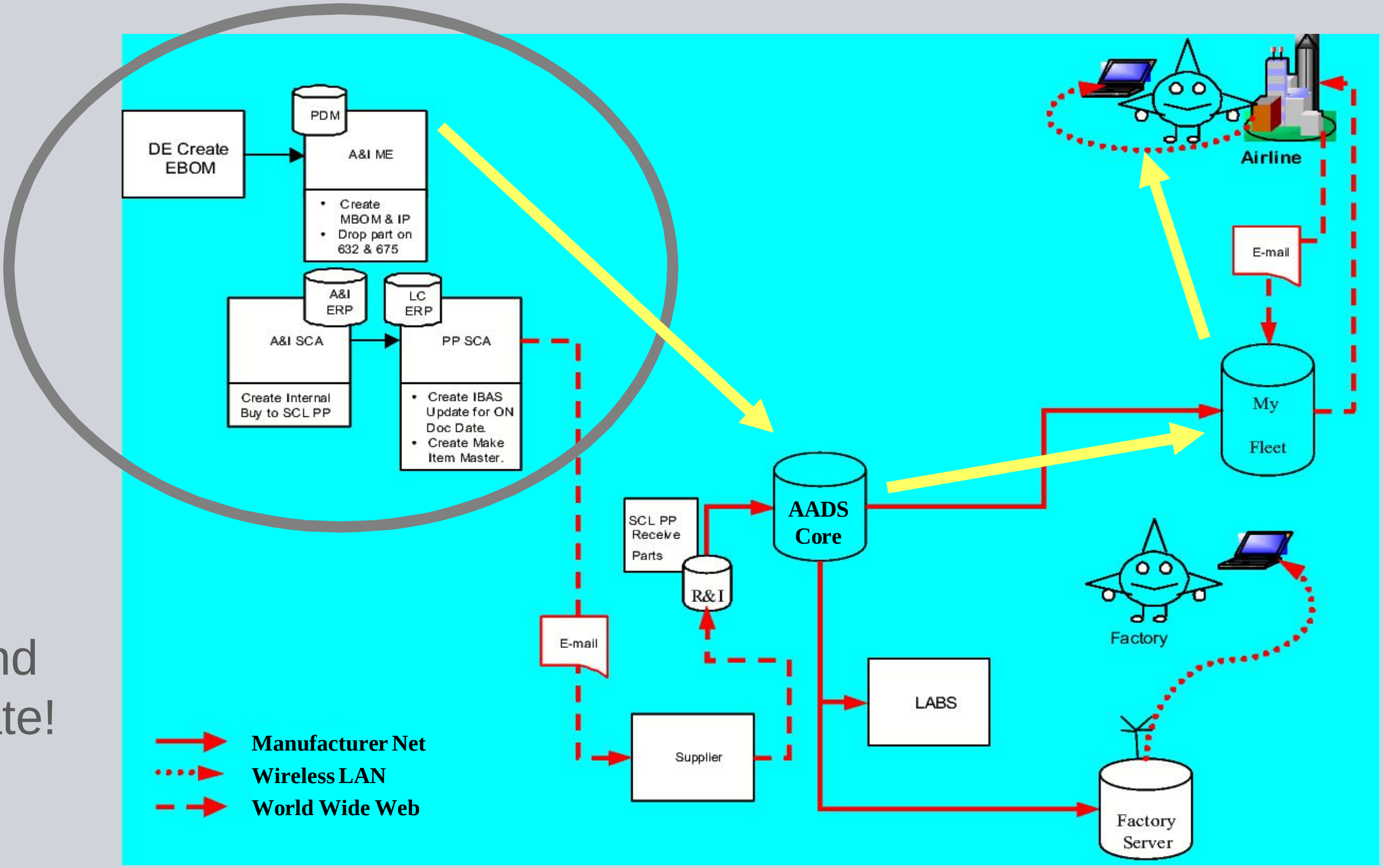
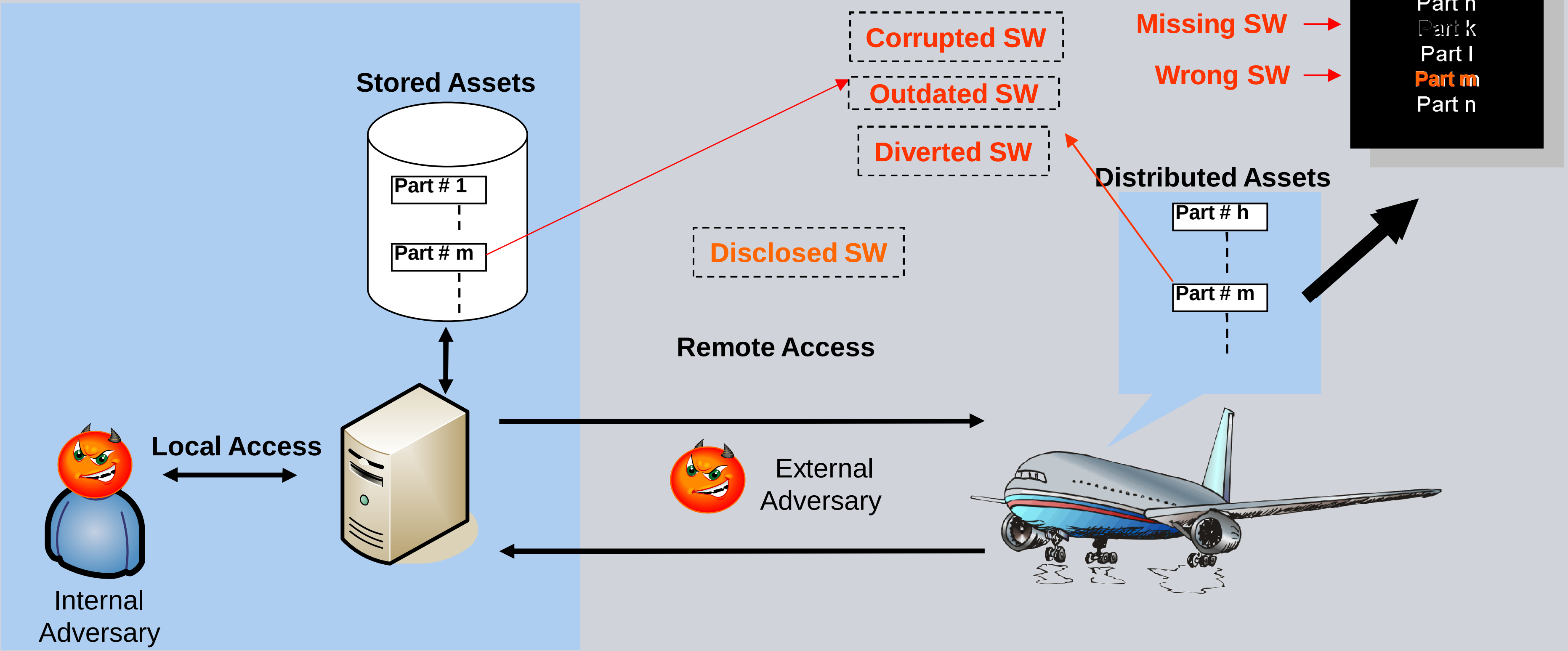


Figure is simplified and not up-to-date!

Security threats at the AADS example

SIEMENS

Attacker's objective: lower airplane safety margins by tampering LSAP, i.e., software to be distributed to aircraft and executed onboard in flight.

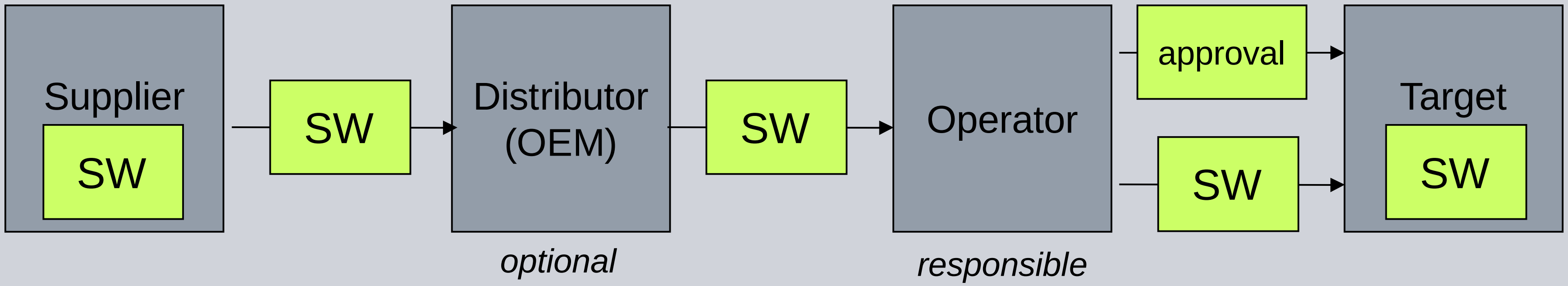


Corruption/Injection **Wrong Version** **Diversion** **Disclosure**

Software Distribution System (SDS)

ICT systems with networked devices in the field
performing safety-critical and/or security-critical tasks.
Field devices require secure software update.

→ Software Distribution System (SDS):
System providing secure distribution of software (SW)
from software supplier to target devices in the field



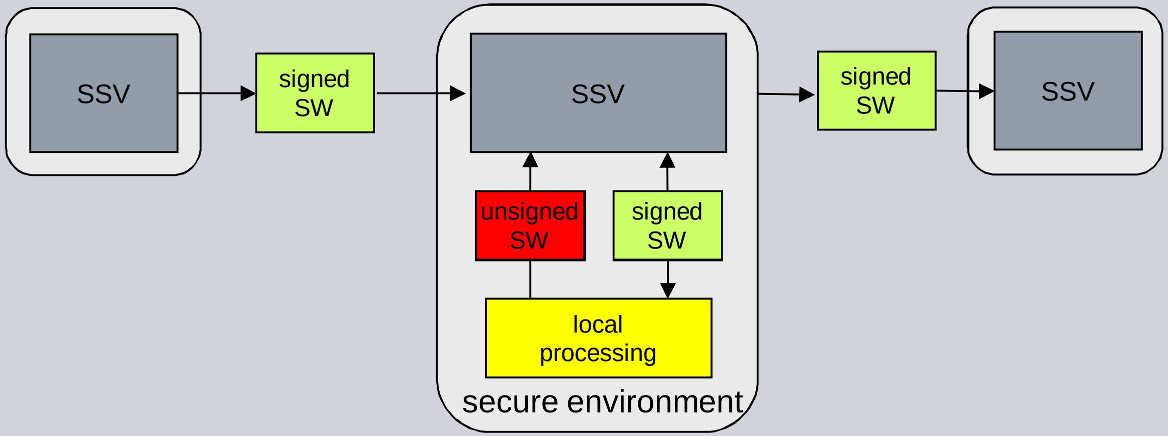
Transition from media-based (CD-ROMs etc.) to networked SW transport increases security risks due to transport over open, untrusted networks

SIEMENS

Software Signer Verifier (SSV)

Each node in SDS runs an SSV instance, used for:

- Introducing initially unsigned software into the SDS, by digitally signing and optionally encrypting it
- Verifying the signature on software received from other SSVs, checking integrity, authenticity and authorization of the sender
- Approving software by adding an authorized signature
- Delivering software out of the SDS after successfully verifying it



Overview

- IT Security at Siemens Corporate Technology
- Software distribution systems
- **Common Criteria certification**
- Smart Metering security requirements
- Formal security analysis
- Research project AVANTSSAR
- Conclusion on formal security analysis

IT Security as a System Engineering Problem

- IT security aims at preventing, or at least detecting, unauthorized actions by agents in an IT system.

In the AADS context, security is a prerequisite of safety.

- Safety aims at the absence of accidents (→ airworthiness)

Situation: security loopholes in IT systems actively exploited

Objective: thwart attacks by eliminating vulnerabilities

Difficulty: IT systems are pretty complex. Security is interwoven with the whole system, so very hard to assess.

Remedy: evaluate system following the Common Criteria approach

- address security systematically in all development phases
- perform document & code reviews and tests
- for maximal assurance, use formal modeling and analysis

Common Criteria (CC) for IT security evaluation

Common Criteria

product-oriented methodology

for IT security assessment

ISO/IEC **standard** 15408

Current version: 3.1R3 of Jul 2009

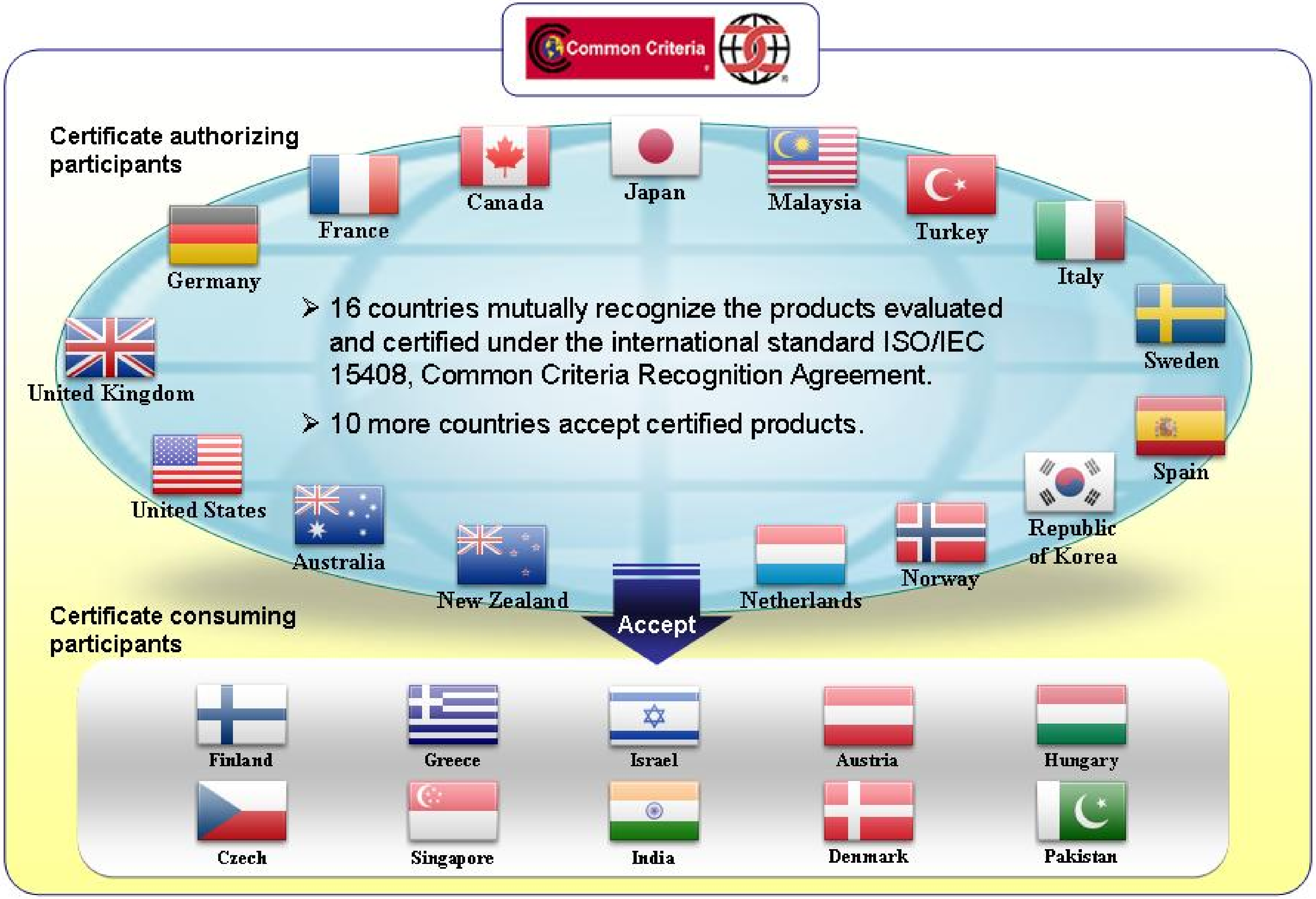
Aim: gain confidence in the security of a system

Approach: assessment of system and documents by neutral experts

- What are the objectives the system should achieve?
- Are the measures employed appropriate to achieve them?
- Are the measures implemented and deployed correctly?

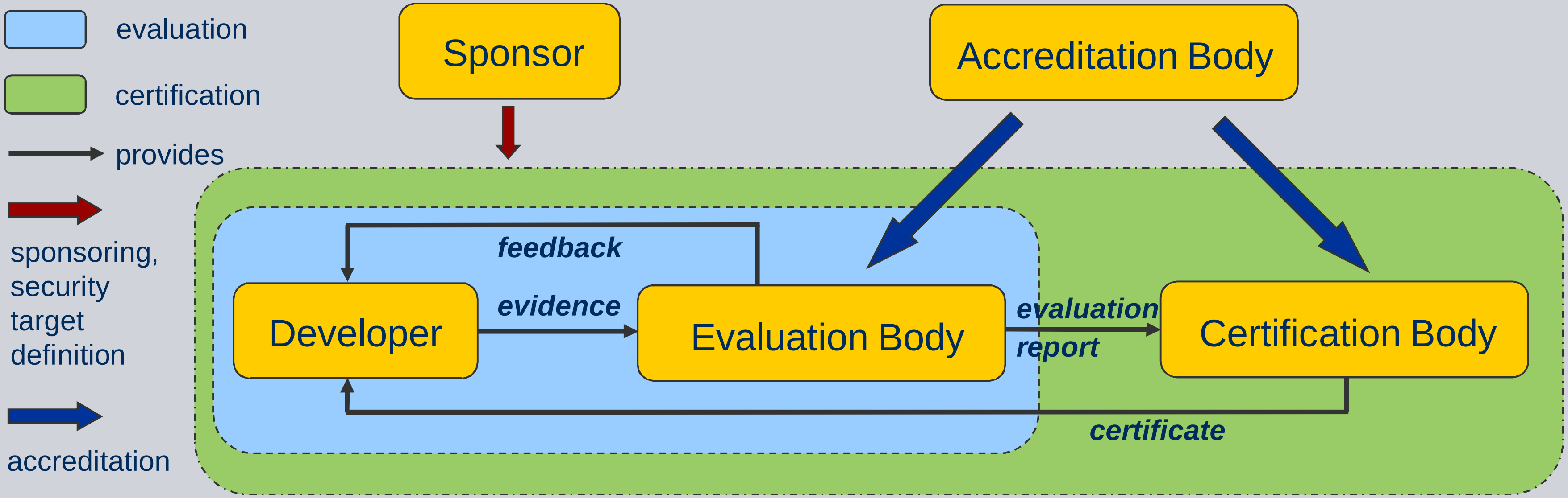
SIEMENS

CC: authorization and international acceptance of certificates



SIEMENS

Common Criteria process overview



Certification according to the Common Criteria is a rather complex, time consuming and expensive process, providing systematic assurance.

A successful, approved evaluation is awarded a certificate.

Lifetime of certificates is theoretically not bounded, but their applicability is limited by technical progress (→ re-certification).

CC: Security requirements documents

Security Target (ST): defines extent and depth of the evaluation

for a specific product called *Target of Evaluation (TOE)*

Protection Profile (PP): defines extent and depth of the evaluation

for a whole class of products, i.e. firewalls

STs and PPs may inherit (‘*claim*’) other PPs.

ST and PP specifications use **generic** “construction kit”:

- Building blocks for defining *Security Functional Requirements (SFRs)*
- Scalable in depth and rigor: *Security Assurance Requirements (SARs)*

layered as *Evaluation Assurance Levels (EALs)*

SIEMENS

CC: Security Target or Protection Profile example overview

Security problem

TOE: Power Plant control

Target of Evaluation

T.1 Unauthorized access to control elements.
T.2 System data corrupted.

Threats

OSP.1 Unused ports and services are disabled.

Organizational security policies

A.1 Administrators are trustworthy.

Assumptions

Solution definition

Security objectives for the Target of Evaluation (TOE)

O.1 Users are authorized before being granted access to the TOE.
O.2 The TOE has to ensure that the integrity of critical system data is preserved.

Security objectives for the operational environment

OE.1 the system administrator disables the following services and ports: …
OE.2 organizational measures ensure that all administrators are competent and trustworthy.

Security Functional Requirements

FIA_UAU.2 User authentication
FDP_ACF.1 Access control
FPT_ITI.1 Detection of modification
FPT_FLS.1 Failure with preservation of secure state

Security Assurance Requirements

EAL 2+: EAL 2 and additionally:
AVA_VAN.3 Focused vulnerability analysis

Threats Addressed by the AADS Security Objectives

Objectives	Threats	Safety-relevant				Business-relevant			
		Corruption	Misconfiguration	Diversion	Staleness	Unavailability	Late Detection	False Alarm	Repudiation
Safety-relevant	Integrity	√							
	Correct Destination			√					
	Latest Version				√				
	Authentication	√	√						√
	Authorization	√	√						
	Timeliness				√				
Business-Relevant	Availability					√			
	Early Detection						√		
	Correct Status							√	
	Traceability	√	√						√
	Nonrepudiation								√
Environment	Part_Coherence	√	√	√					
	Loading_Interlocks	√	√	√					
	Protective_Channels	√							
	Network_Protection				√	√			
	Host_Protection	√							√
Assumptions	Adequate_Signing	√							
	Configuration		√						
	Development	√	√	√	√	√	√	√	√
	Management	√	√						√

CC: Security Functional Requirements (SFRs) overview

FAU: Security audit

- Security audit automatic response (FAU_ARP)
- Security audit data generation (FAU_GEN)
- Security audit analysis (FAU_SAA)
- Security audit review (FAU_SAR)
- Security audit event selection (FAU_SEL)
- Security audit event storage (FAU_STG)

FCO: Communication

FCS: Cryptographic support

FDP: User data protection

FIA : Identification and authentication

FMT: Security management

FPR: Privacy

FPT: Protection of the TSF

FRU: Resource utilization

FTA: TOE access

FTP: Trusted path/channels

SIEMENS

CC: Evaluation Assurance Levels

Assurance requirements are grouped as Evaluation Assurance Levels:

	EAL designation
EAL1	functionally tested
EAL2	structurally tested
EAL3	methodically tested and checked
EAL4	methodically designed, tested and reviewed
EAL5	semiformally designed and tested
EAL6	semiformally verified design and tested
EAL7	formally verified design and tested

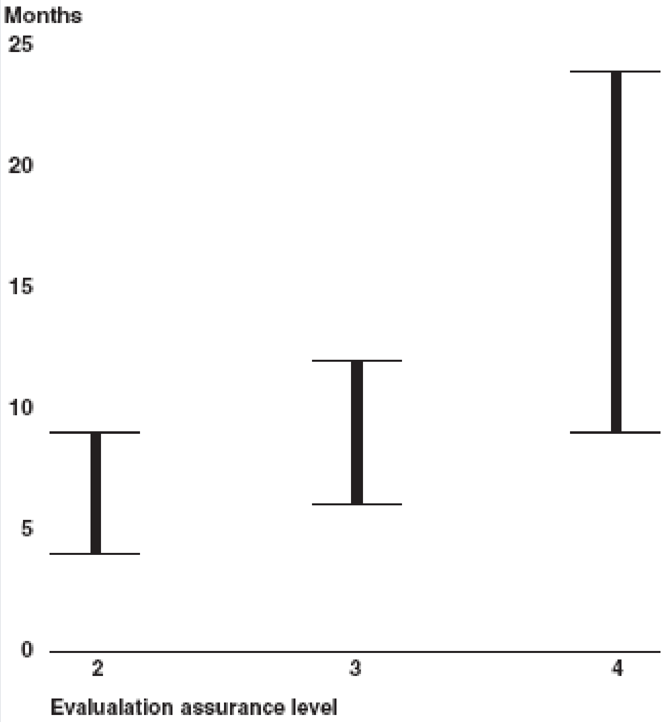
Increasing requirements on scope, depth and rigor of evaluation.

EAL does not say how secure a product is, but how well its requirements are checked.

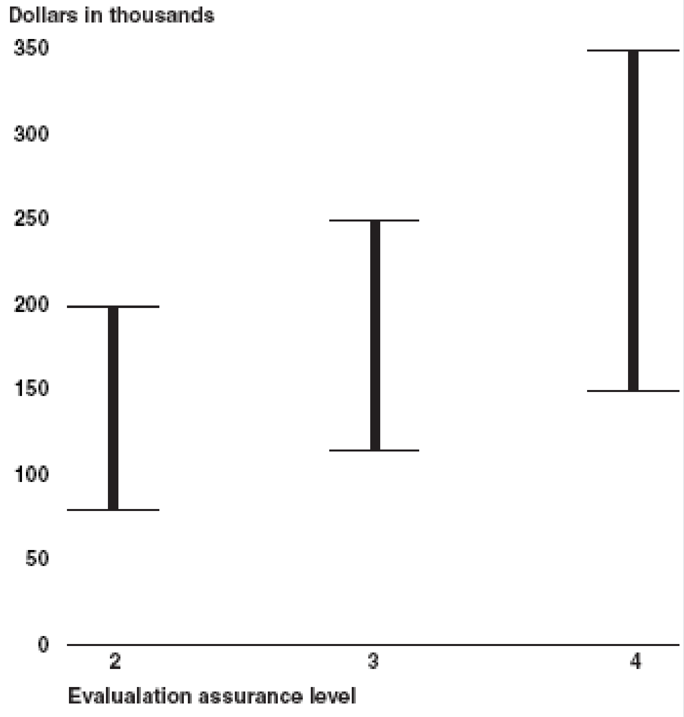
Assurance is grounds for confidence that an IT product meets its security objectives.

CC: Factors determining the evaluation effort

- Boundary of TOE vs. TOE environment
- Definition of Threats and Security Objectives for the TOE
- Definition of Security Functional Requirements (SFRs)
- Selection of Evaluation Assurance Level (EAL)



Source: GAO analysis of data provided by laboratories.



Source: GAO analysis of data provided by laboratories.

SIEMENS

Selection of Evaluation Assurance Level (EAL) for AADS

	Flight safety	Airline business
Threat Level assume sophisticated adversary with moderate resources who is willing to take XXX risk	**T5**: XXX = significant e.g. intl. terrorists	**T4**: XXX = little e.g. organized crime, sophisticated hackers, intl. corporations
Information Value violation of the protection policy would cause YYY damage to the security, safety, financial posture, or infrastructure of the organization	**V5**: YYY= exceptionally grave Risk: loss of lives	**V4**: YYY = serious Risk: airplanes out of service, or damage airline reputation
Evaluation Assurance Level for the given Treat Level and Information Value	**EAL 6**: semiformally verified design and tested	**EAL 4**: methodically designed, tested, and reviewed

Evaluating the whole AADS at EAL 6 would be extremely costly.

Currently available Public Key Infrastructure (PKI) certified only at EAL 4.

Two-level approach: evaluate only LSAP integrity & authenticity at EAL 6.

Conclusion (1) on AADS

- Challenges for AADS development
  - pioneering system design and architecture
  - complex, heterogeneous, distributed system
  - security is critical for both safety and business
- Common Criteria (CC) offer widely accepted, adequate methodology for assessment, at least for small products / systems components
- Systematic approach, in particular formal analysis, enhances
  - understanding of the security issues
  - quality of specifications and documentation
  - confidence (of Boeing, customers, FAA, etc.) in the security solutions

Conclusion (2) on AADS

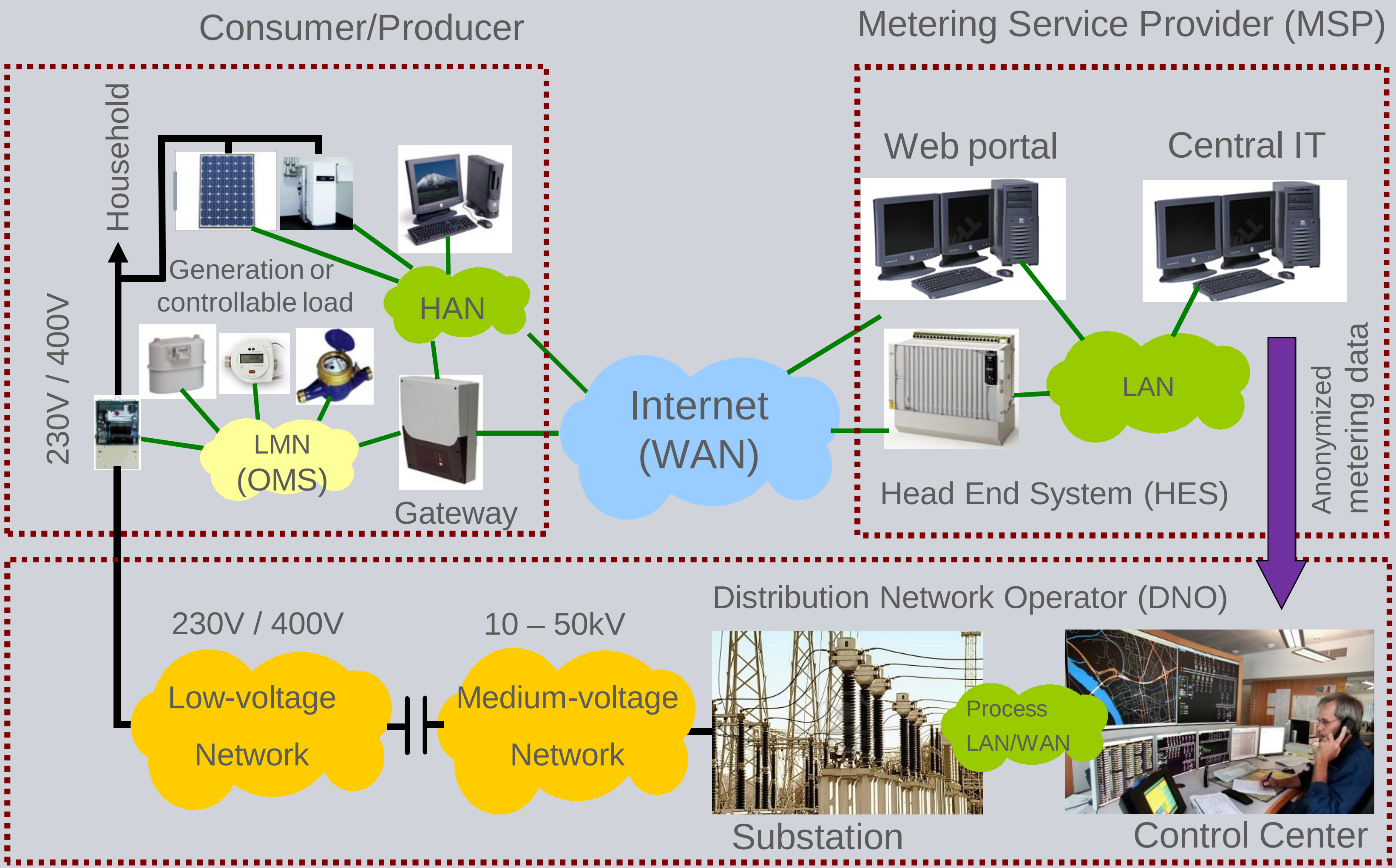
- Experience with AADS evaluation
  - CC offer good guidance for systematic security problem definition:
    threats, assumptions, organizational policies, objectives
  - Shape system architecture to alleviate security evaluation
  - Use formal analysis where cost/benefit ratio is best
  - Problem of compositional security evaluation not solved

- Aspects omitted so far:
  - Key management
    Public Key Infrastructure (PKI) components etc.
  - Configuration management
    with installation instructions and status/completion reports

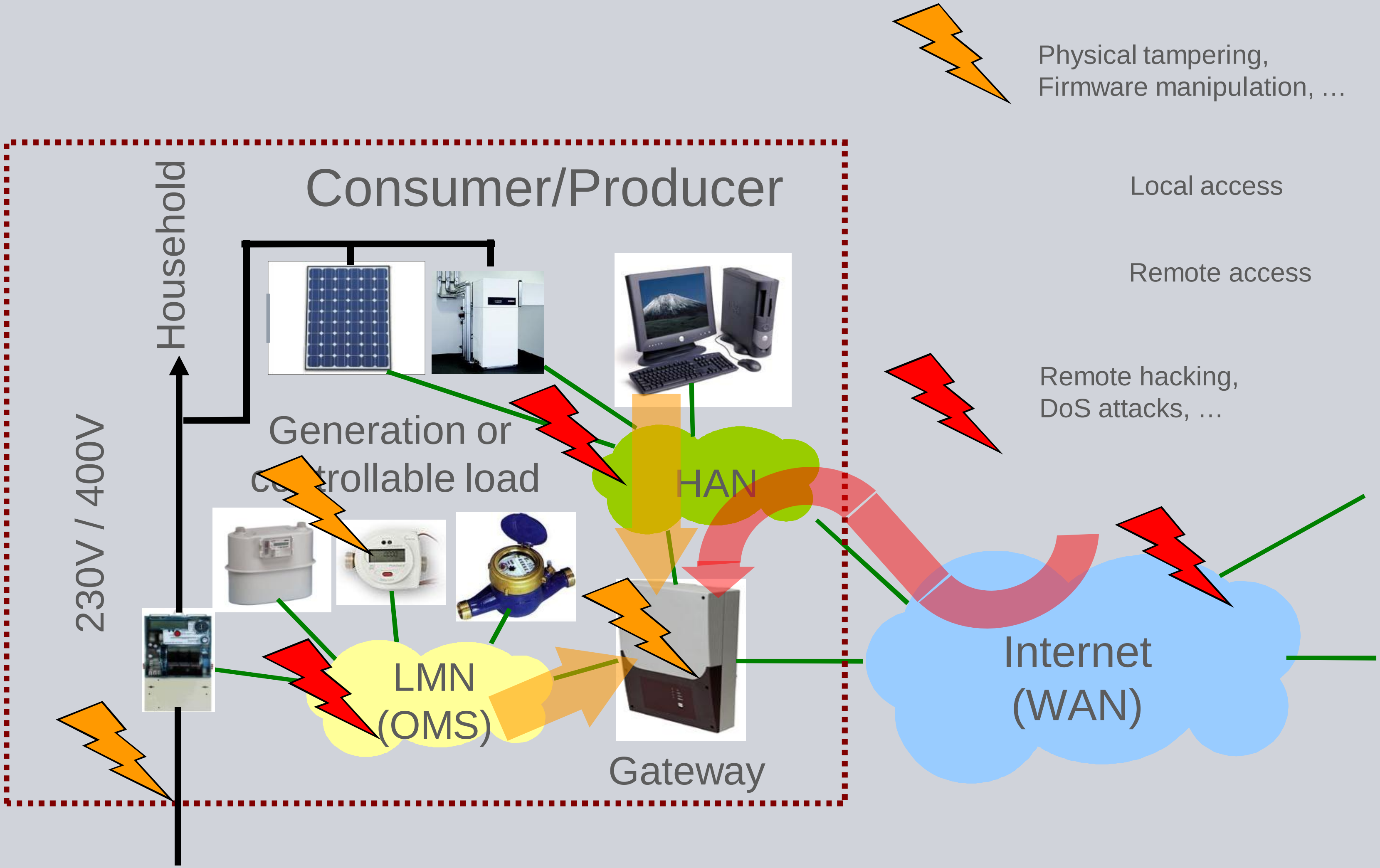
Overview

- IT Security at Siemens Corporate Technology
- Software distribution systems
- Common Criteria certification
- **Smart Metering security requirements**
- Formal security analysis
- Research project AVANTSSAR
- Conclusion on formal security analysis

Context of the Smart Metering Gateway



Local network with Smart Meter Gateway and attack points



History of Germany Smart Metering GW security regulations

- In September 2010, the BMWi (Bundesministerium für Wirtschaft und Technologie) commissioned the BSI (Bundesamt für Sicherheit in der Informationstechnik) to provide a Protection Profile for SM Gateways.
- According to the Common Criteria (CC) approach, the SM Gateway Protection Profile (PP) shall define the minimum security requirements for Smart Metering gateways in an implementation-independent way.
- Since mid-2011, partly to ensure interoperability of Smart Metering devices, several more detailed supplementary guidance documents (TR: Technische Richtlinie) are under development.
- Several commenting rounds with industry have been executed; high amount of feedback has been partly considered in revisions.
- Deadline according to EnWG (§21e.(4) Energiewirtschaftsgesetz) for mandatory use of certified SM gateways was end-2012, but postponed by at least two years due to significant delays in the definition process.

SIEMENS

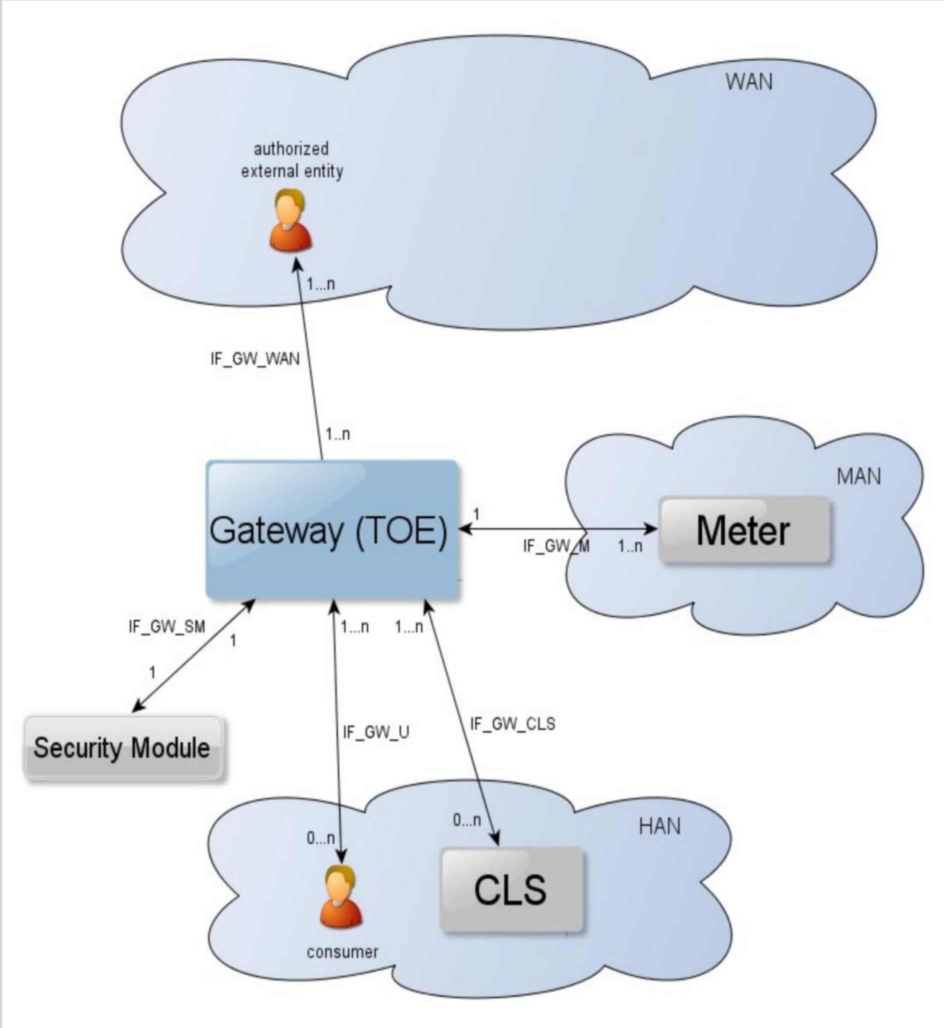
BSI PP for the Gateway of a Smart Metering System: TOE definition (1)

TOE: the local gateway between

Metrological Area Network (MAN)
with meters for commodities

Home Area Network (HAN)
with consumer display and CLS

Wide Area Network (WAN)
with authorized Service Providers



SIEMENS

BSI PP for the Gateway of a Smart Metering System: TOE definition (2)

- The TOE of the SM PP is a gateway serving as the communication unit between devices of private and commercial consumers and *Service Providers* of a commodity industry (i.e., electricity, gas, water).
- *Service Providers*: the Gateway Operator, Meter Operator, Metering Service Provider, Grid Operator, Commodity Supplier and others.
- Typically, the Gateway will be placed in the household or premises of the consumer and enables access to local meters and *Controllable Local Systems (CLS).*
- The gateway collects, processes and stores meter data and is responsible for the secure distribution of this data to external parties.
- It protects all critical information using digital signatures and encryption.
- It also serves as a firewall and should have a fail-safe design.
- It contains a mandatory user interface with access control.

BSI PP for SM GW: Security functional requirements (1)

1. Communication security
   - Transport-level protection on all channels, with mandatory use of TLS v1.1
   - Application-level confidentiality, integrity, and authenticity protection
   - Firewall functionality: GW is connection initiator with optional wake-up mechanism
2. Cryptography support, mandatory use of Hardware Security Module (HSM)
   - Elliptic Curve Cryptography (ECC-256)
   - Advanced Encryption Standard (AES-128)
   - Secure Hash Algorithm (SHA-256)
   - Random number generation (according to BSI AIS 20 / AIS 31)
3. Local key/certificate management with mandatory use of full-blown PKI
   - Generate public/private key pairs and secret keys internally
   - Store private/secret keys confidentially
   - Send public keys in CSR to a sub-CA of the PKI
   - Receive certificates from sub-CA
   - Store certificates in a tamper-proof way
   - Full certificate chain checking including CRLs
   - Update of outdated or compromised key material

BSI PP for SM GW: Security functional requirements (2)

4. Meter data handing
   - Secure time-stamping of meter data
   - Secure logging of application-level events
   - Pseudonymization of personal data to support data protection requirements

5. Device management
   - Tamper protection and detection
   - Secure incident logging
   - Secure GW software update
   - Key management for connected meters and CLS

6. Local user management
   - Authentication of users
   - Access control (for consumers and administrator)

Assurance Requirements

EAL4 (methodically designed, tested and reviewed), augmented by

- *AVA_VAN.5 (Advanced vulnerability analysis; resistance to high attack potential)*
- *ALC_FLR.2 (Life-cycle support; flaw reporting procedures)*

Comments on the BSI's SM GW PP

- Clear security requirements for the gateway
- High assurance level of critical system component
- Strong national standard ensuring interoperability
- Real-time communication support and DoS protection not addressed
- Technical detail: Multiple layers of protection, comprehensive PKI, mandatory use of HW crypto module and point-to-point connections
- Potentially high costs per GW device, installation, and system operation
- Overall system security not addressed

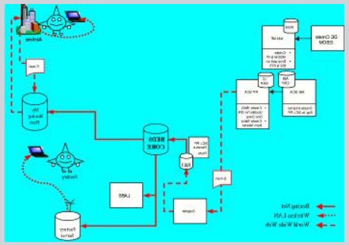
Overview

SIEMENS

- IT Security at Siemens Corporate Technology
- Software distribution systems
- Common Criteria certification
- Smart Metering security requirements
- **Formal security analysis**
- Research project AVANTSSAR
- Conclusion on formal security analysis

Formal Security Analysis: Approach and Benefits

Mission: security analysis with maximal precision
Approach: formal modeling and verification

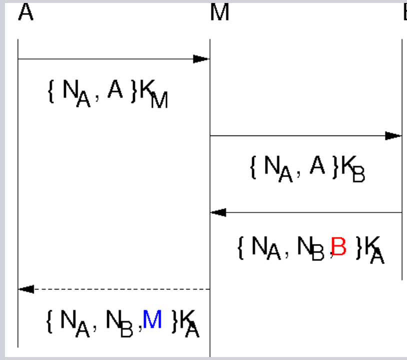


Spec.

Impl.

Abstraction

Interpretation



Improving the quality
of the system specification

Checking for the existence
of security loopholes

AVANTSSAR Specification Language
Model checkers (AVANTSSAR Tool)

Interacting State Machines
Interactive theorem prover (Isabelle)

Tools of the avantssar.eu project

Needham-Schroeder Public Key Protocol

[Needham-Schroeder 1978]
http://en.wikipedia.org/wiki/Needham-Schroeder_protocol

Simplified version without key server, assuming that
A and B already know the public key of their peers:

$$A \rightarrow B: \{Na.A\}_{pk(B)}$$
$$B \rightarrow A: \{Na.Nb\}_{pk(A)}$$
$$A \rightarrow B: \{Nb\}_{pk(B)}$$

Goal: strong mutual authentication

SIEMENS

Example: ASLan++ model NSPK_Cert (1): Alice and Bob

```
specification NSPK_Cert
  …
  entity Alice (Actor, B: agent) {
    symbols
     Na, Nb: message;
    body {
      if(trusted_pk(B)) {
        secret_Na:(Na) := fresh();
        Actor -> B: {Na).Actor}_pk(B);
        B -> Actor: {Alice_freshly_auth_Bob_on_Na:(Na.secret_Nb:(?Nb)}_pk(Actor);
        Actor -> B: {Bob_freshly_auth_Alice_on_Nb:(Nb)}_pk(B); } }
  }
  entity Bob (A, Actor: agent) {
    symbols
      Na, Nb: message;
    body {
      ? -> Actor: {secret_Na:(?Na).?A}_pk(Actor); % Bob learns A here!
      if (trusted_pk(A)) {
        secret_Nb:(Nb) := fresh();
        Actor -> A: {Alice_freshly_auth_Bob_on_Na:(Na).Nb)}_pk(A);
        A -> Actor: {Bob_freshly_auth_Alice_on_Nb:(Nb)}_pk(Actor); } }
  } …
}
```

Example: ASLan++ model NSPK_Cert (2): certificates

```
specification NSPK_Cert channel_model CCM
entity Environment {

  symbols
    trusted_pk(agent): fact;
    trusted_agent(agent): fact;
    root_ca, ca: agent;
    issued(message): fact;

  macros
    A->signed(M)  = {M}_inv(pk(A)).M;
    C->cert(A,PK) = C->signed(C.A.PK); % no validity period etc.

  clauses
    trusted_pk_direct(C):
      trusted_pk(C) :-
      trusted_agent(C);

    trusted_pk_cert_chain(A,B):
      trusted_pk(A) :-
      trusted_pk(B) & issued(B->cert(A,pk(A)));
```


Example: ASLan++ model NSPK_Cert (3): goals and sessions

```
entity Session (A, B: agent) {
  entity Alice (Actor, B: agent) {…}
  entity Bob (A, Actor: agent) {…}
  body {
    issued(ca->cert(A,pk(A)));
    issued(ca->cert(B,pk(B)));
    new Alice(A,B);
    new Bob(B);
  }
  goals
    secret_Na:(_) {A,B};
    secret_Nb:(_) {A,B};
    Alice_freshly_auth_Bob_on_Na:(_) B *->> A;
    Bob_freshly_auth_Alice_on_Nb:(_) A *->> B;
}
body { % need two sessions for Lowe's attack
  trusted_agent(root_ca);
  issued(root_ca->cert(ca,pk(ca))); % root-signed CA certificate
  issued(     ca->cert(i ,pk(i ))); % CA-signed intruder cert
  any A B. Session(A,B) where A!=B;
  any A B. Session(A,B) where A!=B; } }
```

Example: Lowe’s attack on NSPK

[Lowe 1995] Man-in-the-middle attack

```
1.1  A -- {Na.A}pk(i) -> i
2.1                      i(A)  - {Na.A}pk(B) -> B
2.2                      i(A) <- {Na.Nb}pk(A) - B
1.2  A <- {Na.Nb}pk(A) - i
1.3  A -- {Nb}pk(i) ---> i
2.3                      i(A)  - {Nb}pk(B)  --> B
```

In the first session, Alice talks with some party, e.g. Chuck, who in fact is an intruder. This in itself is fine.

In the second session, Bob thinks that he was contacted by Alice but actually talks to the intruder. The intruder can trick Bob because he obtains the nonce Nb via the first session.

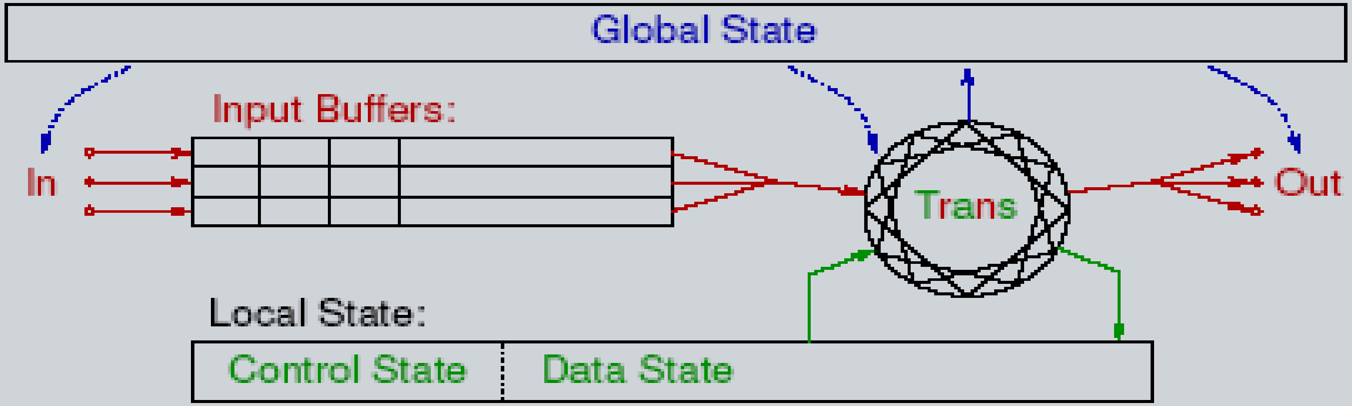
Formal Security Models

SIEMENS

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

Interacting State Machines (ISMs)

Automata with (nondeterministic) state transitions + buffered I/O, simultaneously on multiple connections.

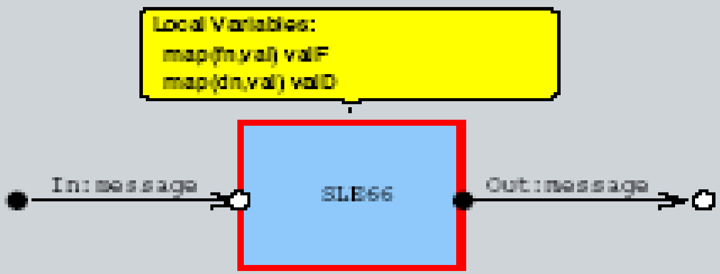


Transitions definable in executable and/or axiomatic style.
An ISM system may have changing global state.
Applicable to a large variety of reactive systems.
By now, not much verification support (theory, tools).

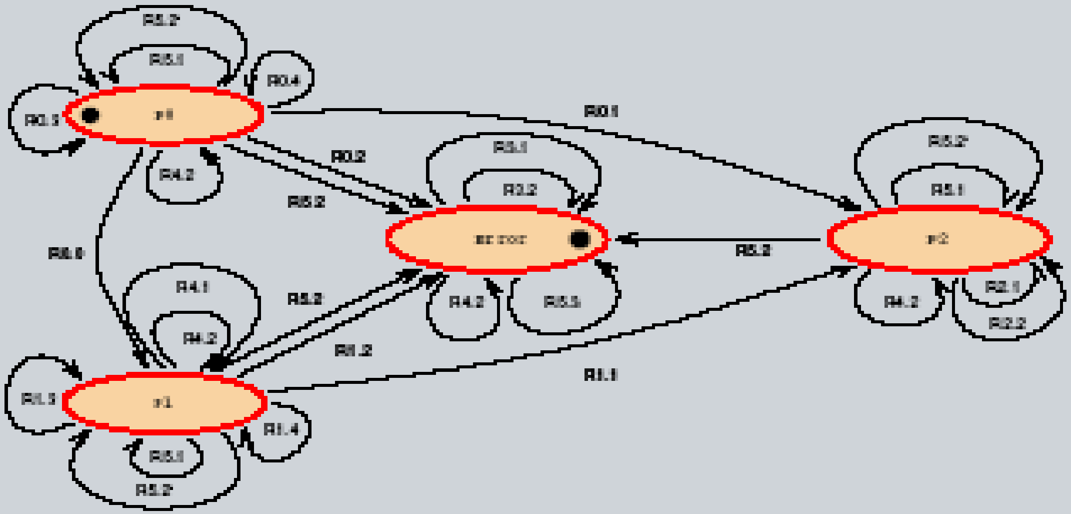
SIEMENS

Formal model of Infineon SLE 66 Smart Card Processor

System Structure Diagram:



State Transition Diagram (abstracted):



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

SIEMENS

Formal RBAC model of Complex Information System

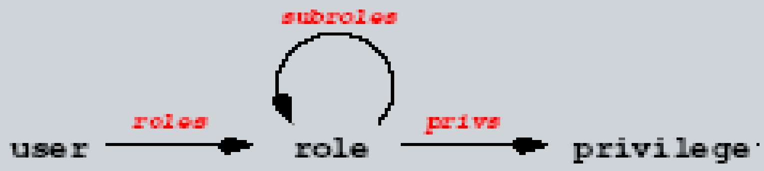
Is the security design (with emergency access etc.) sound?

Privileges:

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

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

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



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

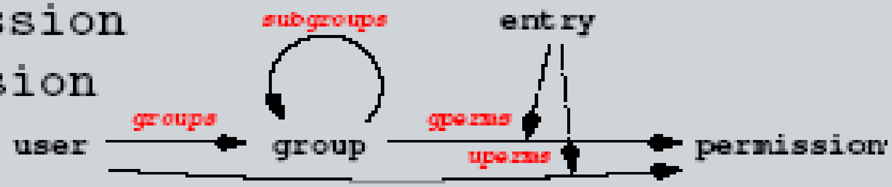
Permissions:

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

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

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

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



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

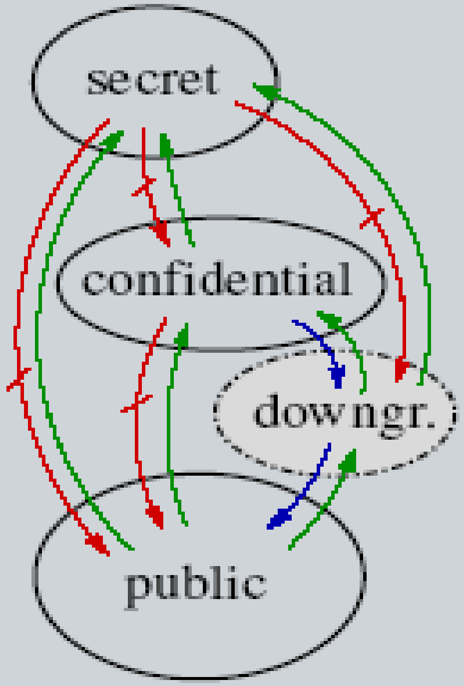
"nagging questions" $\leadsto$ clarifications improving specification quality.

Open issue: relation between model and implementation ($\leadsto$ testing).

SIEMENS

Information Flow Models

- Identify knowledge/information domains
- 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, ...

Very strong, but rarely used in practice

Available: connection with ISMs

Language-based Information Flow Security

Policy: no assignments of high-values
to low-variables, enforced by type system

Semantically: take (x, y) as elements of the state space
with high-level data (on left) and low-level data (on right).

Step function $S(x, y) = (S_H(x, y), S_L(x, y))$
does not leak information from high to low
if $S_L(x_1, y) = S_L(x_2, y)$ (functional independence).

Observational equivalence $(x, y) \overset{L}{\sim} (x', y') \; :\longleftrightarrow \; y = y'$
allows re-formulation:

$$\boxed{s \overset{L}{\sim} t \longrightarrow S(s) \overset{L}{\sim} S(t) \quad (\text{preservation of } \overset{L}{\sim})}$$

Generalization to action sequences α and arbitrary policies $\rightsquigarrow$

SIEMENS

Cryptoprotocol models

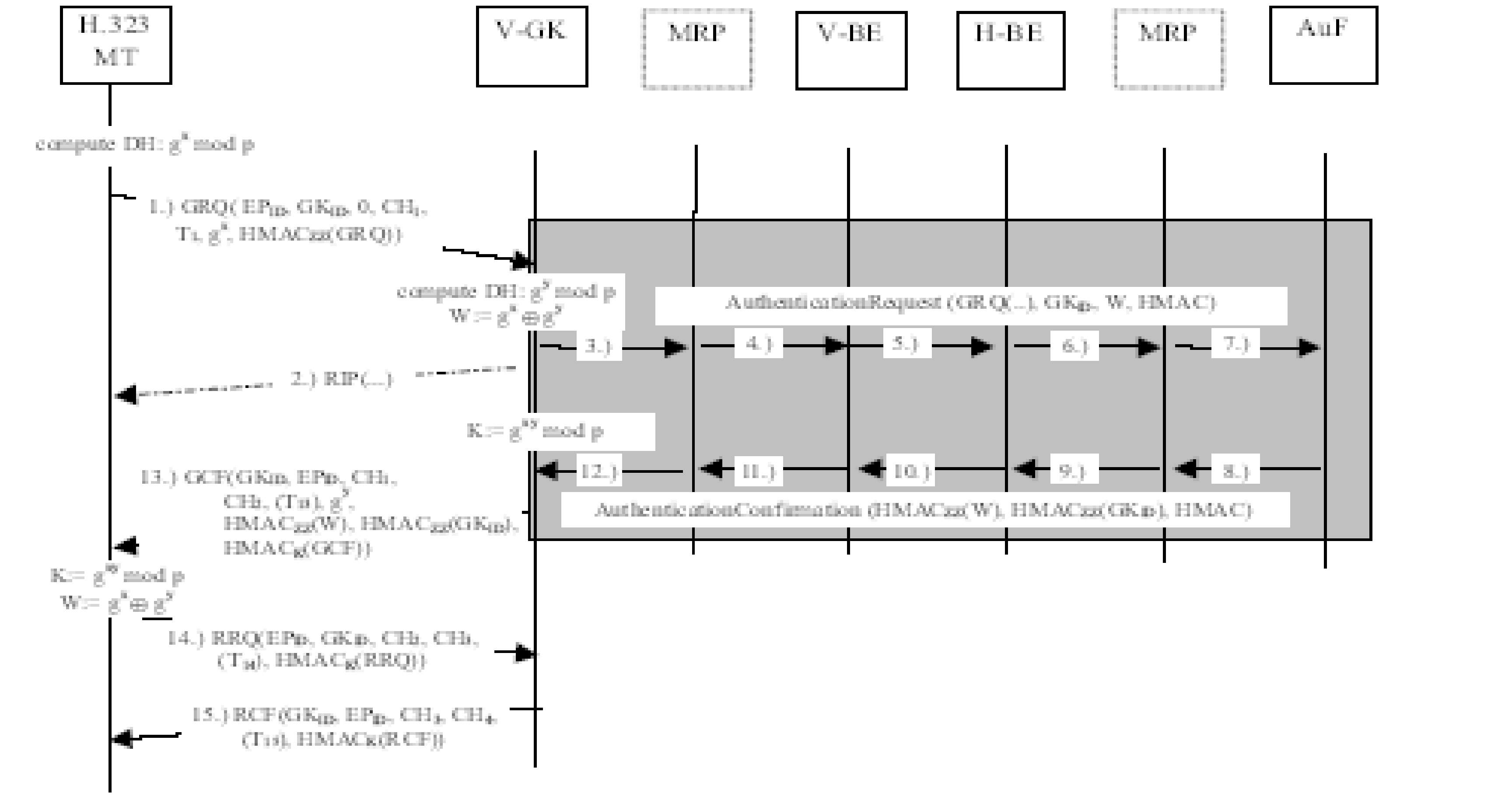
- Describe message exchange between processes or principals

- Take cryptographic operations as perfect primitives
- Describe system with specialized modeling languages
- State secrecy, authentication, . . . goals
- Verify (mostly) automatically using model-checkers

EU project AVISPA , ...

![SIEMENS]

Example: H.530 Mobile Roaming Authentication



Two vulnerabilities found and corrected. Solution standardized.

Overview

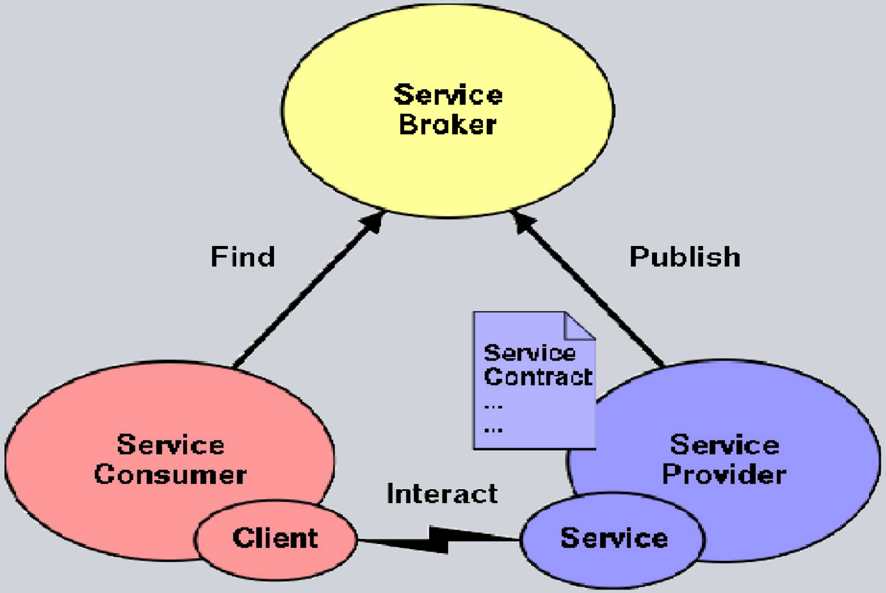
- IT Security at Siemens Corporate Technology
- Software distribution systems
- Common Criteria certification
- Smart Metering security requirements
- Formal security analysis
- **Research project AVANTSSAR**
- Conclusion on formal security analysis

AVANTSSAR

SIEMENS

avantssar.eu

Model-checking SOA security — research project AVANTSSAR[1]



[1] **A**utomated **Va**lidatio**N** of **T**rust and **S**ecurity of **S**ervice-oriented **Ar**chitectures

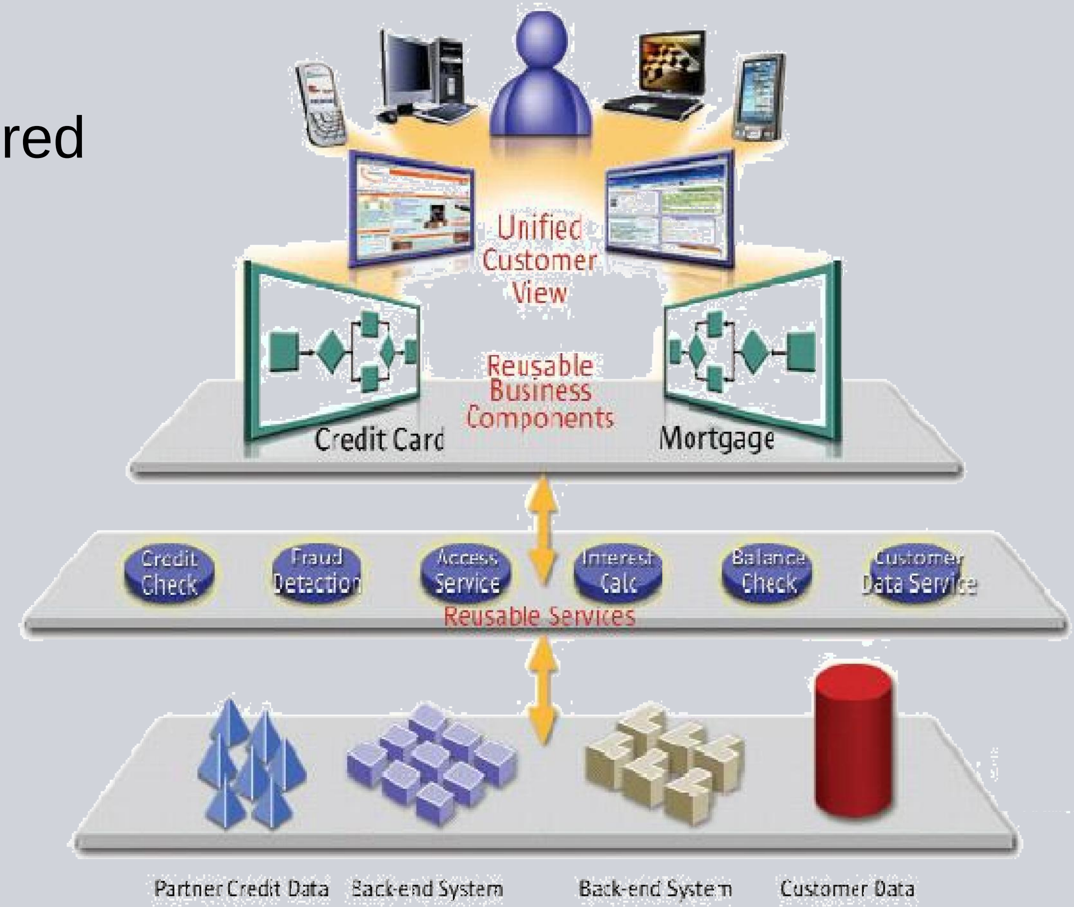
FP7-2007-ICT-1, ICT-1.1.4, STREP project no. 216471
Jan 2008 - Dec 2010, 590 PMs, 6M€ budget, 3.8M€ EC contribution

AVANTSSAR project motivation

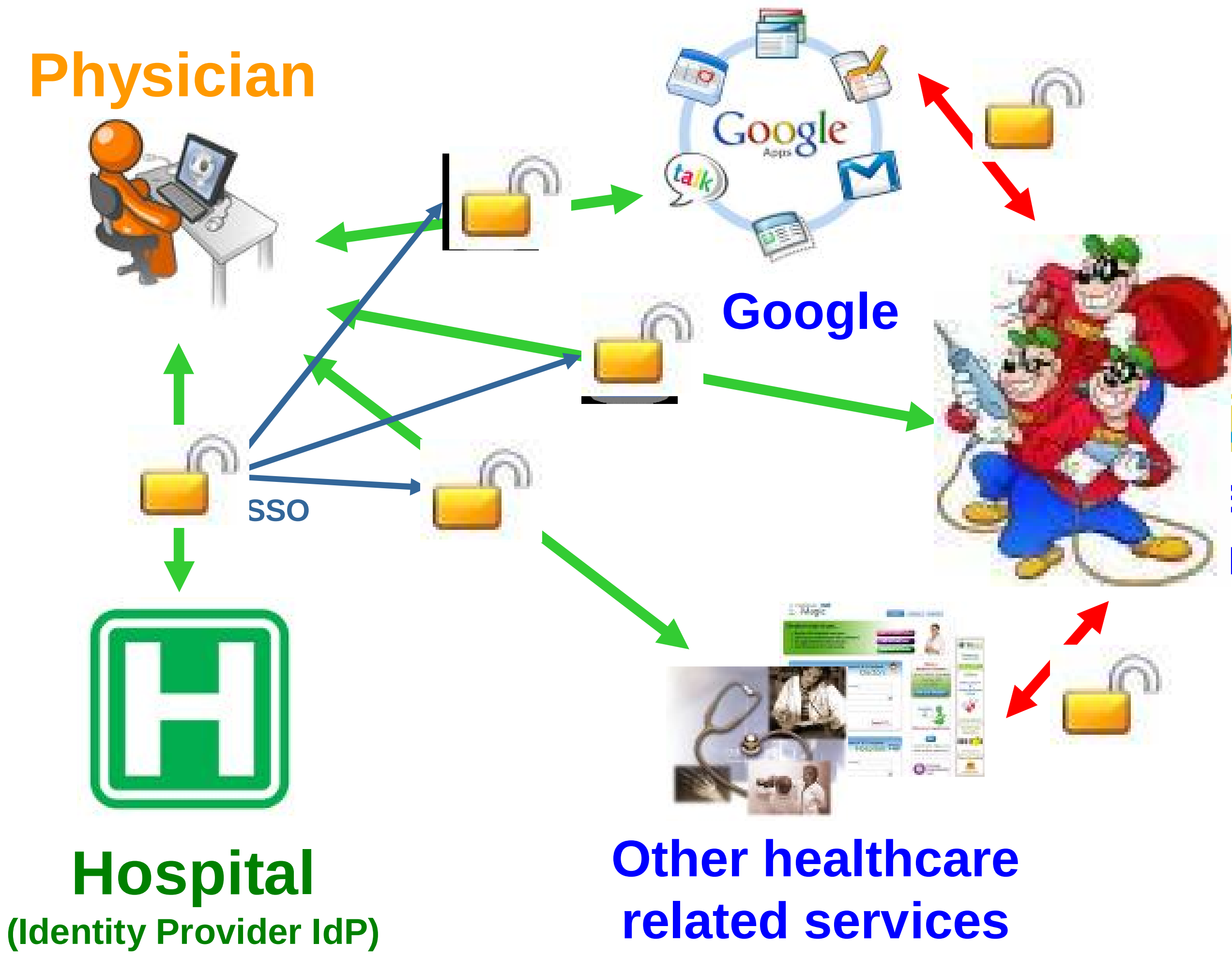
ICT paradigm shift: from components to services, composed and reconfigured dynamically in a demand-driven way.

Trustworthy services may interact with others causing novel trust and security problems.

For the composition of individual services into service-oriented architectures, validation is dramatically needed.



Example 1: Google SAML-based Single Sign-On (SSO)



A malicious service provider can access the data of the physician located at all other services connected via Google SSO

SIEMENS

Example 1: Google SAML SSO protocol flaw

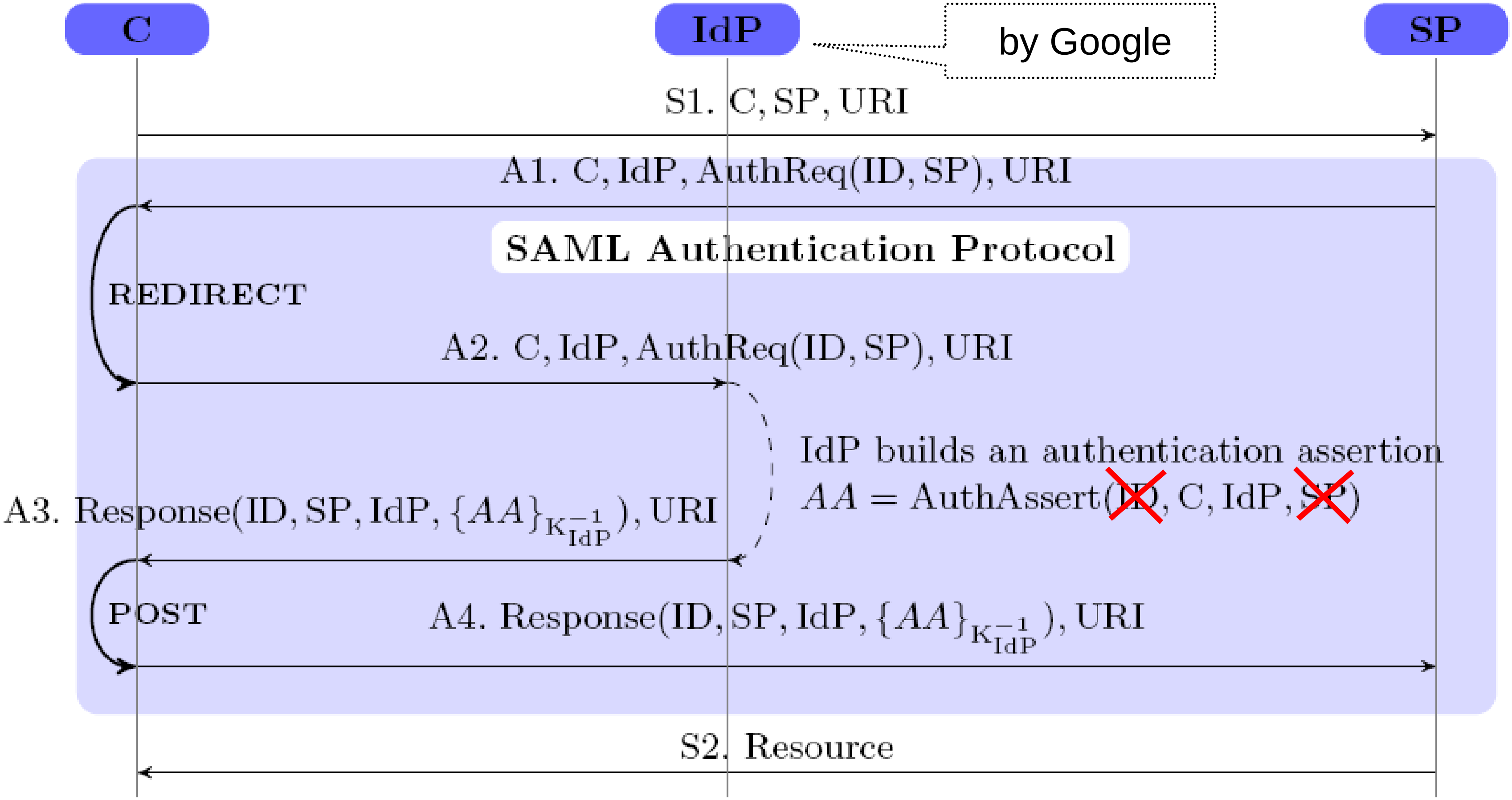


Fig. 1. SP-Initiated SSO with Redirect/POST Bindings

AVANTSSAR consortium

SIEMENS

Industry

SAP Research France, Sophia Antipolis

Siemens Corporate Technology, München

IBM Zürich Research Labs (initially)

OpenTrust, Paris

Academia

Università di Verona

Università di Genova

ETH Zürich

INRIA Lorraine

UPS-IRIT Toulouse

IEAT Timişoara

Expertise

Service-oriented enterprise architectures

Security solutions

Standardization and industry migration

Security engineering

Formal methods

Automated security validation

AVANTSSAR main objectives and principles

AVANTSSAR product: Platform for formal specification and automated validation of trust and security of SOAs

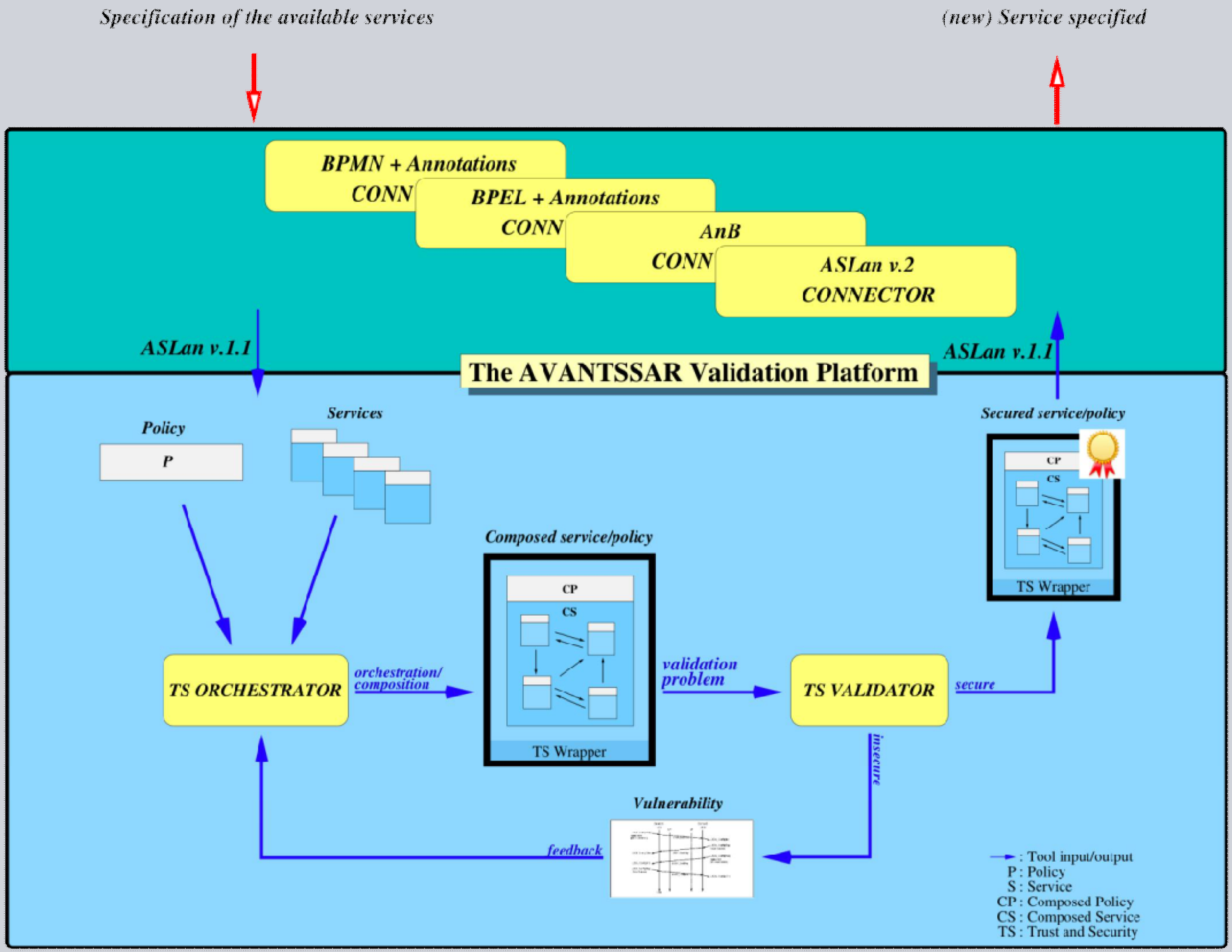
- Formal language for specifying trust and security properties of services, their policies, and their composition into service-oriented architectures
- Automated toolset supporting the above
- Library of validated industry-relevant case studies

Migration of platform to industry and standardization organizations

- Speed up development of new service infrastructures
- Enhance their security and robustness
- Increase public acceptance of Web services and SOA systems

AVANTSSAR project results and innovation

SIEMENS

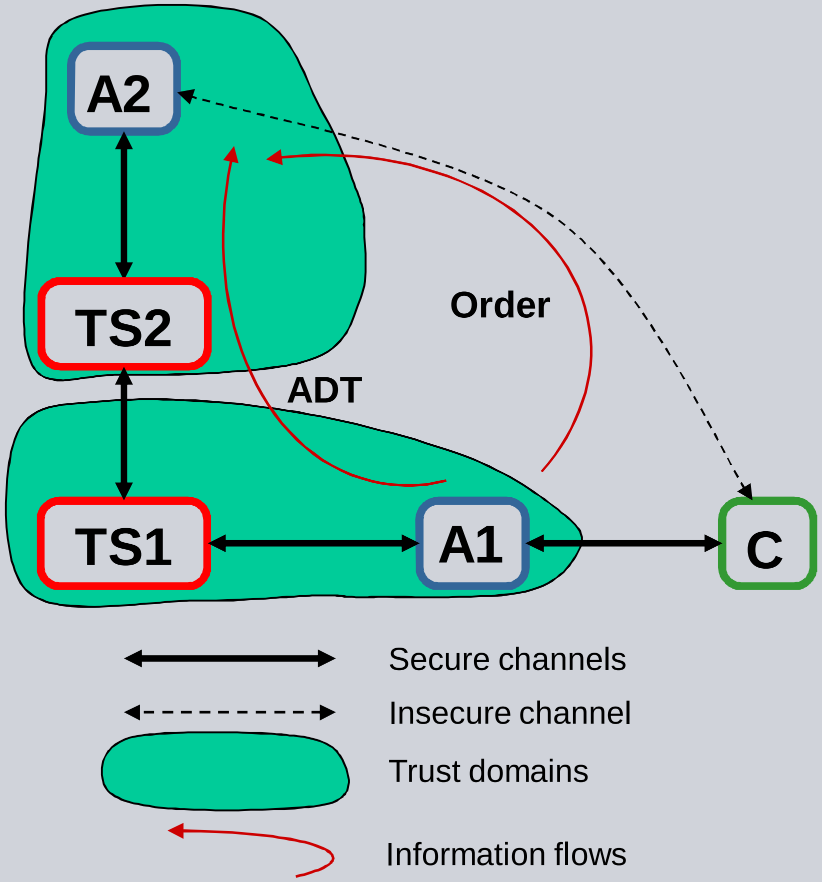


Example 2: Process Task Delegation (PTD)

SIEMENS

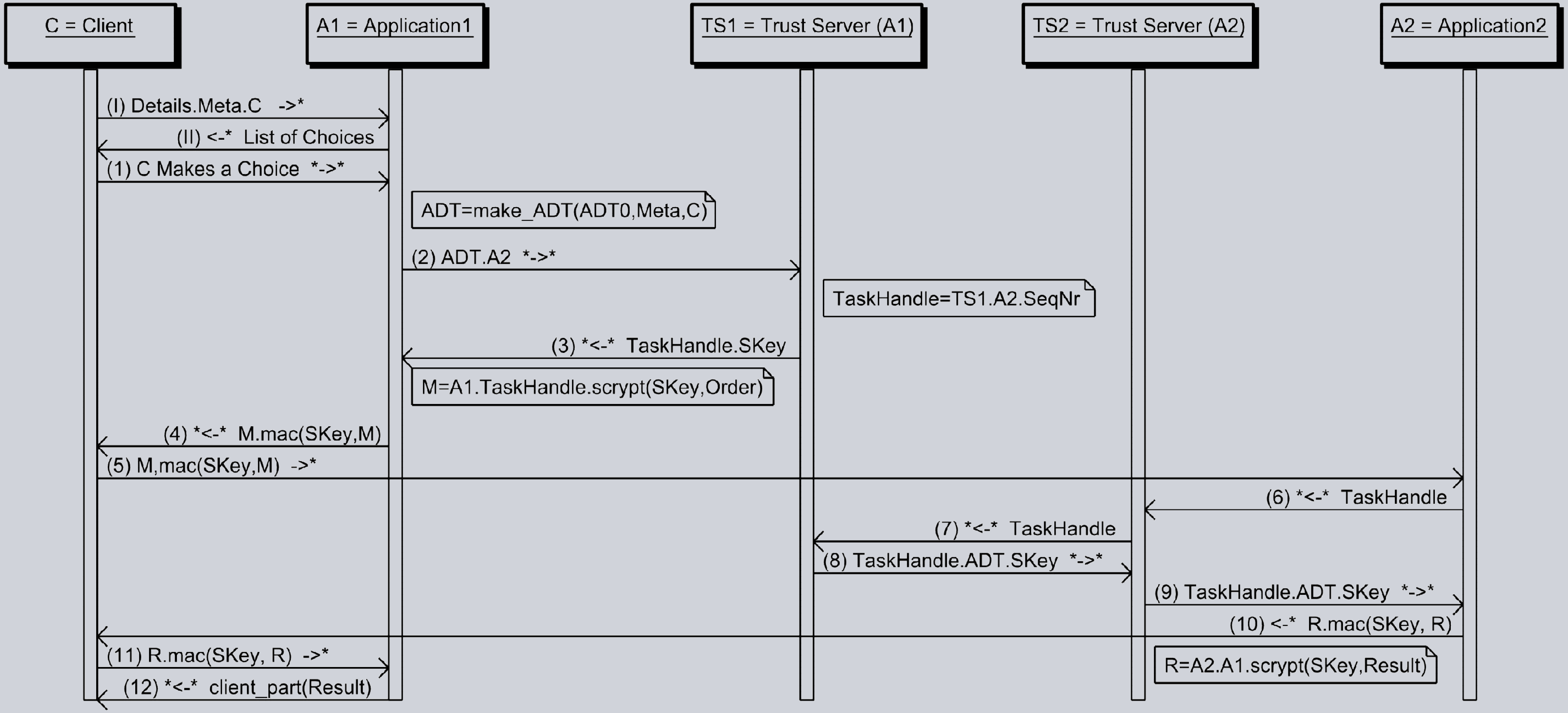
- **Authorization and trust management via token passing**
- There are three roles in the protocol (**C, A, TS)** and potentially several instances for each role
- The *client* **C** (or *user*) uses the system for SSO, authorization and trust management
- Each *application* **A** is in one domain, each domain has exactly one active *token server* **TS**
- **A1** uses the system to pass to **A2** some **Order** and an **ADT (Authorization Decision Token)**
  - **Order** contains:
    - workflow task information
    - application data
    - information about the client **C** and his current activity

    to be delivered securely (integrity and confidentiality)
  - **ADT** is mainly authorization *attributes* and *decisions*
    - sent via **TS1** and **TS2**, <u>who may weaken it</u>
    - must remain unaltered, apart from weakening by **TS**
    - must remain confidential among intended parties
- **C**, **A1**, and **A2** must be authenticated among each other



- **Security prerequisites**:
- PKI is used for **A** and **TS**, username & pwd for **C**
- **TS** enforces a strict time-out

Example 2: Message Sequence Chart of PTD

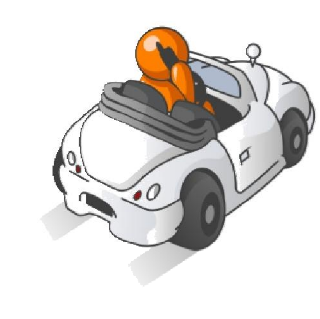


Example 2: ASLan++ model of A2

```
entity A2 (Actor: agent, TS2: agent) {   % Applicaton2, connected with TokenServer2
  symbols
    C0,C,A1: agent;
    CryptedOrder, Order, Order0, Details, Results, TaskHandle, ADT, HMAC: message;
    SKey: symmetric_key;
  body { while (true) {
    select {
      % A2 receives (via some C0) a package from some A1. This package includes encrypted and
      % hashed information. A2 needs the corresponding key and the Authorization Decision Token.
      on (?C0 -> Actor: (?A1.Actor.?TaskHandle.?CryptedOrder).?HMAC): {
        % A2 contacts its own ticket server (TS2) and requests the secret key SKey and the ADT.
        Actor *->* TS2: TaskHandle;
      }
        % A2 receives from A1 the SKey and checks if the decrypted data corresponds to the hashed data
      on (TS2 *->* Actor: (?ADT.?SKey).TaskHandle  & CryptedOrder = scrypt(SKey,?Order0,?Details.?C)
           & HMAC = hmac(SKey, A1.Actor.TaskHandle.CryptedOrder)): {
        % A2 does the task requested by A1, then sends to A1 via C the results encrypted with the secret key.
        Results := fresh(); % in general, the result depends on Details etc.
        Actor -> C: Actor.C.A1. scrypt(SKey,Results);
   } } }
  goals
    authentic_C_A2_Details: C  *-> Actor: Details;
    secret_Order: secret (Order0,Details.C, {Actor, A1});
}
```

SIEMENS

Example 3: Electronic Car Registration policies



local policy

RegOffCA can say
who is RegOffHead
who is RegOffEmpl

certificate

Peter is RegOffEmpl
of CarRegOffice
(signed by RegOffCA)

ACL

anybody,
get empty forms
RegOffHead, write
RegOffEmpl, read
RegOffEmpl, write,
if *his* RegOffHead
says so

CentrRep

write(..)

Peter

Melinda

RegOffCA

certificate

Melinda is RegOffHead
of CarRegOffice
(signed by RegOffCA)

certificate

Peter can write
CentrRep
(signed by Melinda)

Question:

May Peter write to CentrRep?

Example 3: On-the-fly inferences via Horn clauses

DKAL-style trust inference, e.g. trust application:

```
trustapp(P,Q,AnyThing):
  P->knows(AnyThing) :-
    P->trusts(Q,AnyThing) &
    P->knows(Q->said(AnyThing));
```

Basic facts, e.g. the central repository fully trusts the CA

```
centrRepTrustCA(AnyThing):
  centrRep->trusts(theCA,AnyThing);
```

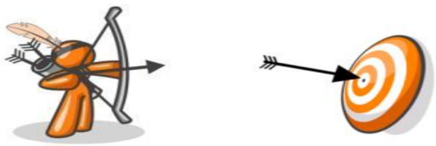
State-dependent (evolving) facts, e.g. department head manages a set of trusted employees:

```
trustedEmplsCanStoreDoc(Head): forall Empl.
  Head->knows(Empl->canStoreDoc) :-
    contains(TrustedEmpls, Empl);
```

Use of certificates, e.g. the central repository trusts the department head on employee's rights:

```
centrRepTrustHead(Head,Empl):
  centrRep->trusts(Head,Empl->canStoreDoc) :-
    centrRep->knows(theCA->said(Head->hasRole(head))) &
    centrRep->knows(theCA->said(Empl->hasRole(employee)));
```

AVANTSSAR final status



SIEMENS

WP2: ASLan++ supports the formal specification of trust and security related aspects of SOAs, and of static service and policy composition

WP3: Techniques for: satisfiability check of policies, model checking of SOAs w.r.t. policies, different attacker models, compositional reasoning, abstraction

WP4: Deploy first prototype of **AVANTSSAR Platform**

WP5: Formalization of **industry-relevant problem cases** as ASLan++ specifications and their validation

WP6: **Ongoing dissemination and migration** into scientific community and industry

AVANTSSAR Tool pre-release

If interested, try the AVANTSSAR platform pre-release at ddvo.net/AVANTSSAR

Overview

- IT Security at Siemens Corporate Technology
- Software distribution systems
- Common Criteria certification
- Smart Metering security requirements
- Formal security analysis
- Research project AVANTSSAR
- **Conclusion on formal security analysis**

Formal Security Analysis: Information Required

- Overview: system architecture (components and interfaces),
  e.g. databases, authentication services, connections,…
- Security-related concepts: actors, assets, states, messages, …
- Threats: which attacks have to be expected.
- Assumptions: what does the environment fulfill.
- Security objectives: what the system should achieve.
  Described in detail such that concrete verification goals can be set up
  e.g. integrity: which contents shall be modifiable by whom, at which times,
  by which operations (and no changes otherwise!)
- Security mechanisms: relation to objectives and how they are achieved.
  e.g. who signs where which contents, and where is the signature checked
  Described precisely but at high level (no implementation details required),
  e.g. abstract message contents/format but not concrete syntax

Shaping a Formal Model

SIEMENS

Formality Level: should be adequate:

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

Choice of Formalism: dependent on ...

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

Abstraction Level: should be ...

- high enough to achieve clarity and limit the effort
- low enough not to loose important detail

refinement allows for both high-level and detailed description

SIEMENS

Development Phases and the Benefits of Formal Analysis

Requirements analysis:

understanding the security issues

- abstraction: keep overview by concentrating on the essentials
- genericity: simplify the analysis by using standardized patterns

Design, documentation:

quality of specifications

- formal modeling enforces preciseness and completeness

Implementation:

effectiveness of security functionality

- formal model as precise reference for testing and verification