Critical Systems Development with UML and Model-based Testing

Jan Jürjens
(contrib. UMLsec group@TUM, S. Houmb)
Software & Systems Engineering
TU Munich, Germany

juerjens@in.tum.de
http://www.jurjens.de/jan

Critical Systems Development

High quality development of critical systems (dependable, security-critical, real-time,...) is difficult.

Many systems developed, fielded, used that do not satisfy their criticality requirements, sometimes with spectacular failures.

Quality vs. cost

Systems on which human life and commercial assets depend need careful development.

Systems operating under possible system failure or attack need to be free from weaknesses.

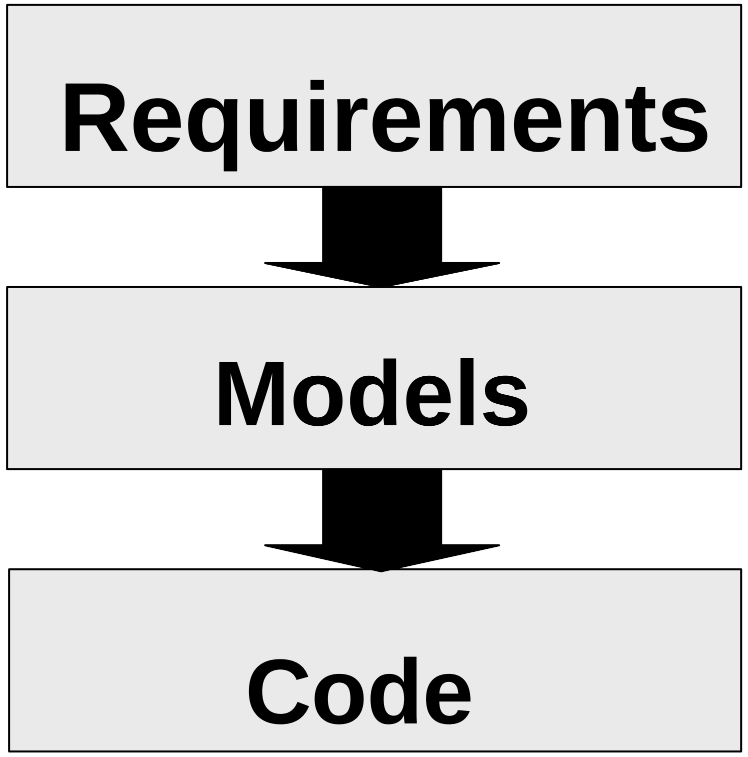
Correctness in conflict with cost.

Thorough methods of system design not used if too expensive.

Model-based Development

Goal: easen transition from human ideas to executed systems.

Increase quality with bounded time-to-market and cost.



Goal: Critical properties by design

Consider critical properties

- from early on
- within development context
- taking an expansive view
- in a seamless way.

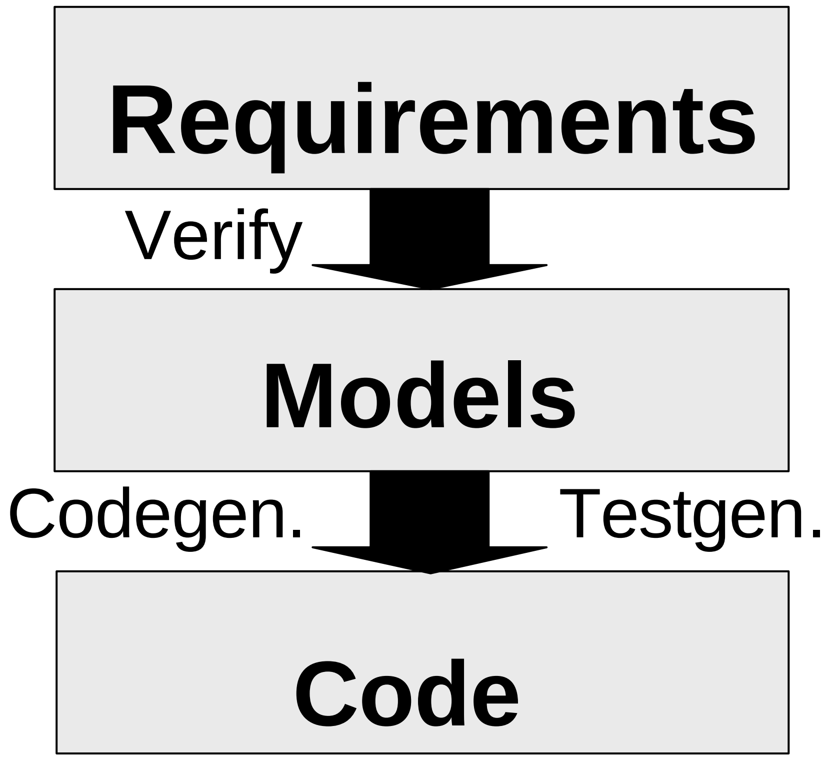
Critical design by model analysis.

Critical implementation by test generation.

Model-based Development

Combined strategy:

- Verify models against requirements
- Generate code from models where reasonable
- Write code and generate test-sequences otherwise.



Using UML

UML: unprecedented opportunity for high-quality critical systems development feasible in industrial context:

- De-facto standard in industrial modeling: large number of developers trained in UML.
- Relatively precisely defined (given the user community).
- Many tools in development (also for analysis, testing, simulation, transformation).

Challenges

- Adapt UML to critical system application domains.
- Correct use of UML in the application domains.
- Conflict between flexibility and unambiguity in the meaning of a notation.
- Improving tool-support for critical systems development with UML.

This tutorial

Background knowledge on using UML for critical systems development.

- UML basics, including extension mechanisms.
- Extensions of UML (UMLsec, UML-RT, ...)
- UML as a formal design technique.
- Model-based testing.
- Tools.
- Case studies.

Concentrate on safety-critical systems.

Generalize to other application domains.

Roadmap

Prologue

UML

UMLsafe

Security-critical systems

UMLsec: The profile

Security analysis

Security patterns

UMLsec case studies

Java security, CORBAsec

Tools

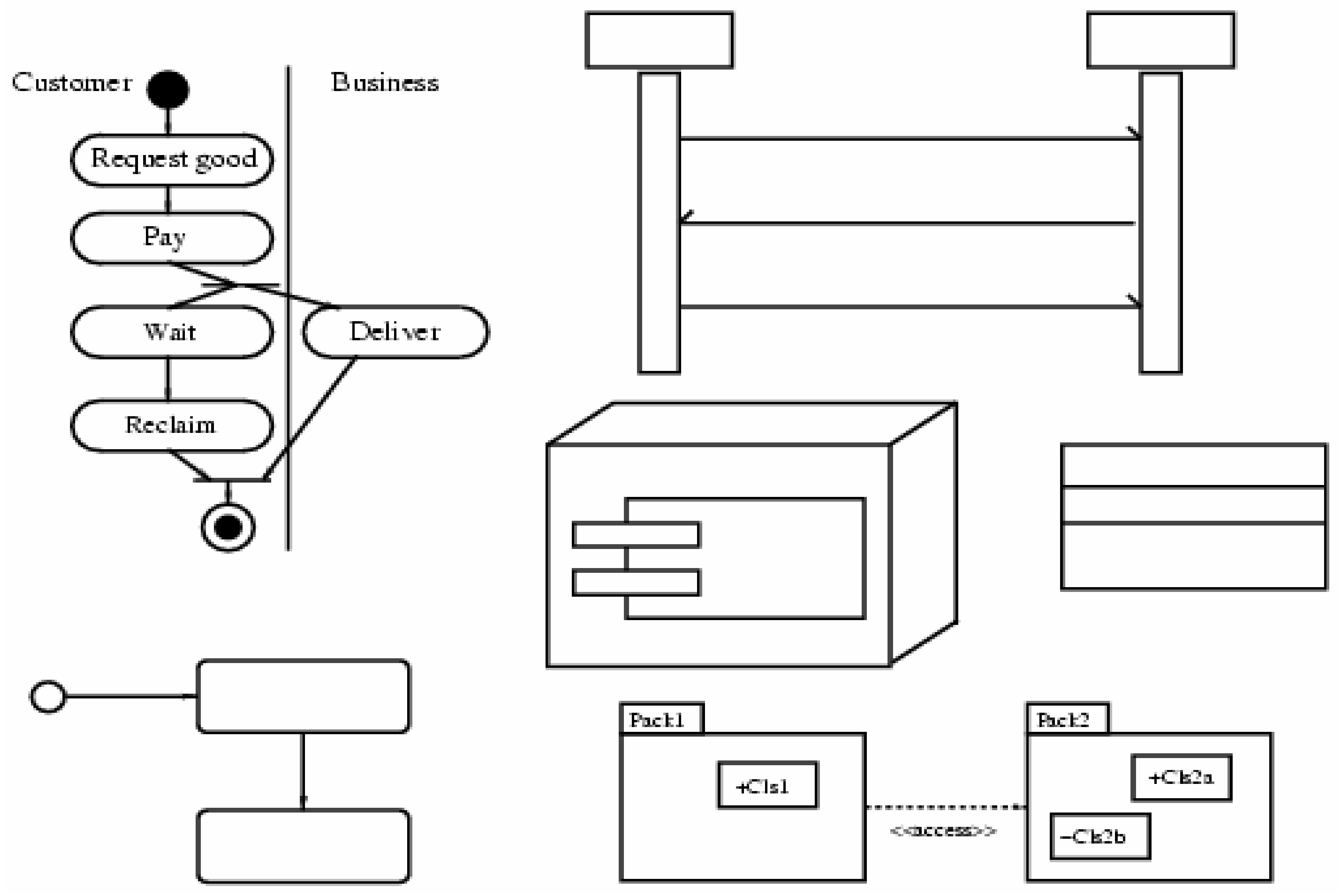
Model-based Testing

Using UML

Unified Modeling Language (UML):

- visual modelling for OO systems
- different views on a system
- high degree of abstraction possible
- de-facto industry standard (OMG)
- standard extension mechanisms

A glimpse at UML



Used fragment of UML

Activity diagram: flow of control between system components

Class diagram: data structure of the system

Sequence diagram: interaction between components by message exchange

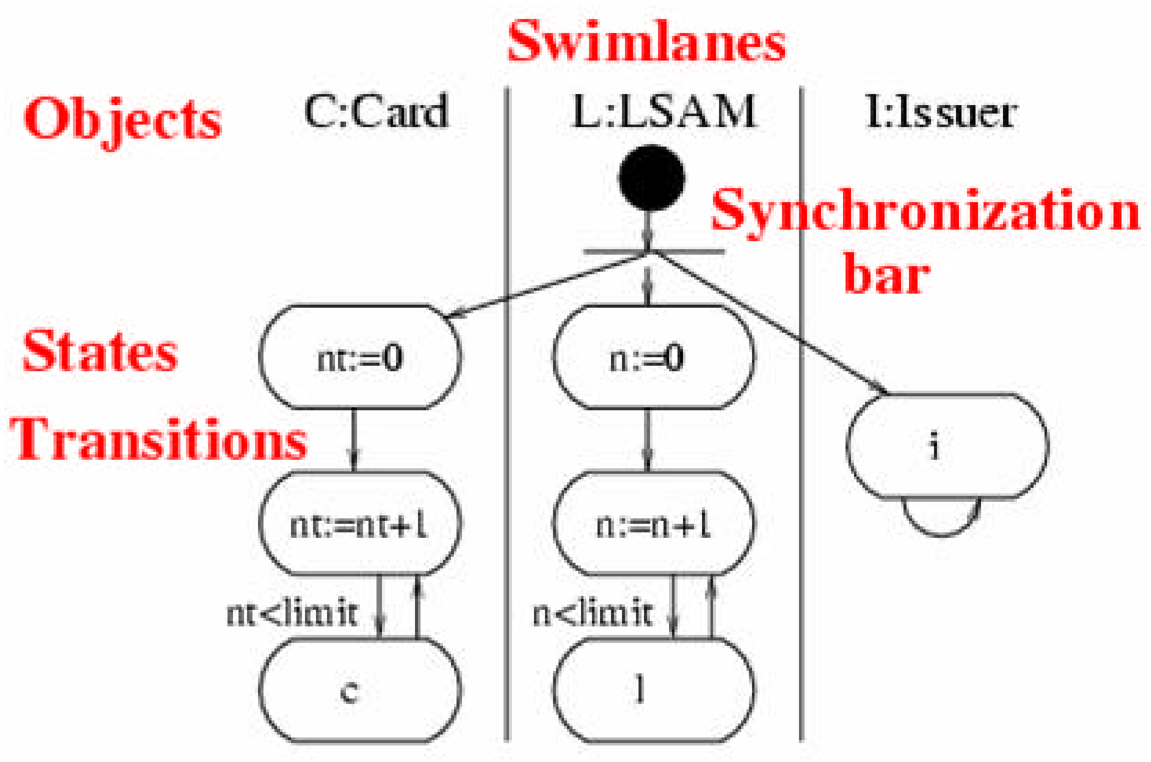
Statechart diagram: dynamic component behaviour

Deployment diagram: Components in physical environment

Package: collect system parts into groups

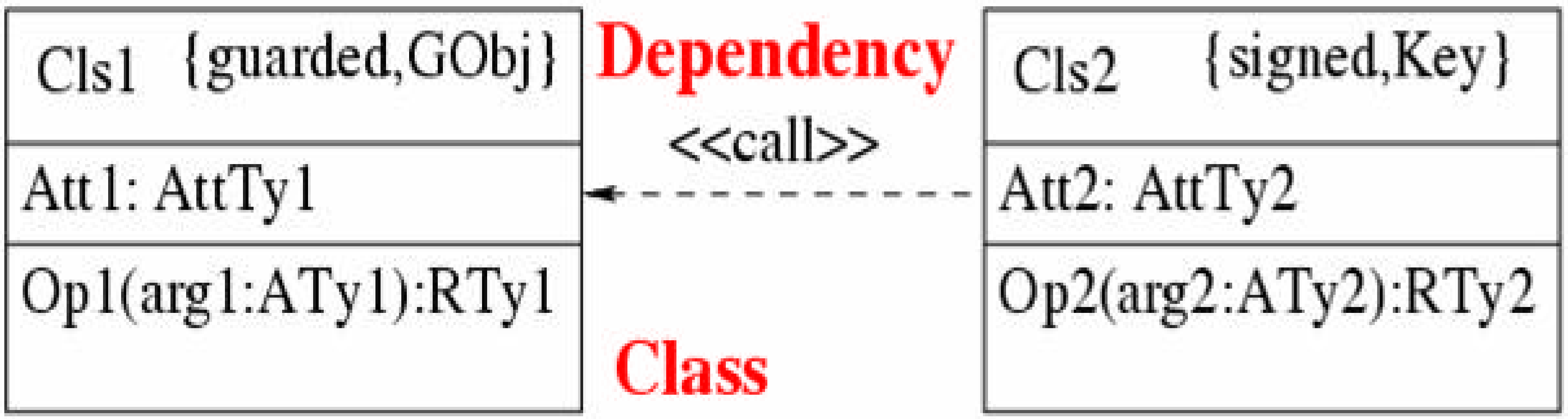
Current: UML 1.5 (released Mar 2003)

UML run–through: Activity diagrams



Specify the control flow between components within the system, at higher degree of abstraction than statecharts and sequence diagrams.

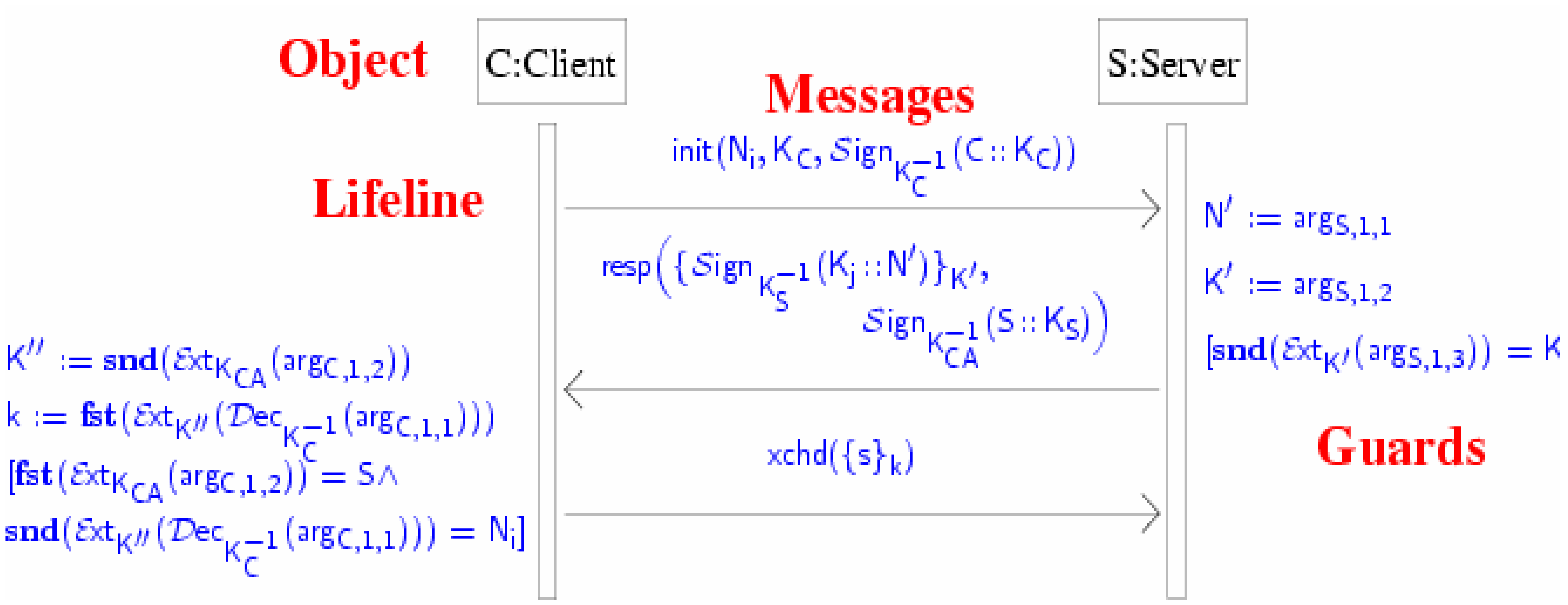
UML run-through: Class diagrams



Class structure of system.

Classes with attributes and operations/signals; relationships between classes.

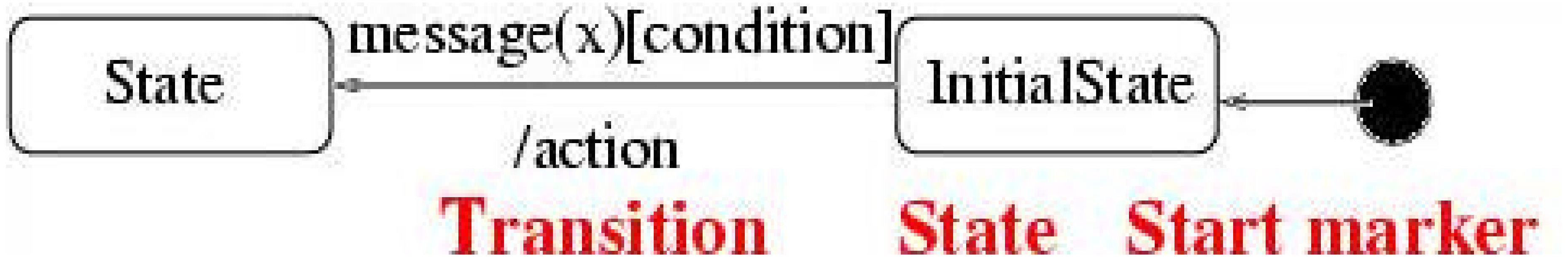
UML run-through: Sequence Diagrams



Object
C:Client
S:Server
Messages
Lifeline
Guards
$\mathrm{init}(N_i, K_C, \mathcal{S}ign_{K_C^{-1}}(C :: K_C))$
$N' := \mathrm{args}_{S,1,1}$
$K' := \mathrm{args}_{S,1,2}$
$[\mathbf{snd}(\mathcal{E}xt_{K'}(\mathrm{args}_{S,1,3})) = K$
$\mathrm{resp}\left(\{\mathcal{S}ign_{K_S^{-1}}(K_j :: N')\}_{K'}, \mathcal{S}ign_{K_{CA}^{-1}}(S :: K_S)\right)$
$K'' := \mathbf{snd}(\mathcal{E}xt_{K_{CA}}(\mathrm{arg}_{C,1,2}))$
$k := \mathbf{fst}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\mathrm{arg}_{C,1,1})))$
$[\mathbf{fst}(\mathcal{E}xt_{K_{CA}}(\mathrm{arg}_{C,1,2})) = S \wedge$
$\mathbf{snd}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\mathrm{arg}_{C,1,1}))) = N_i]$
$\mathrm{xchd}(\{s\}_k)$

Describe interaction between objects or components via message exchange.

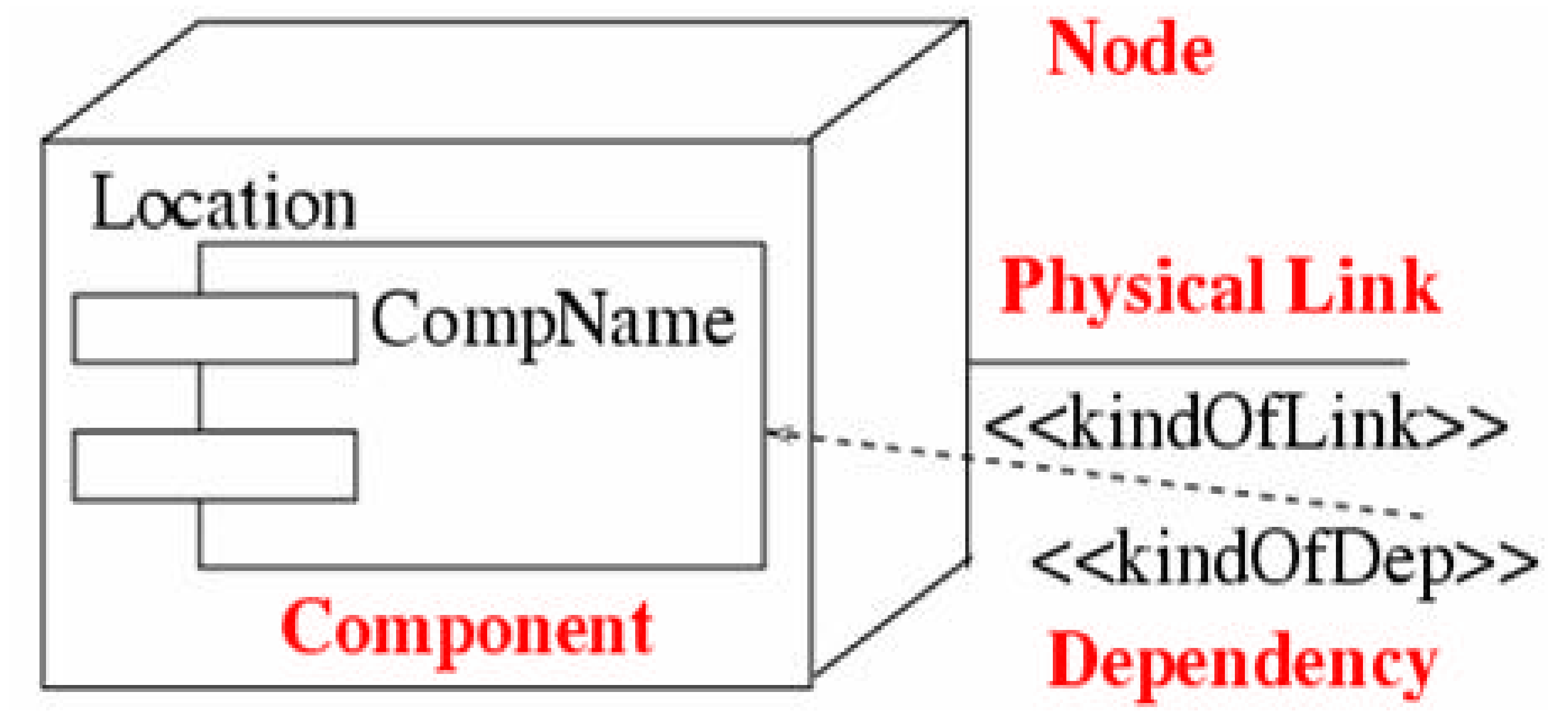
UML run-through: Statecharts



Dynamic behaviour of individual component.

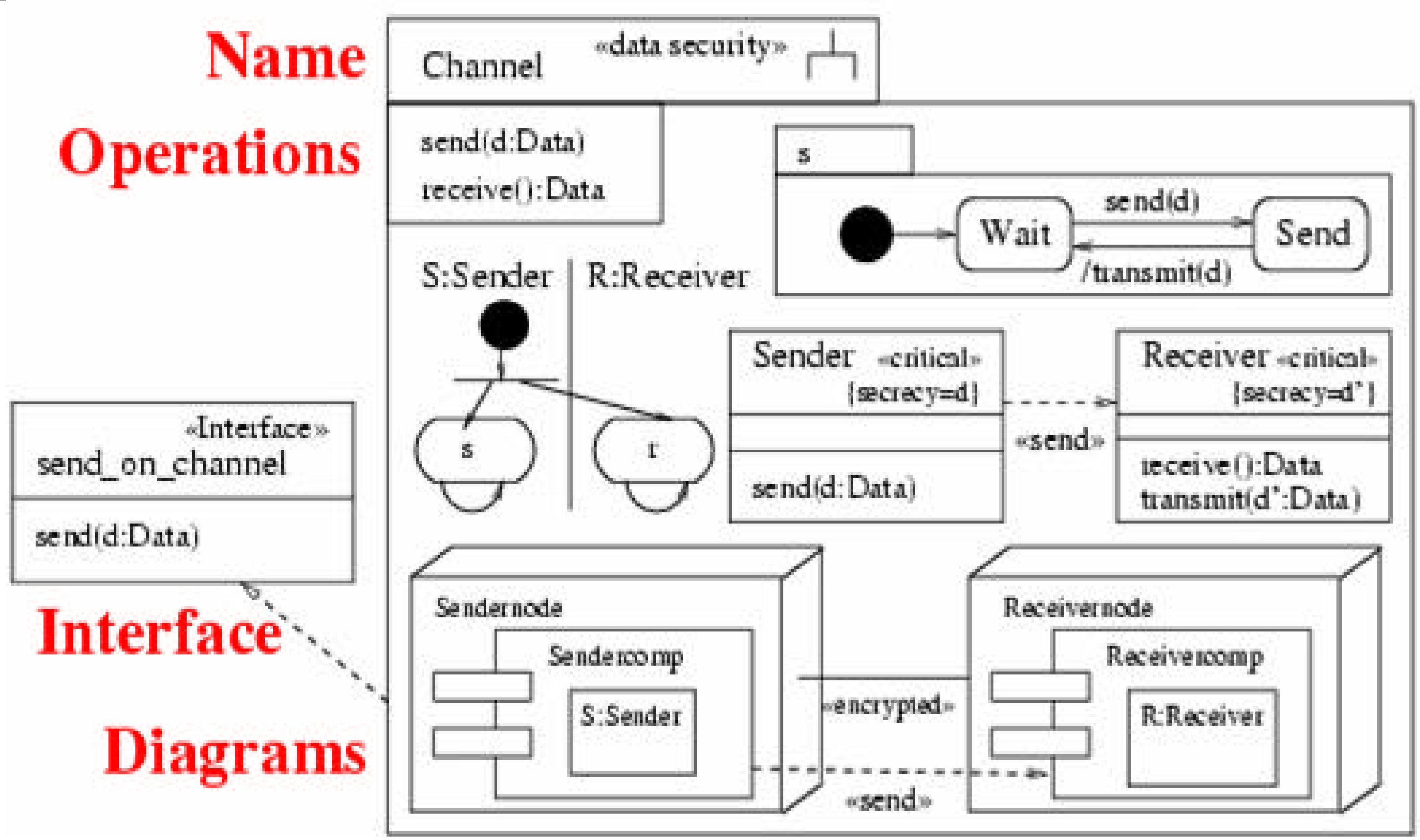
Input events cause state change and output actions.

UML run-through: Deployment diagrams



Describe the physical layer on which the system is to be implemented.

UML run-through: Package



May be used to organize model elements into groups.

UML Extension mechanisms

Stereotype: specialize model element using ¿labelÀ.

Tagged value: attach {tag=value} pair to stereotyped element.

Constraint: refine semantics of stereotyped element.

Profile: gather above information.

Roadmap

Safety

Safety-critical systems: five failure condition categories: catastrophic, hazardous, major, minor, no effect.

Corresponding safety levels A - E (DO-178B standards in avionics).

Safety goals: via the maximum allowed failure rate. For high degree of safety, testing not sufficient (1 failure per 100,000 years).

Failures

Exchanged data may be

- delayed (and possibly reordered)
- lost
- corrupted.

Often, failures occur randomly (e.g. hardware).

Failure semantics examples:

- crash/performance: component may crash or exceed time limit, but partially correct.
- value: component may deliver incorrect values.

Fault-tolerance

Redundancy model determines which level of redundancy provided.

Goal: no hazards in presence of single-point failures.

Embedded Systems

In particular, embedded software increasingly used in safety-critical systems (flexibility):

- Automotive
- Avionics
- Aeronautics
- Robotics, Telemedicine
- …

Our treatment of safety-critical systems also applies to embedded systems.

UMLsafe: goals

Extensions for safe systems development.

- evaluate UML specifications for weaknesses in design
- encapsulate established rules of prudent safety engineering as checklist
- make available to developers not specialized in safety-critical systems
- consider safety from early design phases, in system context
- make certification cost-effective

The UMLsafe profile

Recurring safety requirements, failure scenarios, concepts offered as stereotypes with tags on component-level.

Use associated constraints to evaluate specifications and indicate possible weaknesses.

Ensures that UML specification provides desired level of safety.

Link to code via test-sequence generation.

Here: only fault tolerance aspects !

Failure semantics modelling

For redundancy model *R*, stereotype s?{ ¿ crash/performance À , ¿ value À }, have set Failures$_R$(s)? {delay(*t*), loss(*p*), corrupt(*q*)}:

- *t*: expected maximum time delay,
- *p*: probability that value not delivered within *t*,
- *q*: probability that value delivered in time corrupted

(in each case incorporating redundancy).

Or use ¿ risk À stereotype with {failure} tag.

Example

Suppose redundancy model *R* uses controller with redundancy *3* and the fastest result. Then could take:

- delay(*t*): *t* delay of fastest controller,
- loss(*p*): *p* probability that fastest result not delivered within *t*,
- corrupt(q): *q* probability that fastest result is corrupted.

¿ guarantee À

Describe guarantees required from communication dependencies resp. system components.

Tags: {goal} with value subset of {immediate(t), eventual(p), correct(q)}, where

- *t*: expected maximum time delay,
- *p*: probability that value is delivered within *t*,
- *q*: probability that value delivered in time not corrupted.

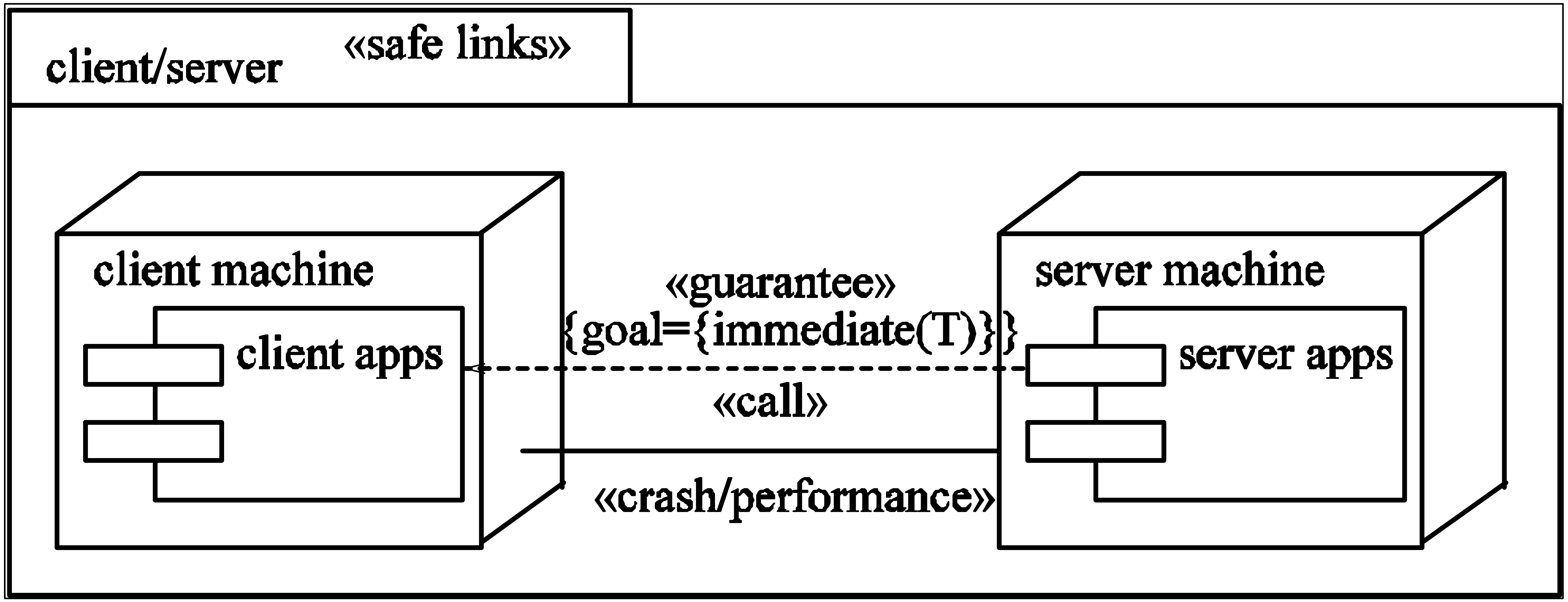
¿ safe links À

Physical layer should meet safety requirements on communication given redundancy model *R*.

Constraint: For dependency *d* stereotyped ¿ guarantee À have corresponding communication link *l* with stereotype *s* such that

- if {goal} has immediate(*t*) as value then delay(*t*‘) 2 Failures$_R$(*s*) implies *t*‘ · *t*,
- if {goal} has eventual(*p*) as value then loss(*p*‘) 2 Failures$_R$(*s*) implies *p*‘ · 1-*p*, and
- if {goal} has correct(*q*) as value then corruption(*q*‘) 2 Failures$_R$(*s*) implies *q*‘ · 1-*q*.

Example ¿ safe links À



Given redundany model none, ¿ safe links À fulfilled iff T · expected delay according to $\text{Failures}_{\text{none}}$(¿ crash/performance À).

¿ safe dependency À

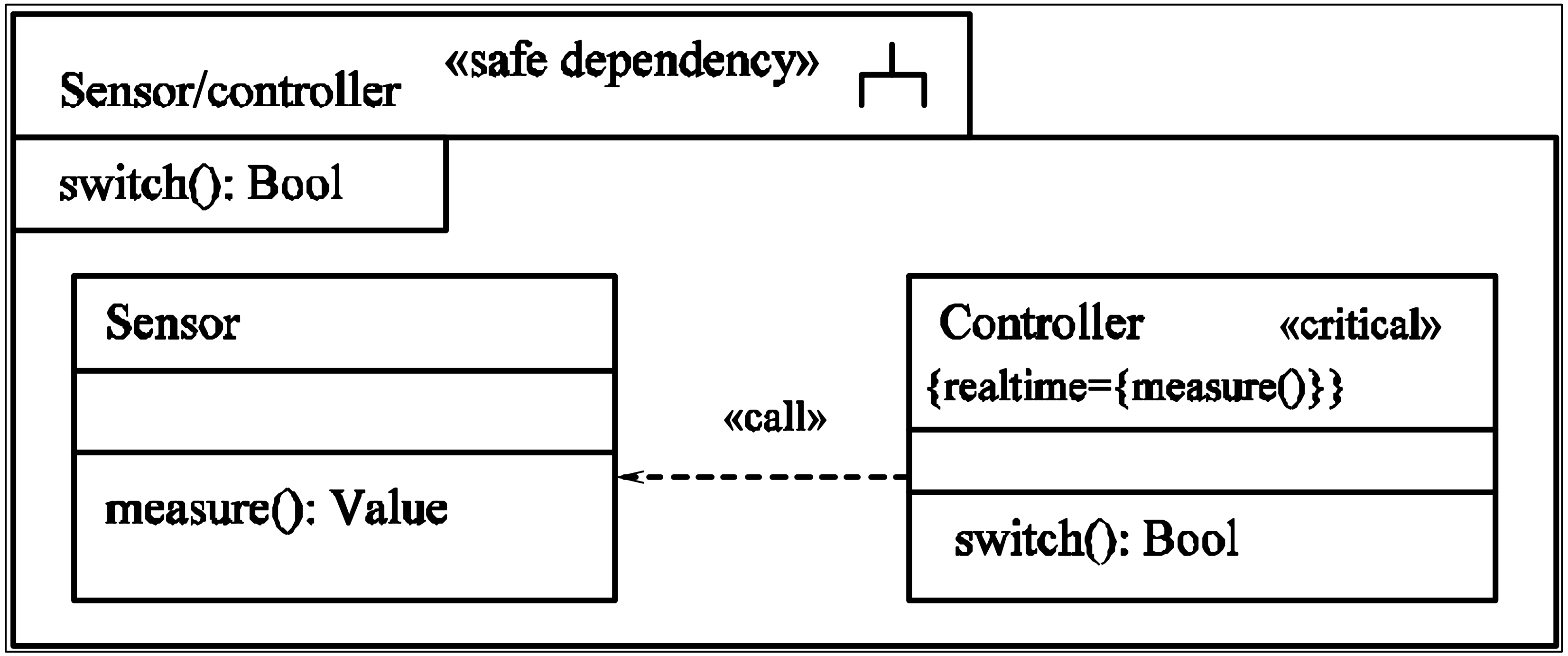
Communication dependencies should respect safety requirements on ¿ critical À data.

For each safety level {*l*} for ¿ critical À data, have goals(*l*) µ {immediate(*t*), eventual(*p*), correct(*q*)}.

Constraint: for each dependency *d* from *C* to *D* stereotyped ¿ guarantee À :

- Goals on data in *D* same as those in *C*.
- Goals on data in *C* also appearing in *D* met by guarantees of *d*.

Example ¿ safe dependency À



Assuming immediate(*t*) 2 goals(realtime), violates ¿ safe dependency À , since Sensor and dependency do not provide realtime goal immediate(*t*) for measure() required by Controller.

¿ safe behaviour À

Ensures that system behavior in presence of failure model provides required safety {goals} by requiring that in any trace *h* of the execution:

- immediate(*t*): Value delivered after at most *t* time steps.
- eventual(*p*): Probability that delivered value is lost during transmission at most 1-*p*.
- correct(*q*): Probability that delivered value corrupted during transmission at most 1-*q*.

¿ containment À

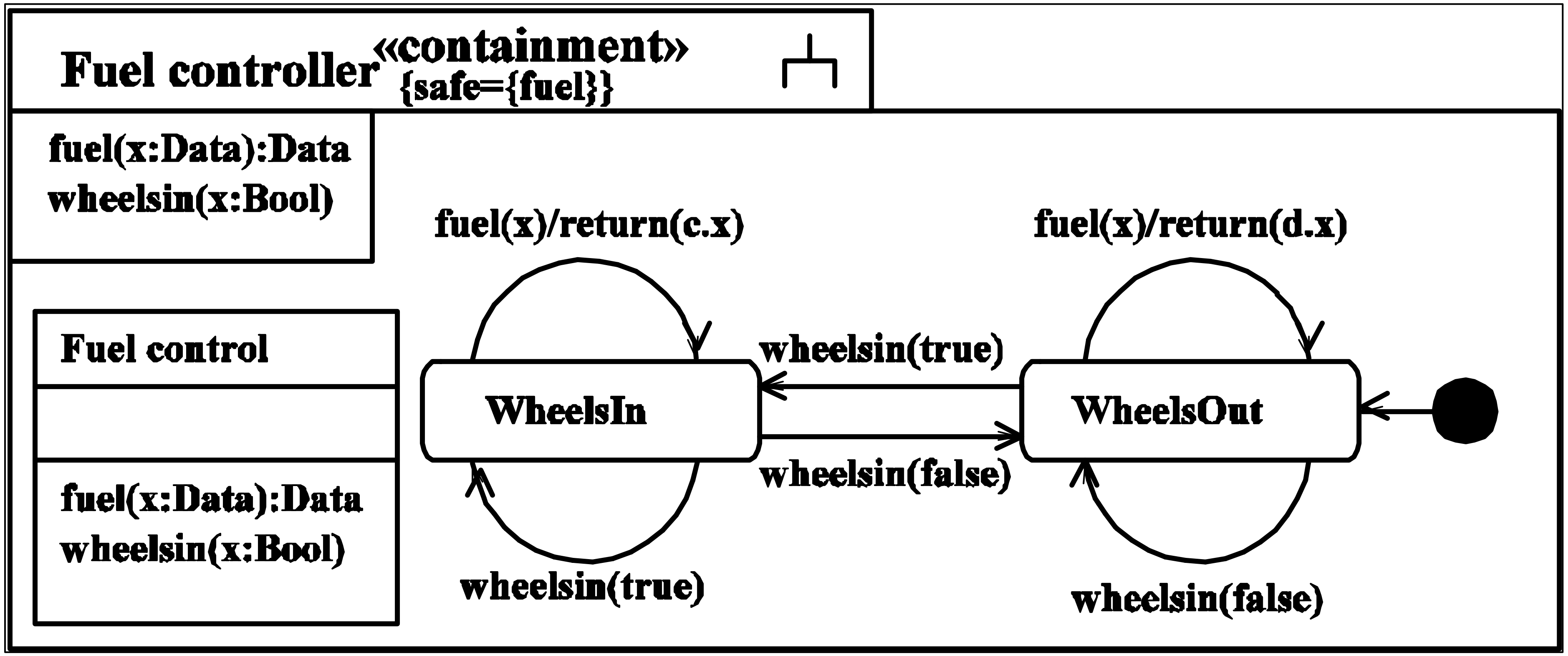
Prevent indirect corruption of data.

Constraint:

Value of any data element *d* may only be influenced by data whose requirements attached to ¿ critical À imply those of *d*.

Make precise by referring to execution semantics (view of history associated with safety level).

Example ¿containmentÀ



Violates containment because a {safe} value depends on un{safe} value.

Can check this mechanically.

Other checks

Have other consistency checks such as

- Is the software‘s response to out-of-range values specified for every input ?
- If input arrives when it shouldn't, is a response specified ?

…and other safety checks from the literature.

Failure models

lq^l_n: messages on link l delayed further n time units.

p^h_n: probability of failure at nth iteration in history h.

For link l stereotyped s where $loss(p) 2 Failures_R(s)$,

- history may give $lq^l_0 := ;$; then append p to $(p^h_n)_{n 2 N}$,
- or no change, then append $1\text{-}p$.

For link l stereotyped s where $corruption(q) 2 Failures_R(s)$,

- history may give $lq^l_0 := \{¥\}$; then append q,
- or no change; append $1\text{-}q$.

For link l stereotyped s with $delay(t) 2 Failures_R(s)$, and $lq^l_0 \neq ;$, history may give $lq^l_n := lq^l_0$ for $n \cdot t$; append $1/t$.

Then for each n, $lq^l_n := lq^l_{n+1}$.

Execution semantics

Behavioral interpretation of a UML subsystem:

(1) Takes input events.

(2) Events distributed from input and link queues between subcomponents to intended recipients where they are processed.

(3) Output distributed to link or output queues.

(4) Failure model applied as defined above.

Roadmap

Prologue
UML
UMLsafe
Security-critical systems
UMLsec: The profile
Security analysis

Security patterns
UMLsec case studies
Java security, CORBAsec
Tools
Model-based Testing

A Need for Security

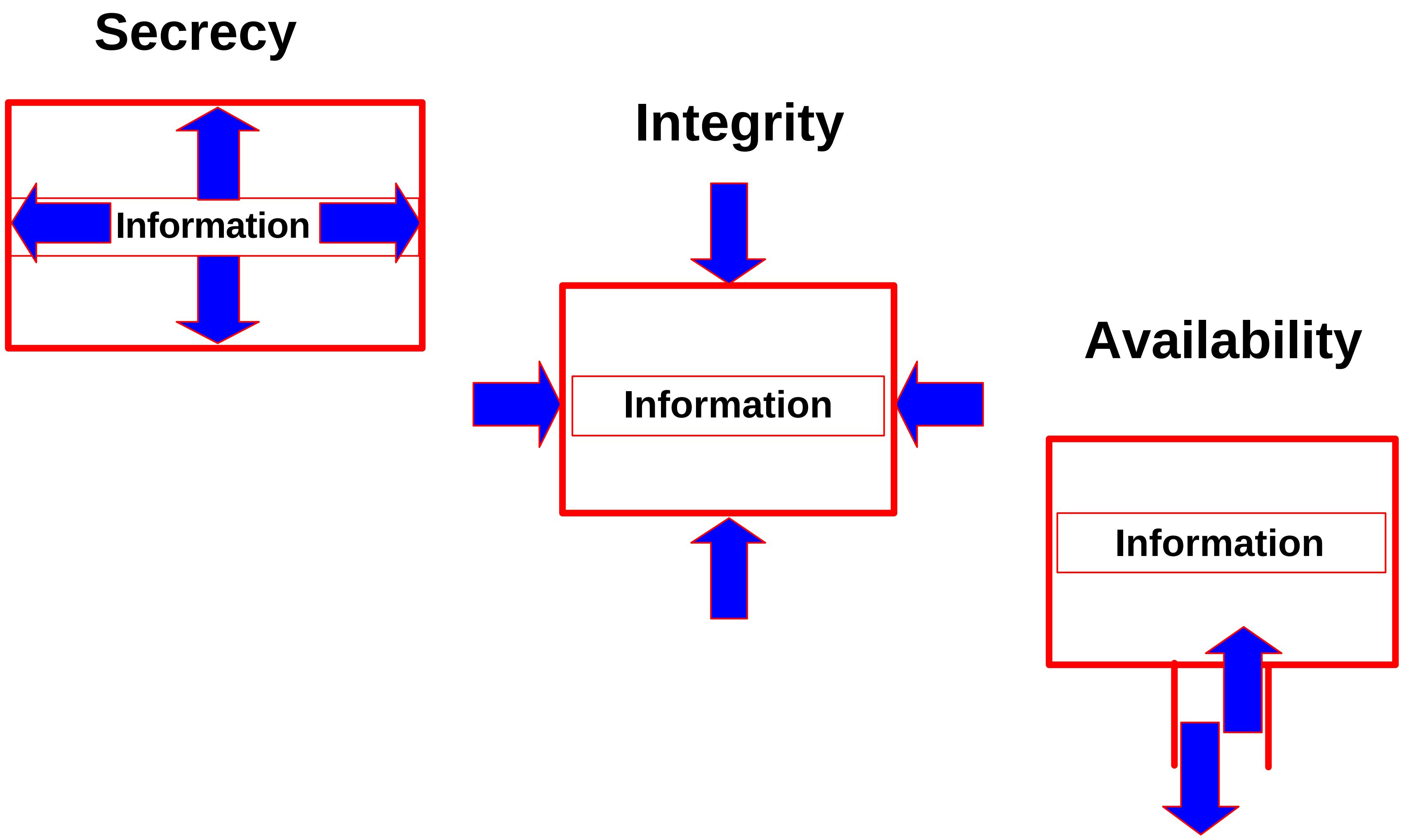
Society and economies rely on computer networks for communication, finance, energy distribution, transportation...

Attacks threaten economical and physical integrity of people and organizations.

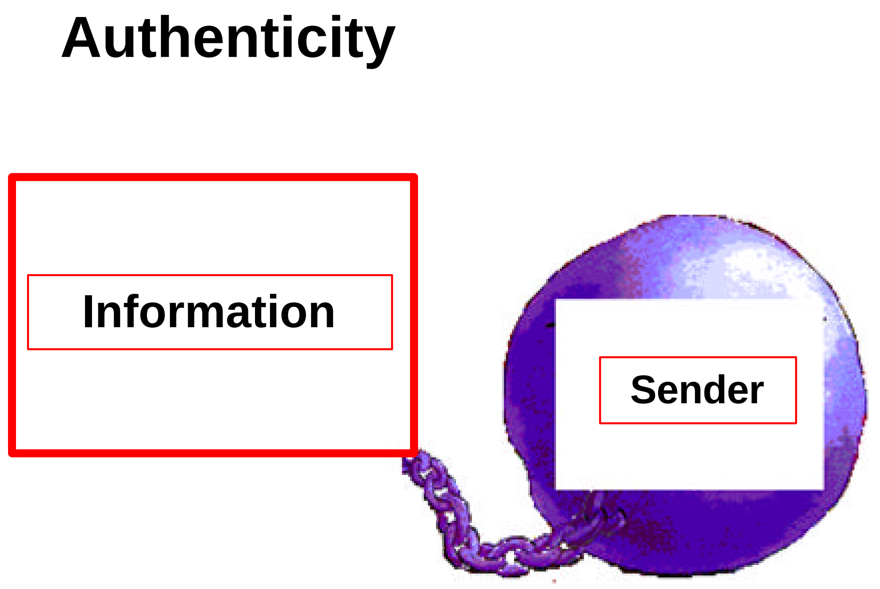
Interconnected systems can be attacked anonymously and from a safe distance.

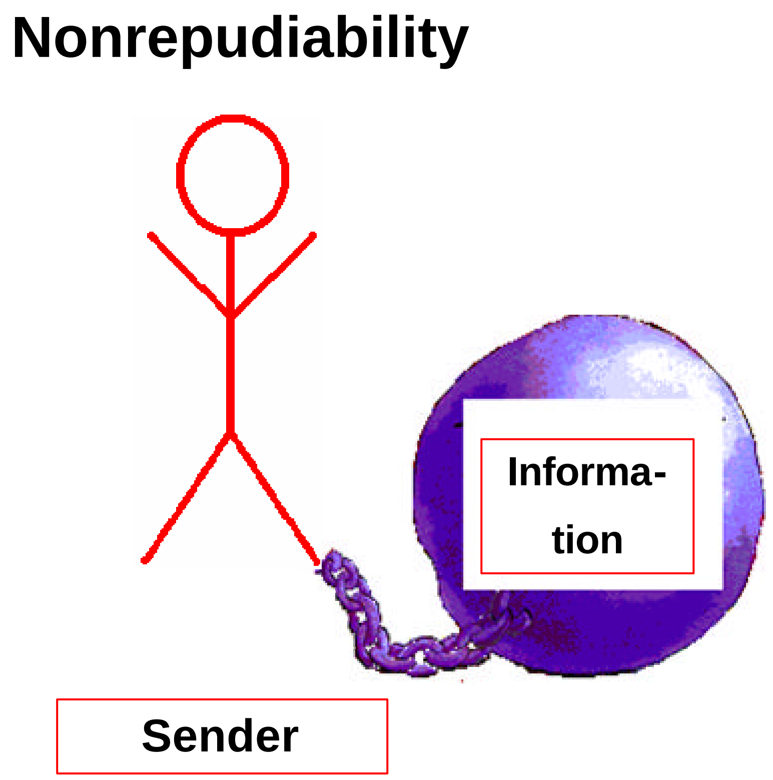
Networked computers need to be secure.

Basic Security Requirements I



Basic Security Requirements II





Problems

Many flaws found in designs of security-critical systems, sometimes years after publication or use.

Spectacular Example (1997):

NSA hacker team breaks into U.S. Department of Defense computers and the U.S.electric power grid system. Simulates power outages and 911 emergency telephone overloads in Washington, D.C..

Causes I

- Designing secure systems correctly is difficult.
  Even experts may fail:
  - Needham-Schroeder protocol (1978)
  - attacks found 1981 (Denning, Sacco), 1995 (Lowe)
- Designers often lack background in security.
- Security as an afterthought.

Causes II

Cannot use security mechanisms „blindly“:

- Security often compromised by circumventing (rather than breaking) them.
- Assumptions on system context, physical environment.

„Those who think that their problem can be solved by simply applying cryptography don`t understand cryptography and don`t understand their problem“ (Lampson, Needham).

Difficulties

Exploit information spreads quickly.

No feedback on delivered security from customers.

Previous approaches

„Penetrate-and-patch“: unsatisfactory.

- insecure (damage until discovered)
- disruptive (distributing patches costs money, destroys confidence, annoys customers)

Traditional formal methods: expensive.

- training people
- constructing formal specifications.

Goal: Security by design

Consider security

- from early on
- within development context
- taking an expansive view
- in a seamless way.

Secure design by model analysis.

Secure implementation by test generation.

Holistic view on Security

„An expansive view of the problem is most appropriate to help ensure that no gaps appear in the strategy“ (Saltzer, Schroeder 1975).

But „no complete method applicable to the construction of large general-purpose systems exists yet“ - since 1975.

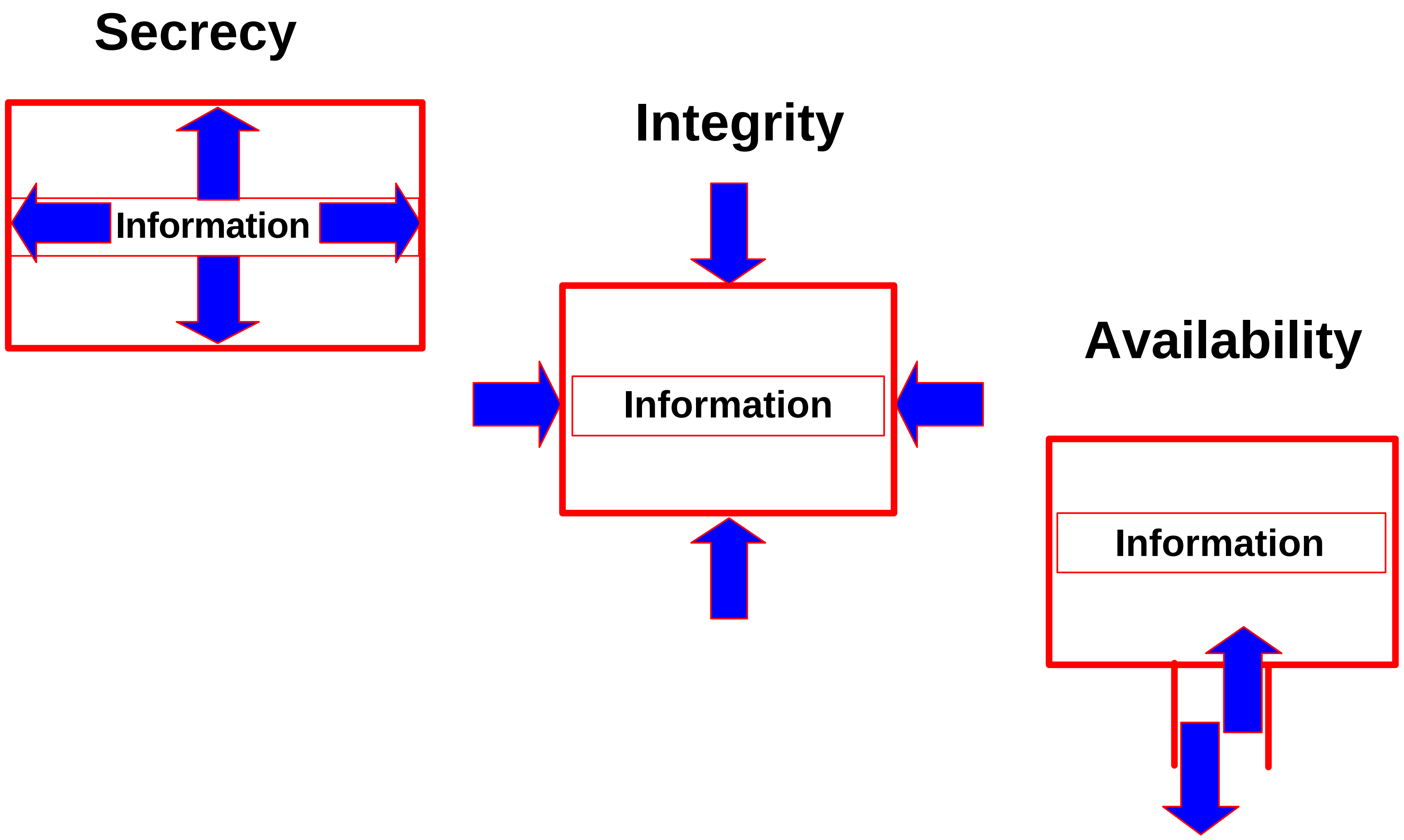
Roadmap

UMLsec

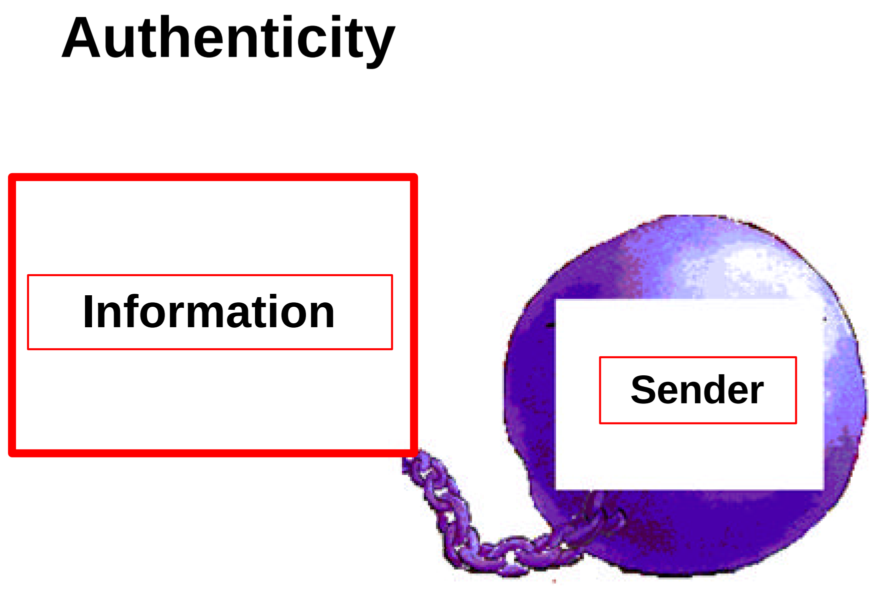
UMLsec: extension for secure systems development.

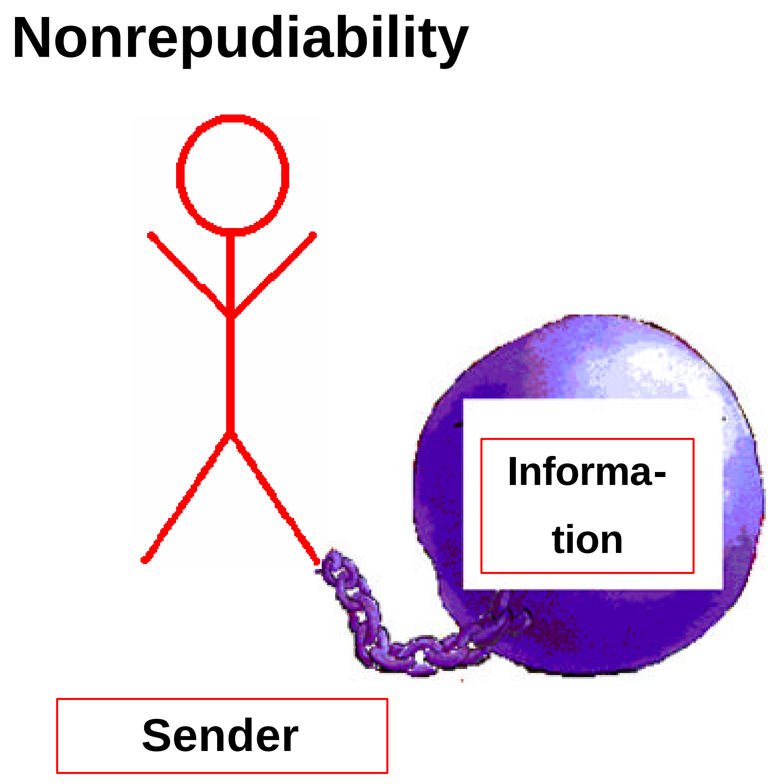
- evaluate UML specifications for vulnerabilities
- encapsulate security engineering patterns
- also for developers not specialized in security
- security from early design phases, in system context
- make certification cost-effective

Basic Security Requirements I



Basic Security Requirements II





The UMLsec profile

Recurring security requirements as stereotypes with tags (secrecy, integrity,...).

Associated constraints to evaluate model, indicate possible vulnerabilities.

Ensures that stated security requirements enforce given security policy.

Ensures that UML specification provides requirements.

Requirements on UML extension for security I

Mandatory requirements:

- Provide basic security requirements such as secrecy and integrity.
- Allow considering different threat scenarios depending on adversary strengths.
- Allow including important security concepts (e.g. *tamper-resistant hardware*).
- Allow incorporating security mechanisms (e.g. access control).

Requirements on UML extension for security II

- Provide security primitives (e.g. (a)symmetric encryption).
- Allow considering underlying physical security.
- Allow addressing security management (e.g. secure workflow).

Optional requirements: Include domain-specific security knowledge (Java, smart cards, CORBA, ...).

From UMLsafe to UMLsec

Safety = „Security against stupid adversaries“

Security = „Safety for paranoids“

Adversaries in security correspond to failures in safety.

Replace failure model in UMLsafe by adversary model to get UMLsec.

UMLsec: general ideas

Activity diagram: secure control flow, coordination

Class diagram: exchange of data preserves security levels

Sequence diagram: security-critical interaction

Statechart diagram: security preserved within object

Deployment diagram: physical security requirements

Package: holistic view on security

UMLsec profile (excerpt)

Stereotype	Base class	Tags	Constraints	Description
Internet	link			Internet connection
secure links	subsystem		dependency security matched by links	enforces secure communication links
secrecy	dependency			assumes secrecy
secure dependency	subsystem		call, send respect data security	structural interaction data security
no down-flow	subsystem	high	prevents down-flow	information flow
data security	subsystem		provides secrecy, integrity	basic datasec requirements
fair exchange	package	start, stop	after start eventually reach stop	enforce fair exchange
guarded access	Subsystem		guarded objects acc. through guards.	access control using guard objects

¿ Internet À , ¿ encrypted À , ...

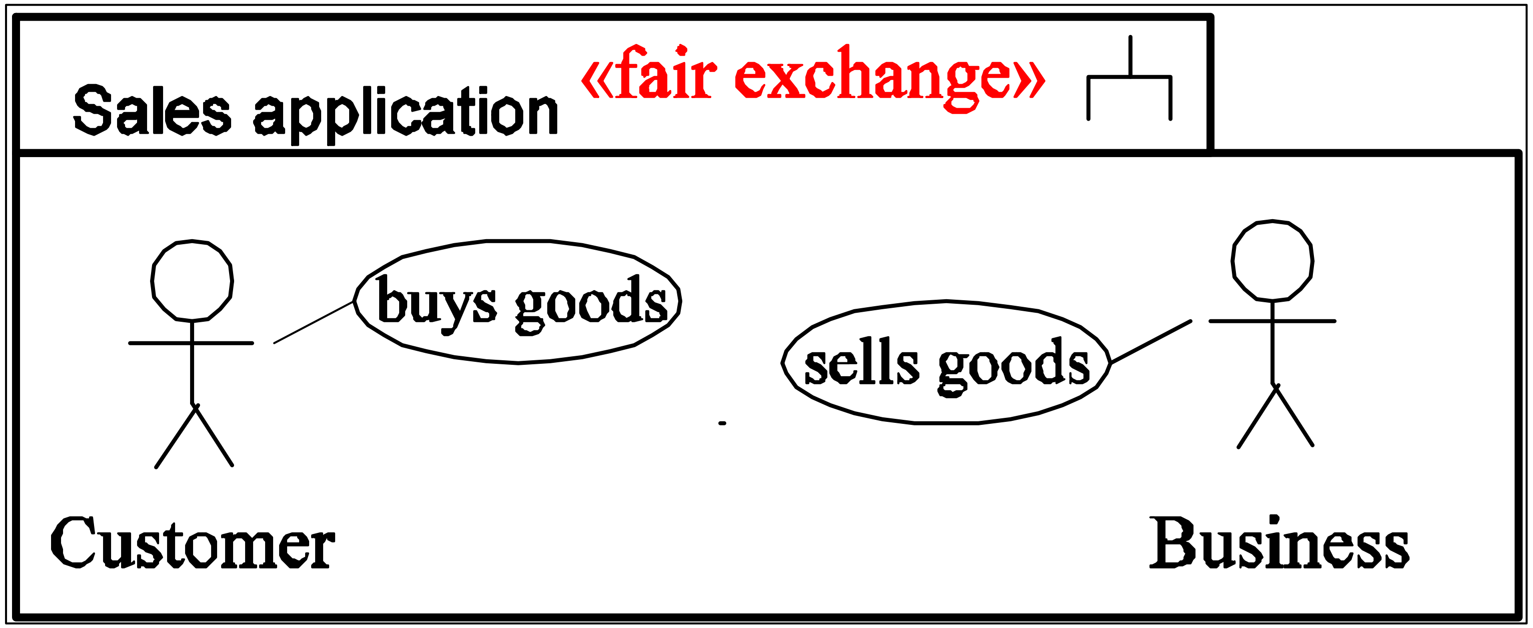
Kinds of communication links resp. system nodes.

For adversary type A, stereotype s, have set $\mathrm{Threats}_A$ (s) ? {delete, read, insert, access} of actions that adversaries are capable of.

Default attacker:

Stereotype	$\mathrm{Threats}_{default}$ ()
Internet	{delete, read, insert}
encrypted	{delete}
LAN	Ø
smart card	Ø

Requirements with use case diagrams



Capture security requirements
in use case diagrams.

Constraint: need to appear in
corresponding activity diagram.

¿ fair exchange À

Ensures generic fair exchange condition.

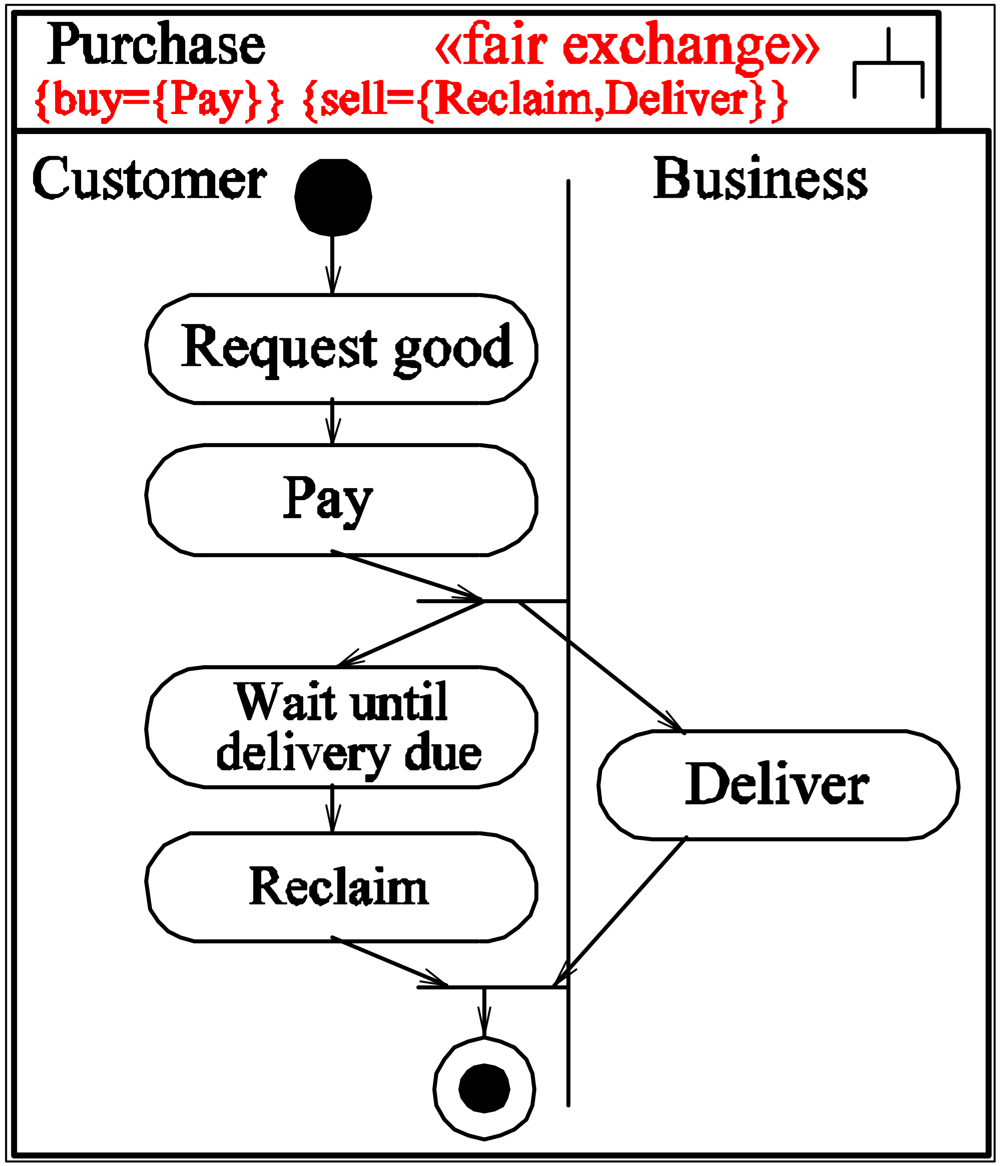
Constraint: after a {buy} state in activity diagram is reached, eventually reach {sell} state.

(Cannot be ensured for systems that an attacker can stop completely.)

Example ¿ fair exchange À

Customer buys a good from a business.

Fair exchange means: after payment, customer is eventually either delivered good or able to reclaim payment.



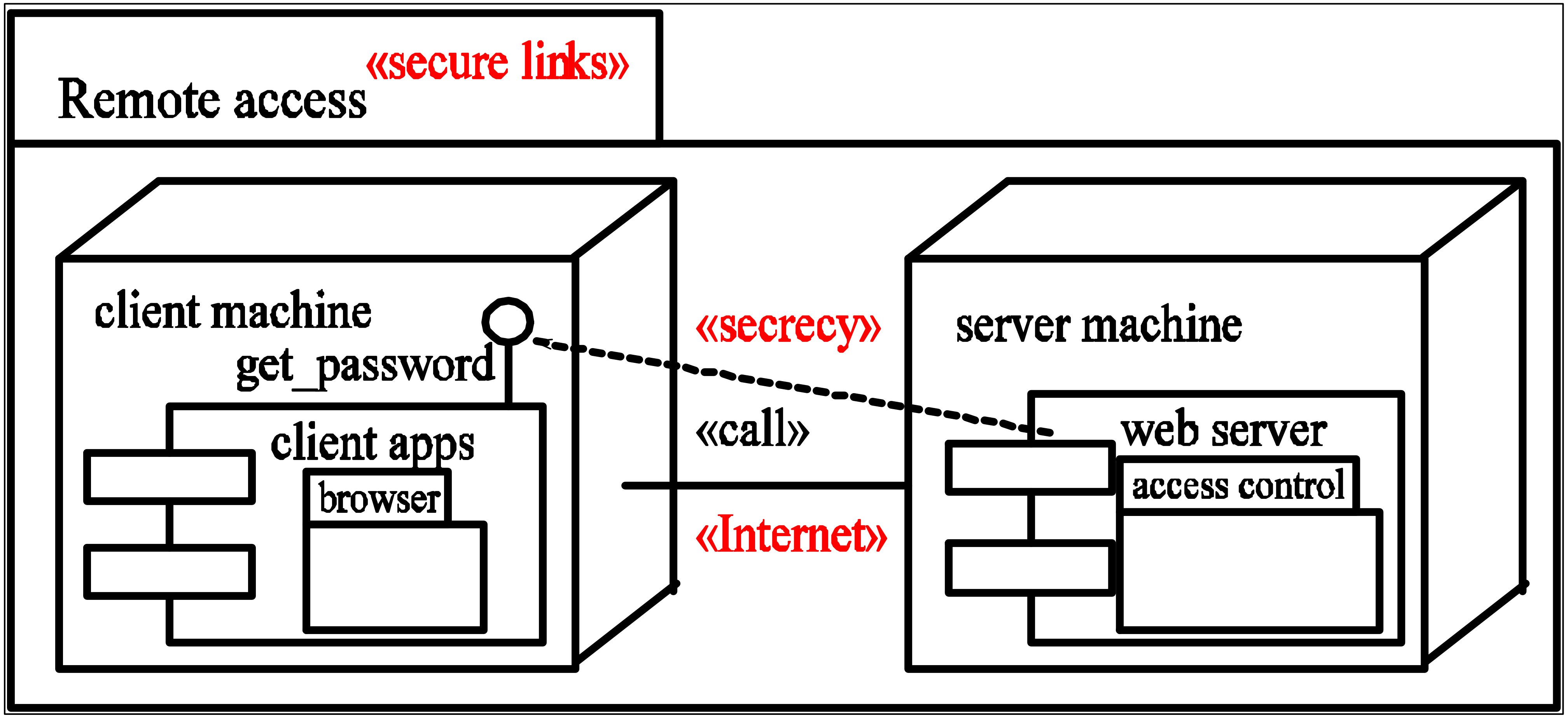
¿ secure links À

Ensures that physical layer meets security requirements on communication.

Constraint: for each dependency *d* with stereotype s ? { ¿ secrecy À , ¿ integrity À } between components on nodes *n*? *m*, have a communication link *l* between *n* and *m* with stereotype *t* such that

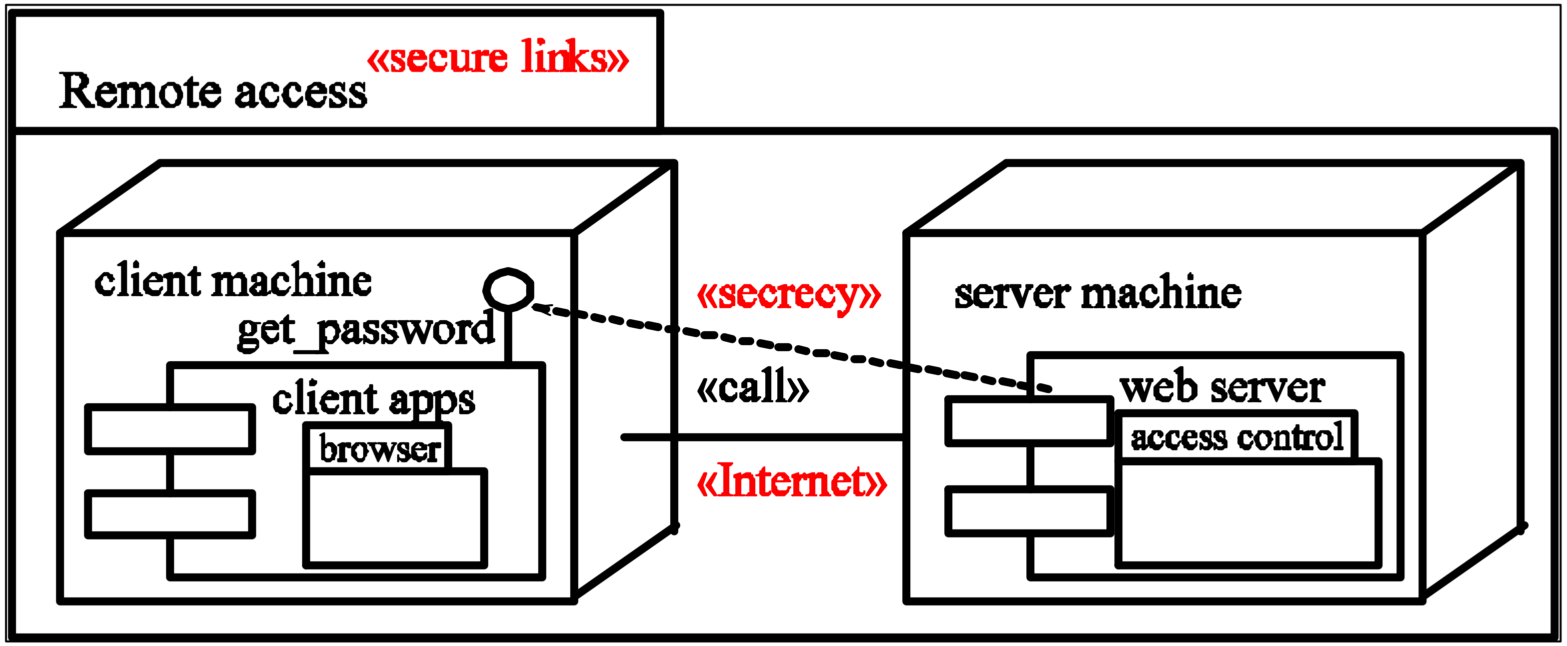
- if *s* = ¿ secrecy À : have read ? Threats$_A$*(t)*.
- if *s* = ¿ integrity À : have insert ? Threats$_A$ *(t)*.

Example ¿ secure links À



Given default adversary type, is ¿ secure links À provided ?

Example ¿ secure links À



Given default adversary type, constraint for stereotype ¿ secure links À violated: According to the Threats$_{default}$(Internet) scenario, ¿ Internet À link does not provide secrecy against default adversary.

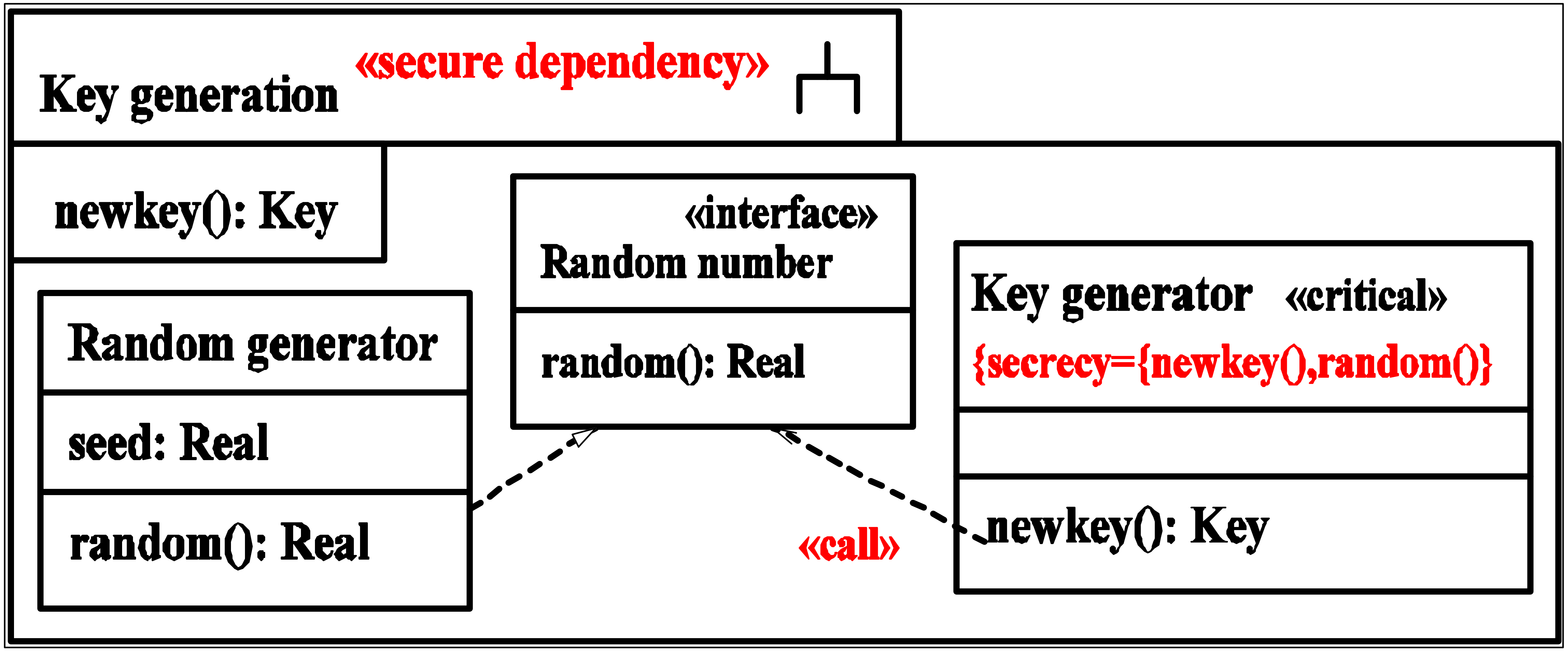
¿ secure dependency À

Ensure that ¿ call À and ¿ send À dependencies between components respect security requirements on communicated data given by tags {secrecy}, {integrity}.

Constraint: for ¿ call À or ¿ send À dependency from *C* to *D* (and similarly for {secrecy}):

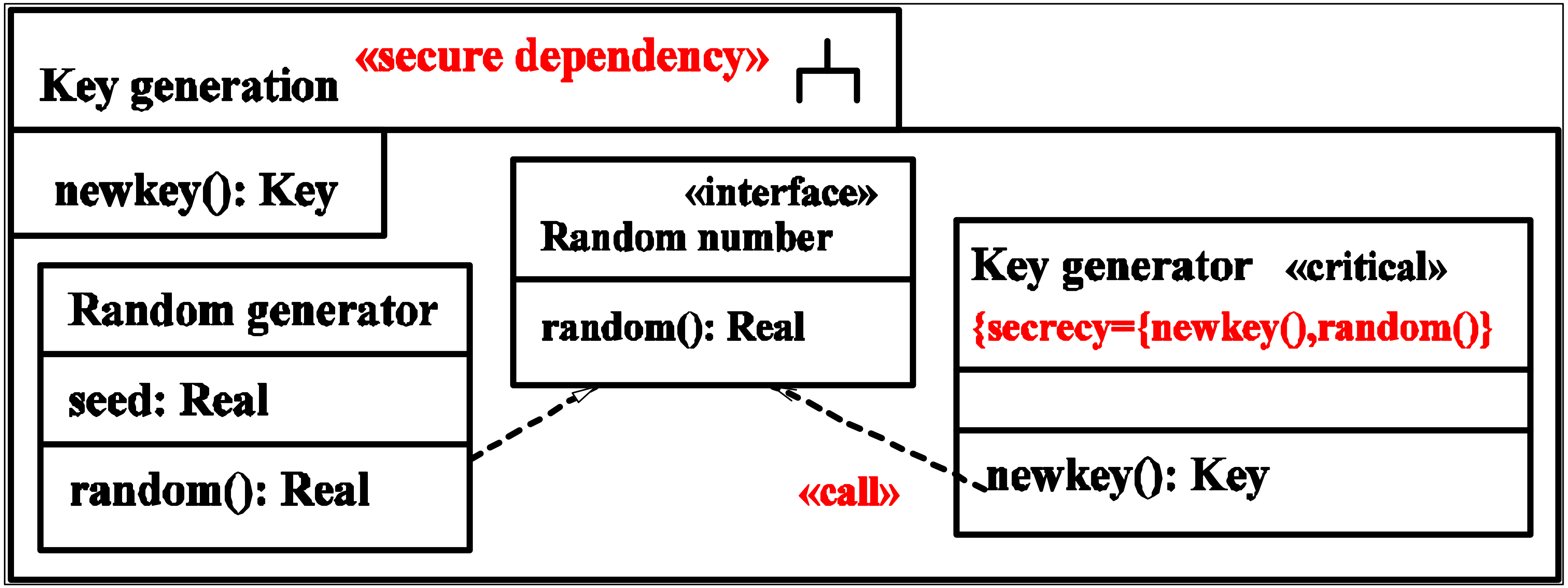
- Msg in *D* is {secrecy} in *C* if and only if also in *D*.
- If msg in *D* is {secrecy} in *C*, dependency stereotyped ¿ secrecy À .

Example ¿ secure dependency À



¿ secure dependency À provided ?

Example ¿secure dependencyÀ



Violates ¿secure dependencyÀ: Random generator and ¿callÀ dependency do not give security level for random() to key generator.

¿ no down–flow À

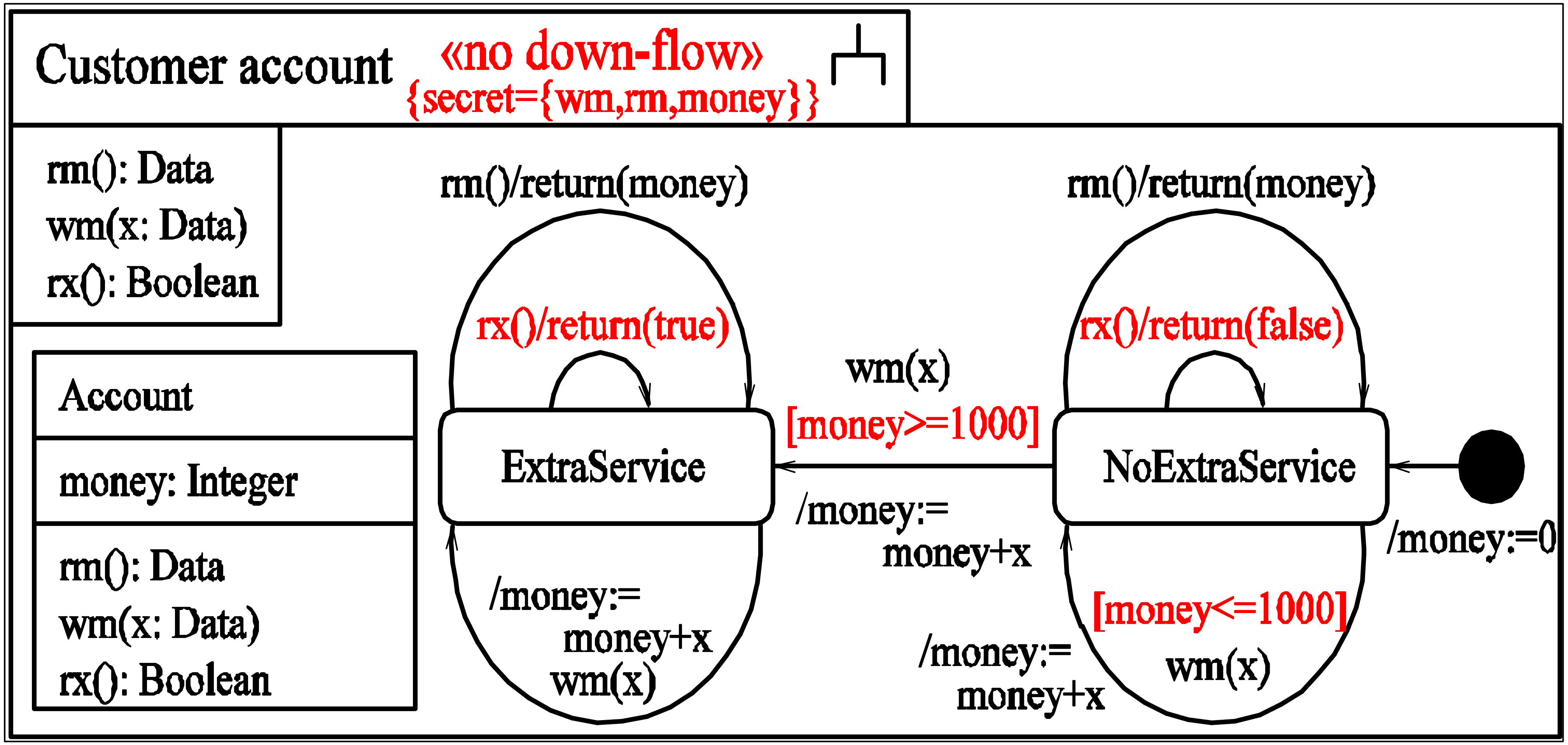
Enforce secure information flow.

Constraint:

Value of any data specified in {secrecy} may influence only the values of data also specified in {secrecy}.

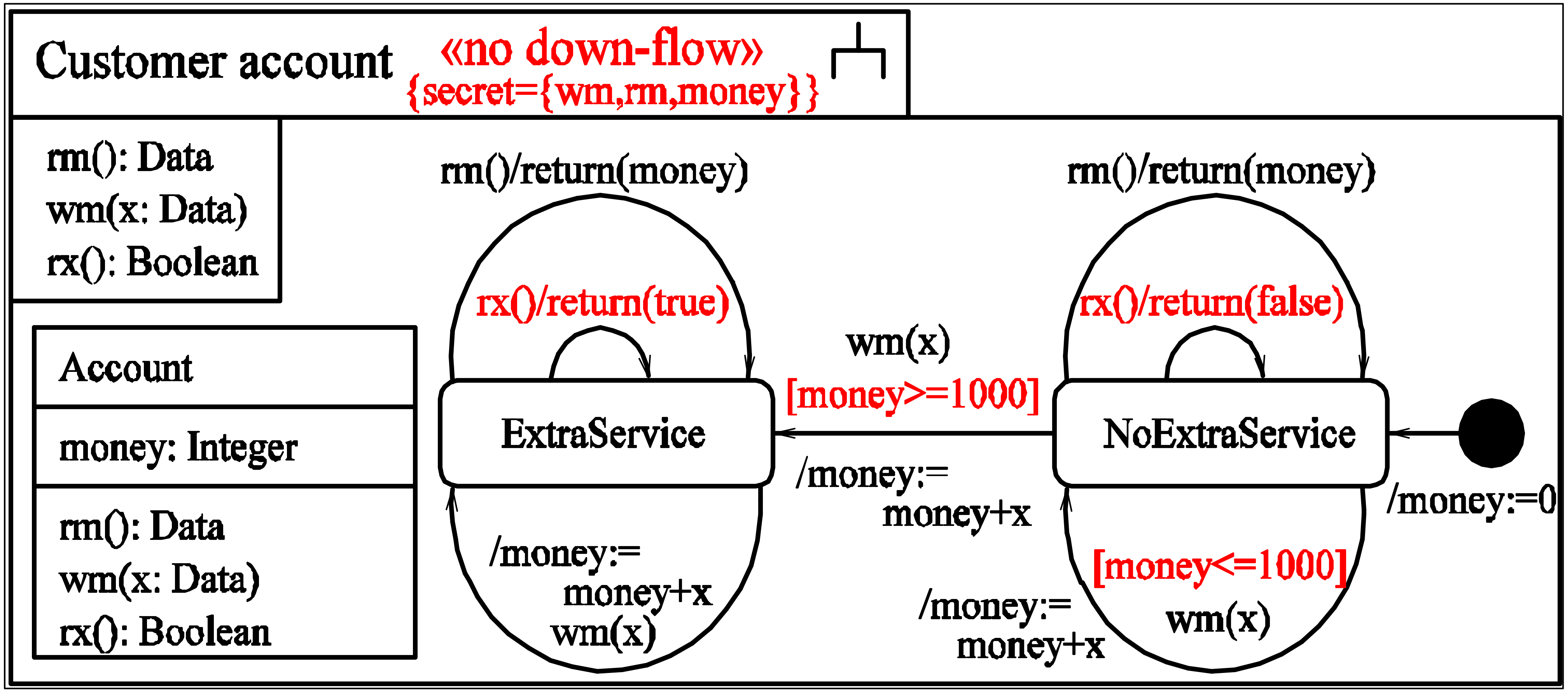
Formalize by referring to formal behavioural semantics.

Example ¿ no down-flow À



¿ no down–flow À provided ?

Example ¿ no down-flow À



¿ no down–flow À violated: partial information on input of high wm() returned by non-high rx().

¿ data security À

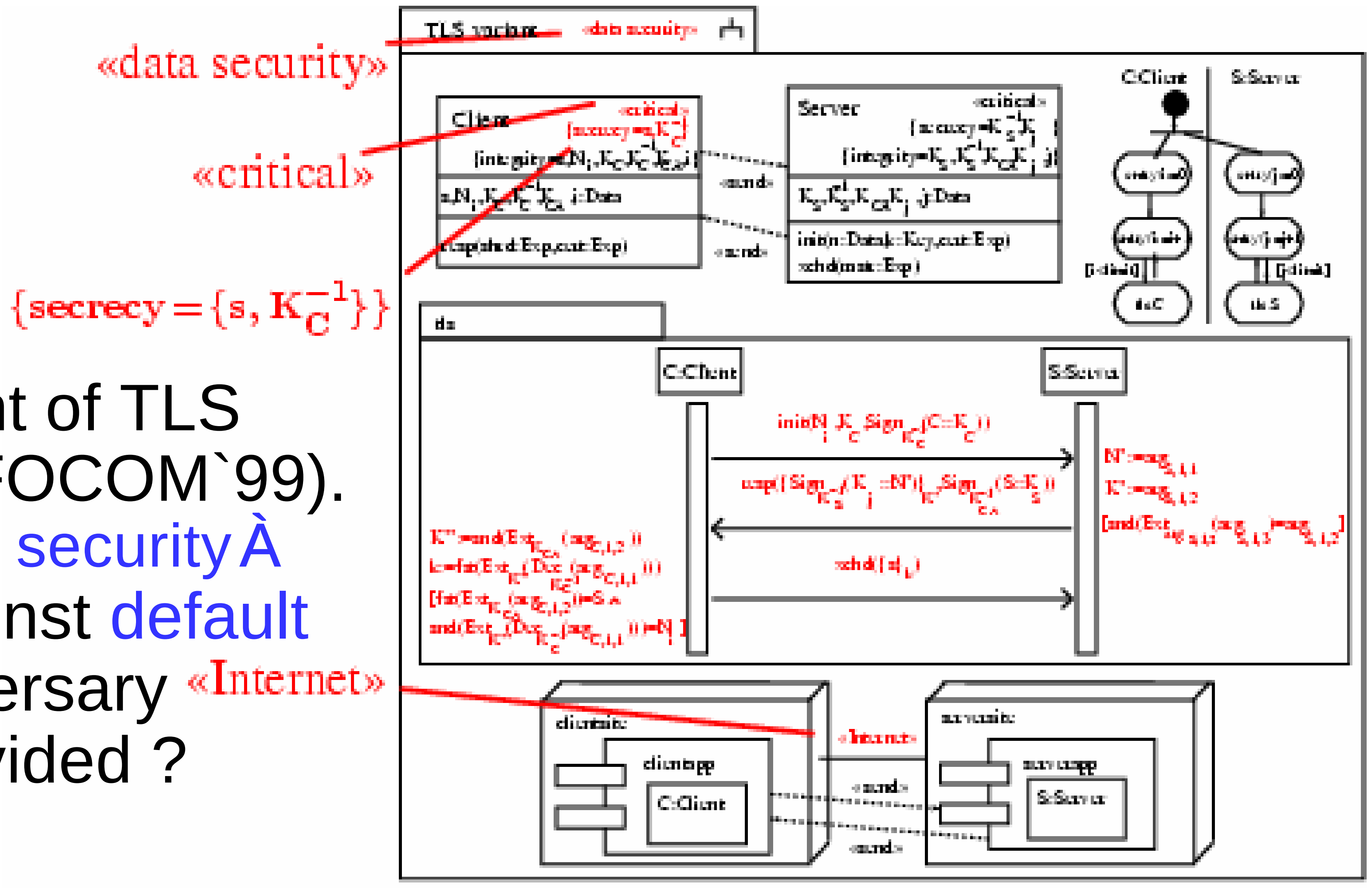
Security requirements of data marked ¿ critical À enforced against threat scenario from deployment diagram.

Constraints:

Secrecy of {secrecy} data preserved.

Integrity of {integrity} data preserved.

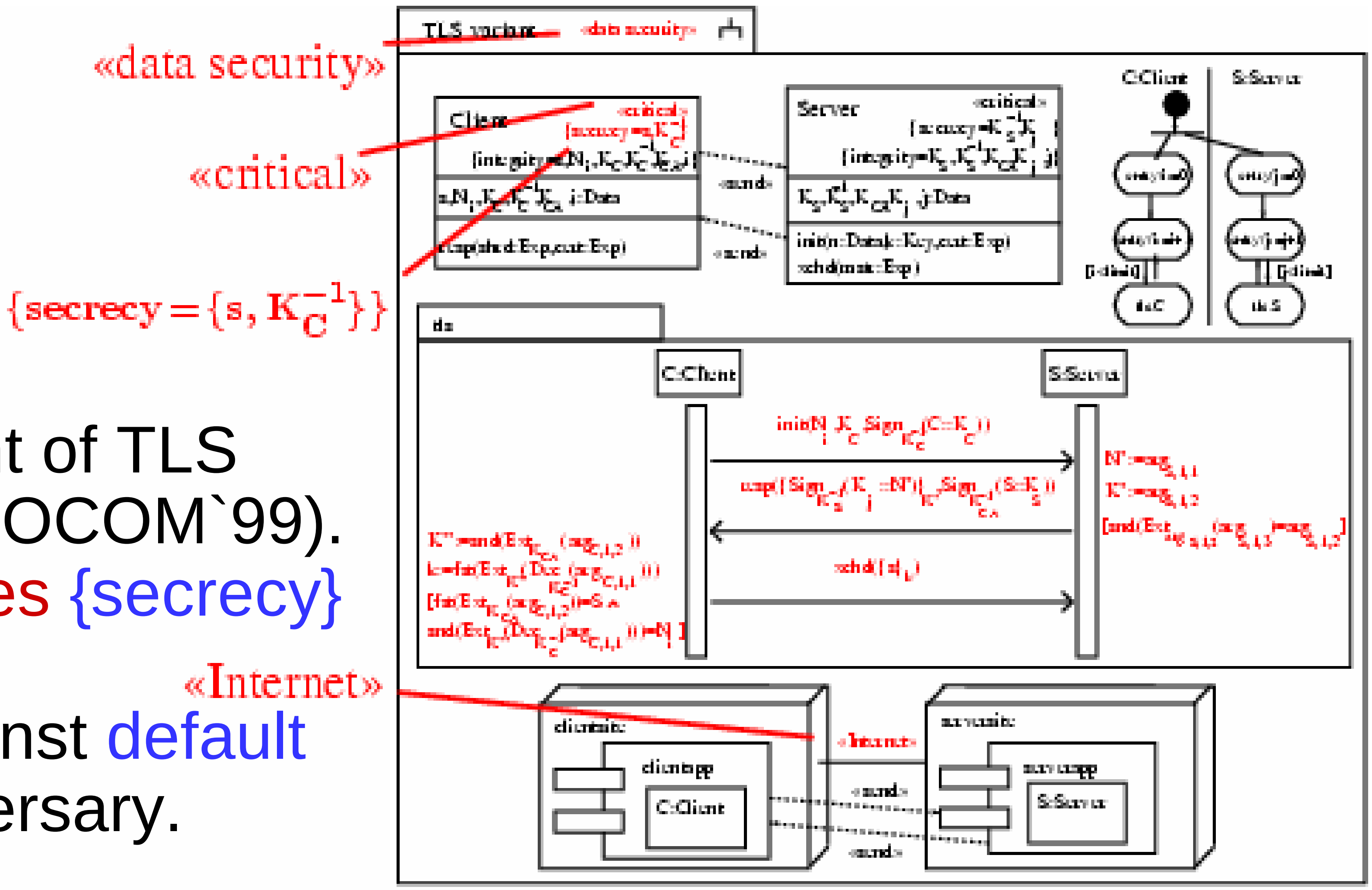
Example ¿ data security À



Variant of TLS (INFOCOM`99).

¿ data security À against default adversary provided ?

Example ¿ data security À



Variant of TLS (INFOCOM`99).

Violates {secrecy} of s against default adversary.

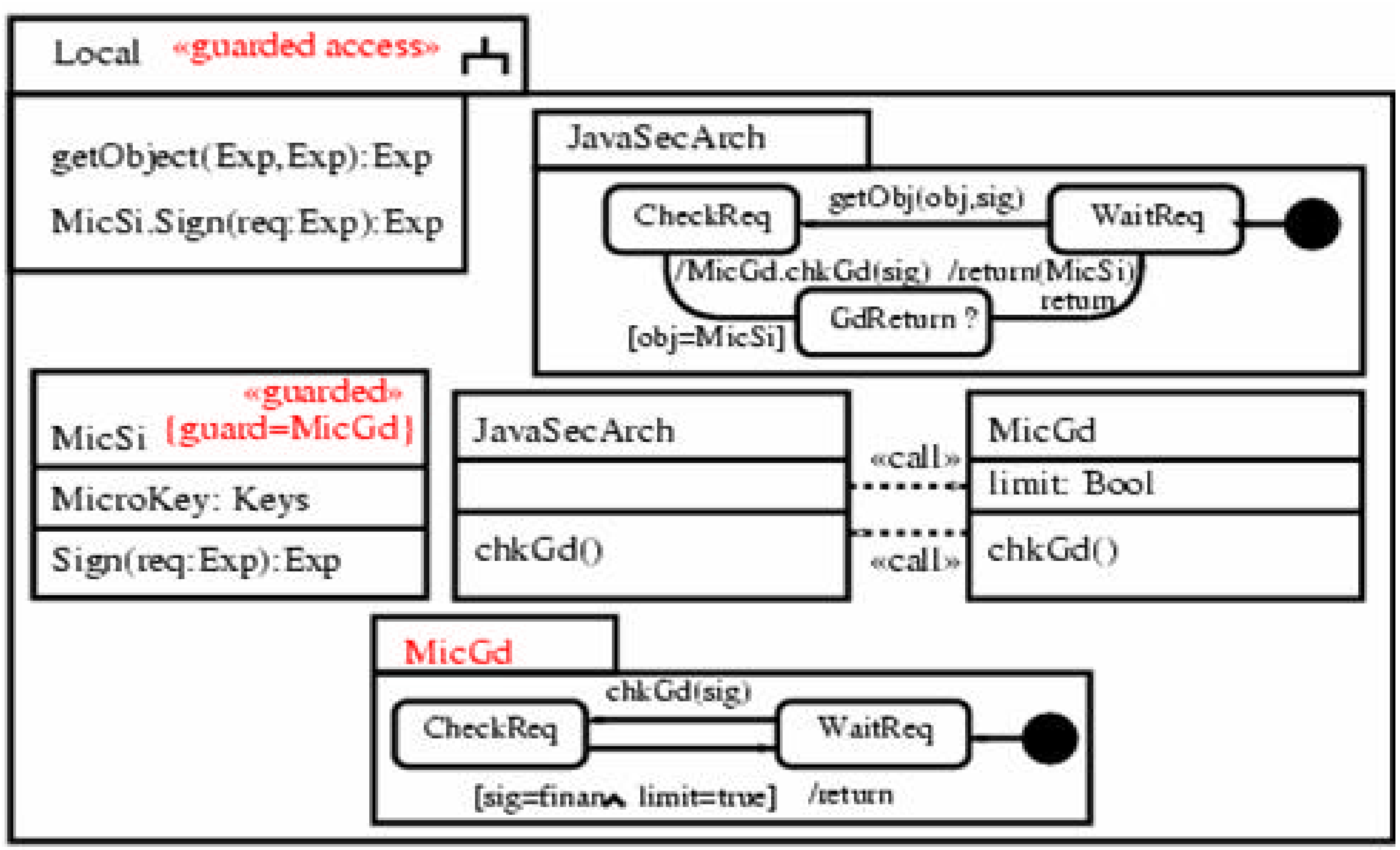
¿ guarded access À

Ensures that in Java, ¿ guarded À classes only accessed through {guard} classes.

Constraints:

- References of ¿ guarded À objects remain secret.
- Each ¿ guarded À class has {guard} class.

Example ¿guarded accessÀ



Provides ¿guarded accessÀ:

Access to MicSi protected by MicGd.

Does UMLsec meet requirements?

Security requirements: ¿ secrecy À ,…

Threat scenarios: Use $\mathrm{Threats}_{\mathrm{adv}}$(ster).

Security concepts: For example ¿ smart card À .

Security mechanisms: E.g. ¿ guarded access À .

Security primitives: Encryption built in.

Physical security: Given in deployment diagrams.

Security management: Use activity diagrams.

Technology specific: Java, CORBA security.

Roadmap

Security Protocols

System distributed over untrusted networks.

„Adversary“ intercepts, modifies, deletes, inserts messages.

Cryptography provides security.

Cryptographic Protocol: Exchange of messages for distributing session keys, authenticating principals etc. using cryptographic algorithms

Security Protocols: Problems

Many protocols have vulnerabilities or subtleties for various reasons

- weak cryptography
- core message exchange
- interfaces, prologues, epilogues
- deployment
- implementation bugs

Using UML

Goal: transport results from formal methods to security practice

Enable developers (not trained in formal methods) to

- check correctness of hand-made security protocols
- deploy protocols correctly in system context
- allow to analyze larger system parts beyond protocols

Security Analysis

Specify protocol participants as processes following Dolev, Yao 1982: In addition to expected participants, model attacker who:

- may participate in some protocol runs,
- knows some data in advance,
- may intercept messages on the public network,
- injects messages that it can produce into the public network

Security Analysis

Model classes of adversaries.

May attack different parts of the system according to threat scenarios.

Example: insider attacker may intercept communication links in LAN.

To evaluate security of specification, simulate jointly with adversary model.

Security Analysis II

Keys are symbols, crypto-algorithms are abstract operations.

- Can only decrypt with right keys.
- Can only compose with available messages.
- Cannot perform statistical attacks.

Specification language

Formal semantics for (even restricted) parts of UML too complicated to present in this talk.

To convey ideas, use simple calculus whose main properties relevant here are similar to UML statechart/sequence diagram behaviour.

- in particular: asynchronous communication (no refusal by receiver)
- include cryptographic primitives

Expressions

Exp: term algebra generated by
Var? Keys? Data and

- *_::_* (concatenation),
- *{ _ }_* (encryption)
- *Dec_( )* (decryption)
- *Sign_( )* (signing)
- *Ext_( )* (extracting from signature)

by factoring out the equations $Dec_{K^{-1}}(\{E\}_K)=E$
and $Ext_K(Sign_{K^{-1}}(E))=E$ (for *K?Keys*).

Programs

$$p \quad ::= \quad \bar{op}(exp).p' \mid \textbf{if } bexp \textbf{ then } p_1 \textbf{else } p_2 \mid \sum_i op_i(var).p_i \mid p_1 || p_2 \mid 0$$

(*exp2 Exp; bexp* Boolean expression over *(Exp,=)*).

Iteration by CCS-style guarded recursive equations:

iter$_i$*(p*$_i$*):=p*$_0$*.***iter**$_i$*(p*$_{i+1}$*)*

Next: Structural Operational Semantics

$$\bar{op}(exp).p \overset{\bar{op}(exp)}{\longrightarrow} p \qquad exp \in \mathbf{Exp}$$

$$\sum_i op_i(var).p_i \overset{op_k(exp)}{\longrightarrow} p[exp/var_k] \qquad exp \in \mathbf{Exp}$$

$$\mathbf{if}\ bexp\ \mathbf{then}\ p_1 \mathbf{else}\ p_2 \overset{\tau}{\rightarrow} p_1 \qquad bexp = true$$

$$\mathbf{if}\ bexp\ \mathbf{then}\ p_1 \mathbf{else}\ p_2 \overset{\tau}{\rightarrow} p_2 \qquad bexp = false$$

$$\frac{p_1 \overset{op(exp)}{\longrightarrow} p_1', p_2 \overset{op(exp)}{\longrightarrow} p_2'}{p_1 || p_2 \overset{op(exp)}{\longrightarrow} p_1' || p_2'} \qquad exp \in \mathbf{Exp}$$

$$\frac{p_1 \overset{op(exp)}{\longrightarrow} p_1', \neg p_2 \overset{op(exp)}{\longrightarrow}}{p_1 || p_2 \overset{op(exp)}{\longrightarrow} p_1' || p_2} \qquad \text{and symmetric}$$

$$\frac{p_1 \overset{\bar{op}(exp)}{\longrightarrow} p_1'}{p_1 || p_2 \overset{\bar{op}(exp)}{\longrightarrow} p_1' || p_2} \qquad \text{and symmetric}$$

Interaction

$$\frac{\mathcal{P}_1 \overset{\bar{op}(exp)}{\longrightarrow} \mathcal{P}_1'}{\mathcal{P}_1 \otimes_q^{\mathcal{I}} \mathcal{P}_2 \xrightarrow{\tau} \mathcal{P}_1' \otimes_{q.msg}^{\mathcal{I}} \mathcal{P}_2} op \in \mathcal{I} \qquad \frac{\mathcal{P}_1 \overset{op(exp)}{\longrightarrow} \mathcal{P}_1'}{\mathcal{P}_1 \otimes_{msg.q}^{\mathcal{I}} \mathcal{P}_2 \xrightarrow{\tau} \mathcal{P}_1' \otimes_q^{\mathcal{I}} \mathcal{P}_2} op \in \mathcal{I}$$

$$\frac{\mathcal{P}_1 \xrightarrow{a} \mathcal{P}_1'}{\mathcal{P}_1 \otimes_q^{\mathcal{I}} \mathcal{P}_2 \xrightarrow{a} \mathcal{P}_1' \otimes_q^{\mathcal{I}} \mathcal{P}_2} \qquad a \notin \mathcal{I}$$

(plus symmetric).

Message buffers *q*, interface I .

Write $\xrightarrow{I}$ for $\xrightarrow{I}_{\emptyset}$.

Interaction via untrusted network

Adversary may be able to access messages on network: read, delete, insert

➔ Messages via adversary

Analyze P - A where A is a non-deterministic process modeling the adversary.

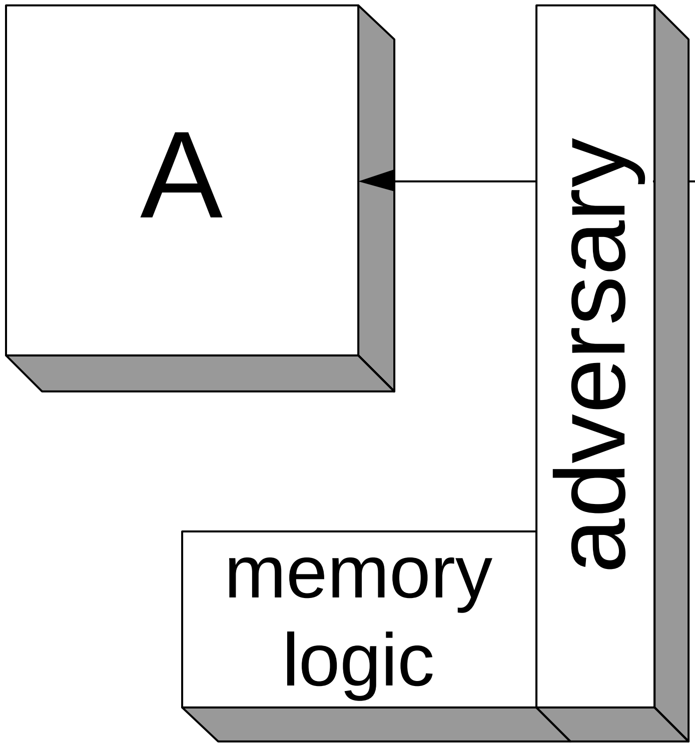
Abstract adversary

Specify set K_A^0 of initial knowledge of an adversary of type *A*.

To test secrecy of *M*∈ Exp$\backslash K_A^0$ against attacker type *A*: Execute *S* with most powerful attacker of type *A* according to threat scenario from deployment diagram.

M kept secret by *S* if *M* never output in clear (Dolev, Yao 1982).

Abstract adversary



* memorize message
* delete message
* insert message
* compose own message
* use cryptographic primitives

Secrecy

p preserves the secrecy of *M2Exp* from adversaries with initial knowledge *K* if exists no adversary A such that P - A outputs *s* in clear.

„Extensional“ definition. Intuitive but cumbersome.

Example: secrecy

Component sending $\{m\}_K :: K \in$ Exp over Internet does not preserve secrecy of m or K against default attackers the Internet. Component sending (only) $\{m\}_K$ does.

Suppose component receives key K encrypted with its public key, sends back $\{m\}_K$. Does not preserve secrecy of m against attackers eavesdropping on and inserting messages on the link, but against attackers unable to insert messages.

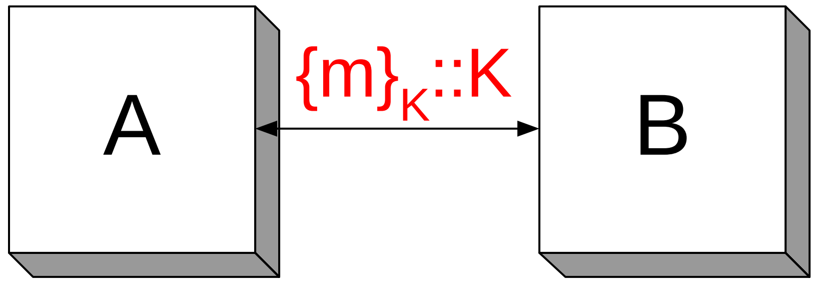
➔

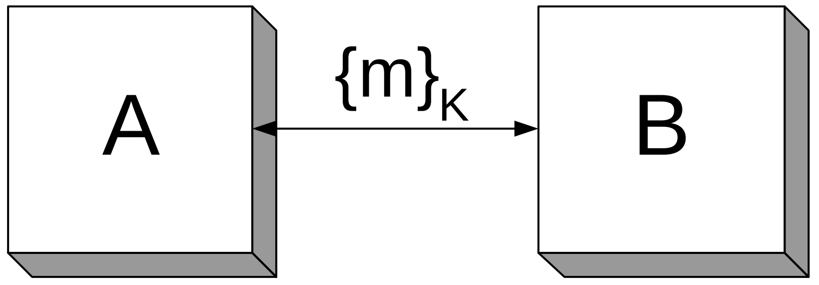
Example: secrecy

$\bar{op}(\{m\}_K :: K)$ does not preserve secrecy of *m* or *K* (against adversaries with arbitrary initial knowledge) but $\bar{op}(\{m\}_K)$ preserves secrecy of *m* against adversaries without *m* or *K* in initial knowledge.

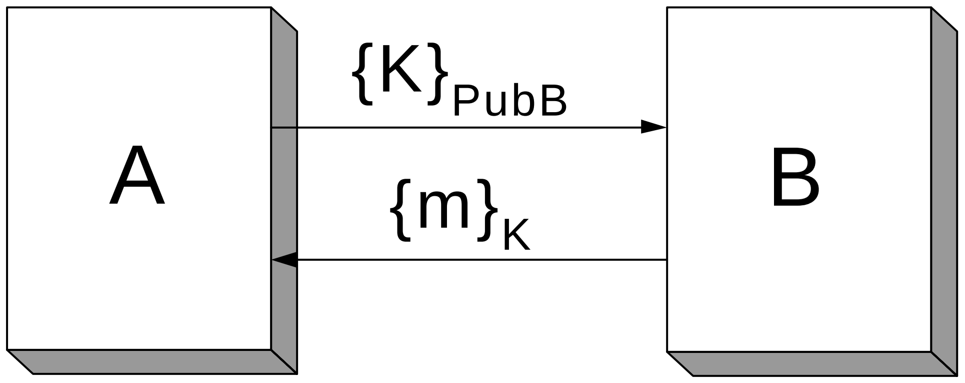
$receive(K).\bar{op}(\{m\}_K)$ does not preserve secrecy of *m* against adversaries with non-empty initial knowledge.

Example: secrecy





Example: secrecy



- Security of *m* is not preserved against an attacker who can delete and insert messages
- Security of *m* is preserved against an attacker who can listen, but not alter the link

Abstract adversary (alternative)

Define: Suppose K_A^{n+1} is the Exp-subalgebra generated by K_A^n and the expressions received after *n+1*st iteration of the protocol.

Theorem.

S keeps secrecy of *M* against attackers of type *A* if there is no *n* with $M \in K_A^n$.

Control Flow Analysis for Security

Idea: approximate set of possible data values flowing through system from above.

Gives secrecy following Dolev-Yao definition.

Cf. eg. Bodei, Degano, 2xNielson 2002.

Here: start by concentrating on possible sets of adversary knowledge.

Next: Adversary knowledge analysis

$$\frac{\mathcal{S}\models\mathcal{K}';p;\mathcal{K}'' \wedge \langle\mathcal{K}\cup\{\mathcal{S}(exp)\}\rangle\subseteq\mathcal{K}'}{\mathcal{S}\models\mathcal{K};\bar{op}(exp).p;\mathcal{K}''}$$

$$\frac{\mathcal{S}\models\mathcal{K};p_i;\mathcal{K}_i \text{ (each } i)}{\mathcal{S}\models\mathcal{K};\sum_i op_i(var).p_i(var);\langle\bigcup_i \mathcal{K}_i\rangle}$$

$$\frac{\mathcal{S}\models\mathcal{K};p_1;\mathcal{K}_1 \quad \mathcal{S}\models\mathcal{K};p_2;\mathcal{K}_1}{\mathcal{S}\models\mathcal{K};\mathbf{if}\ b\ \mathbf{then}\ p_1\mathbf{else}\ p_2;\langle\mathcal{K}_1\cup\mathcal{K}_2\rangle}$$

$$\frac{\mathcal{S}\models\mathcal{K};c_1;\mathcal{K}_1 \quad \mathcal{S}\models\mathcal{K}_1;p_1\|(c_2.p_2);\mathcal{K}'_1}{\mathcal{S}\models\mathcal{K};(c_1.p_1)\|(c_2.p_2);\langle\mathcal{K}'_1\cup\mathcal{K}'_2\rangle}$$

$$\frac{\mathcal{S}\models\mathcal{K}_i;p_i;\mathcal{K}_{i+1} \text{ (each } i)}{\mathcal{S}\models\mathcal{K}_0;\mathbf{iter}_i(p_i);\langle\bigcup_i \mathcal{K}_i\rangle}$$

Approximation

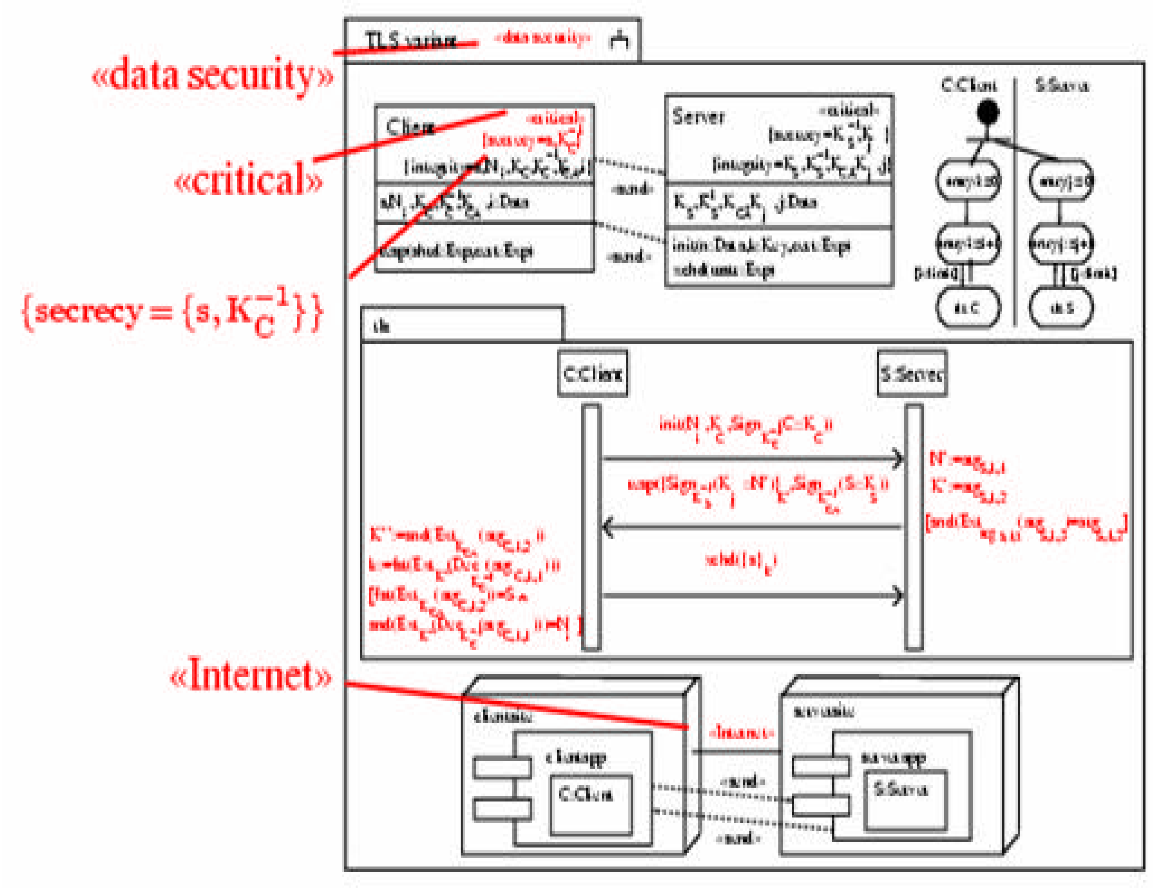
If exists A with initial knowledge K such that P - A outputs *s*

then

exists S such that S ² K;*p*;K‘ with *s*2K‘.

Not conversely (pessimistic approximation).

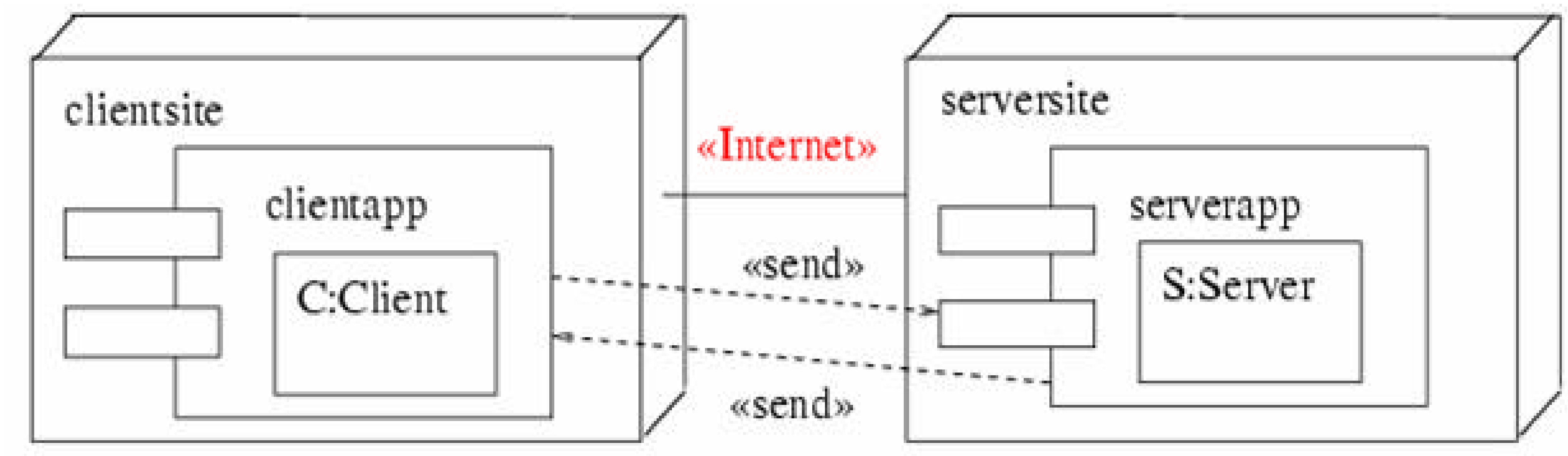
Example: Proposed Variant of TLS (SSL)



Apostolopoulos, Peris, Saha; IEEE Infocom 1999

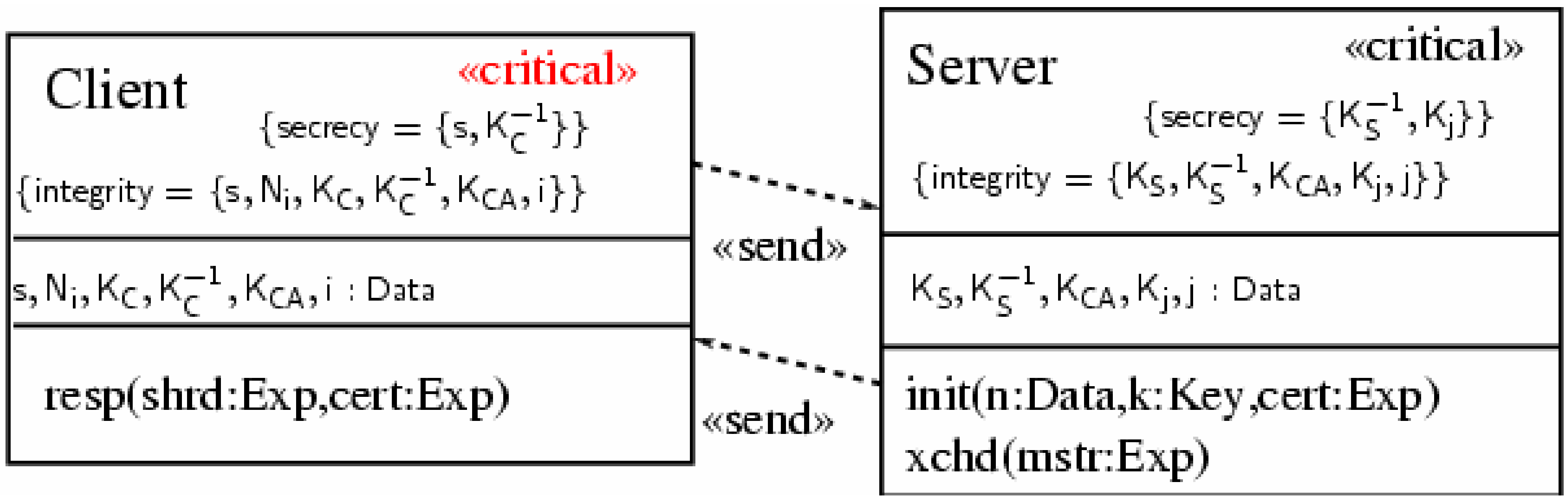
Goal: send secret *s* protected by session key K_j.

TLS Variant: Physical view



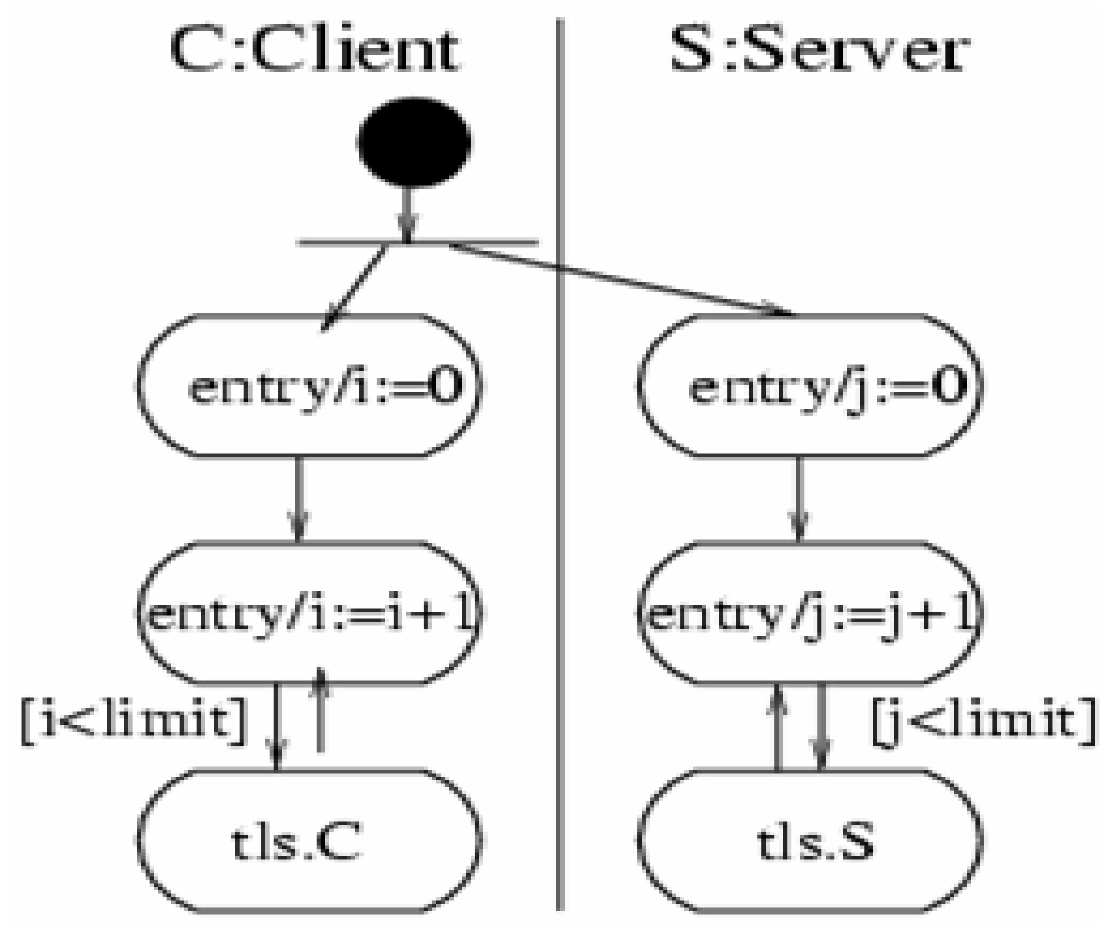
Deployment diagram.

TLS Variant: Structural view


Client
«critical»
$\{secrecy = \{s, K_C^{-1}\}\}$
$\{integrity = \{s, N_i, K_C, K_C^{-1}, K_{CA}, i\}\}$
$s, N_i, K_C, K_C^{-1}, K_{CA}, i$: Data
resp(shrd:Exp,cert:Exp)
«send»
«send»
Server
«critical»
$\{secrecy = \{K_S^{-1}, K_j\}\}$
$\{integrity = \{K_S, K_S^{-1}, K_{CA}, K_j, j\}\}$
$K_S, K_S^{-1}, K_{CA}, K_j, j$: Data
init(n:Data,k:Key,cert:Exp)
xchd(mstr:Exp)

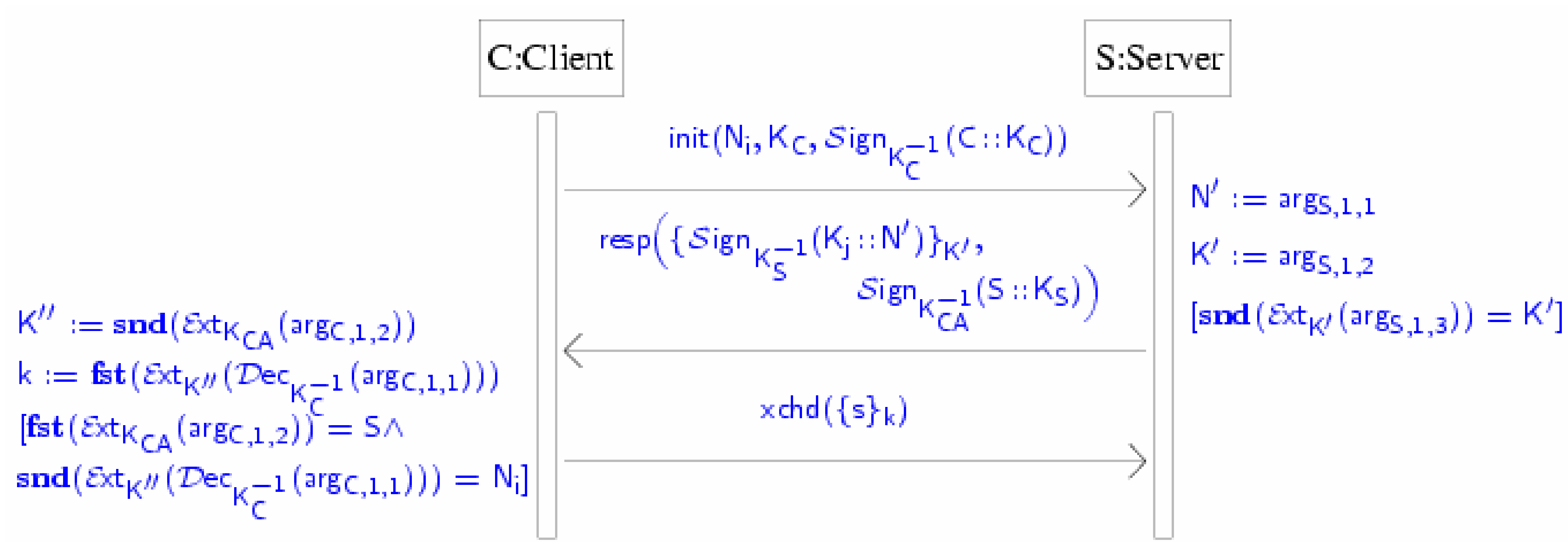
Class diagram

TLS Variant: Coordination view



Activity diagram.

TLS Variant: Interaction view


C:Client
S:Server
$\mathrm{init}(N_i, K_C, \mathcal{S}ign_{K_C^{-1}}(C::K_C))$
$\mathrm{resp}\left(\{\mathcal{S}ign_{K_S^{-1}}(K_j::N')\}_{K'}, \mathcal{S}ign_{K_{CA}^{-1}}(S::K_S)\right)$
$\mathrm{xchd}(\{s\}_k)$
$N' := \mathrm{args}_{S,1,1}$
$K' := \mathrm{args}_{S,1,2}$
$[\mathbf{snd}(\mathcal{E}xt_{K'}(\mathrm{args}_{S,1,3})) = K']$
$K'' := \mathbf{snd}(\mathcal{E}xt_{K_{CA}}(\mathrm{arg}_{C,1,2}))$
$k := \mathbf{fst}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\mathrm{arg}_{C,1,1})))$
$[\mathbf{fst}(\mathcal{E}xt_{K_{CA}}(\mathrm{arg}_{C,1,2})) = S \wedge$
$\mathbf{snd}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\mathrm{arg}_{C,1,1}))) = N_i]$

Sequence diagram.

TLS variant specification

$$
\begin{aligned}
C \quad := \quad & \mathbf{iter}_i(i\bar{n}it(N_i :: K_C :: \mathcal{S}ign_{K_C^{-1}}(C :: K(C))).\\
& resp(m_1 :: m_2).\\
& \mathbf{if}\ \mathbf{fst}(\mathcal{E}xt_{K_{CA}}(m_2)) = S_i \wedge\\
& \mathbf{snd}(\mathcal{E}xt_{\mathbf{snd}(\mathcal{E}xt_{K_{CA}}(m_2))}(\mathcal{D}ec_{K_C^{-1}}(m_1))) = N_i\\
& \mathbf{then}\ xc\bar{h}d(\{s_i\}_{\mathbf{fst}(\mathcal{E}xt_{\mathbf{snd}(\mathcal{E}xt_{K_{CA}}(m_2))}(\mathcal{D}ec_{K_C^{-1}}(m_1)))}))\\
S \quad := \quad & \mathbf{iter}_i(init(N :: K :: M).\\
& \mathbf{if}\ \mathbf{snd}(\mathcal{E}xt_K(M)) = K\\
& \mathbf{then}\ r\bar{e}sp(\{\mathcal{S}ign_{K_S^{-1}}(K_j :: N))\}_K ::\\
& \mathcal{S}ign_{K_{CA}^{-1}}(S :: K(S))).xchd(s))
\end{aligned}
$$

The flaw

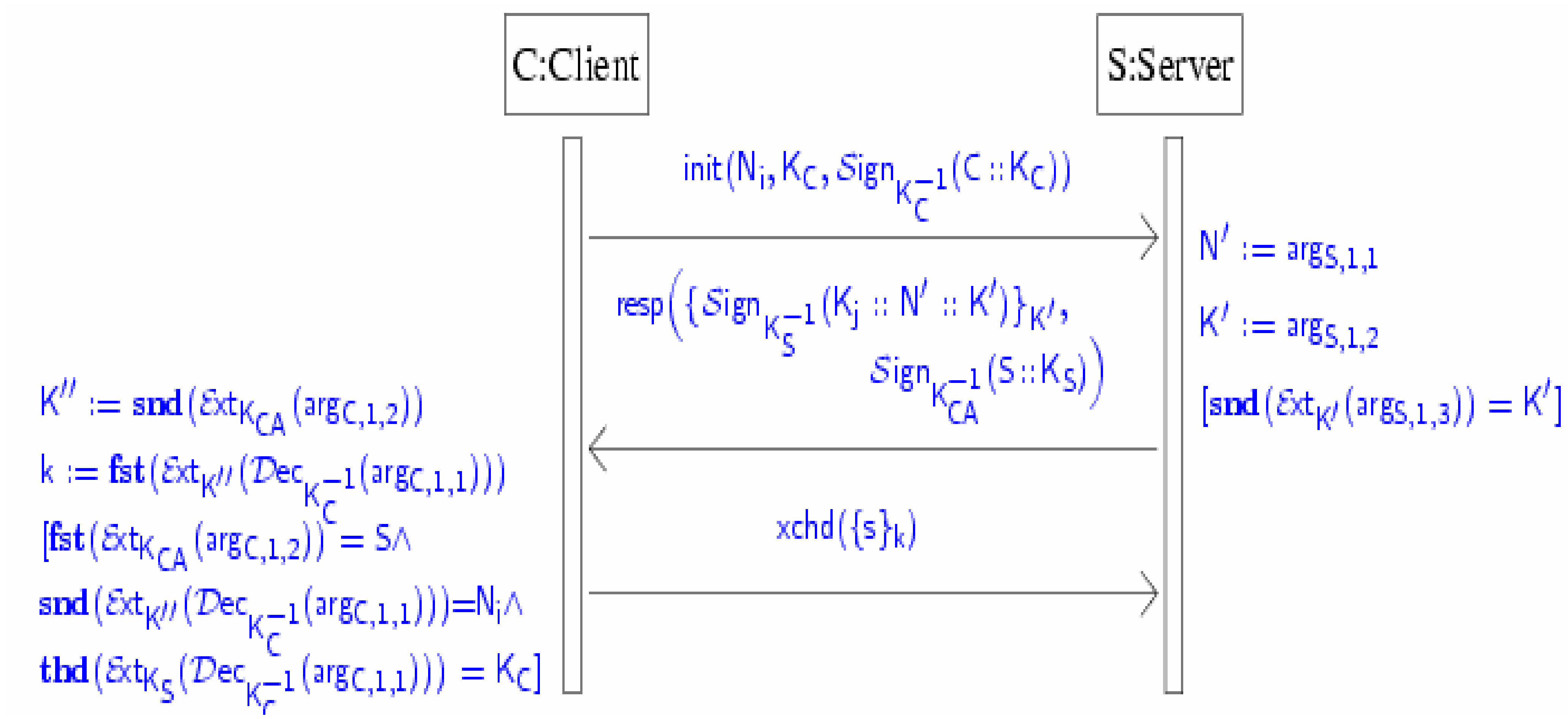
Surprise: $C||S$ does not preserve secrecy of s against adversaries whose initial knowledge contains K_A, K_A^{-1}.

Man-in-the-middle attack.

The attack

$$\begin{tikzcd}
C \arrow[r, "N_i::K_C::Sign_{K_C^{-1}}(C::K_C)"] & A \arrow[r, "N_i::K_A::Sign_{K_A^{-1}}(C::K_A)"] & S \\
 & A & S \arrow[l, "\{Sign_{K_S^{-1}}(K_j::N_i)\}_{K_A}::Sign_{K_{CA}^{-1}}(S::K_S)"'] \\
C & A \arrow[l, "\{Sign_{K_S^{-1}}(K_j::N_i)\}_{K_C}::Sign_{K_{CA}^{-1}}(S::K_S)"'] & \\
C \arrow[r, "\{s\}_{K_j}"] & A \arrow[r, "\{s\}_{K_j}"] & S
\end{tikzcd}$$

The fix


C:Client
S:Server
init$(N_i, K_C, \mathcal{S}ign_{K_C^{-1}}(C :: K_C))$
resp$\left(\{\mathcal{S}ign_{K_S^{-1}}(K_j :: N' :: K')\}_{K'}, \mathcal{S}ign_{K_{CA}^{-1}}(S :: K_S)\right)$
xchd$(\{s\}_k)$
$N' := \text{args}_{S,1,1}$
$K' := \text{args}_{S,1,2}$
$[\mathbf{snd}(\mathcal{E}xt_{K'}(\text{args}_{S,1,3})) = K']$
$K'' := \mathbf{snd}(\mathcal{E}xt_{K_{CA}}(\text{arg}_{C,1,2}))$
$k := \mathbf{fst}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\text{arg}_{C,1,1})))$
$[\mathbf{fst}(\mathcal{E}xt_{K_{CA}}(\text{arg}_{C,1,2})) = S \wedge$
$\mathbf{snd}(\mathcal{E}xt_{K''}(\mathcal{D}ec_{K_C^{-1}}(\text{arg}_{C,1,1}))) = N_i \wedge$
$\mathbf{thd}(\mathcal{E}xt_{K_S}(\mathcal{D}ec_{K_C^{-1}}(\text{arg}_{C,1,1}))) = K_C]$

Modified TLS variant

$$\begin{aligned}
C \;&:=\; \mathbf{iter}_i(\overline{init}(N_i :: K_C :: \mathcal{S}ign_{K_C^{-1}}(C :: K(C))).\\
&\quad resp(m_1 :: m_2).\\
&\quad \mathbf{if}\ \mathbf{fst}(\mathcal{E}xt_{K_{CA}}(m_2)) = S_i \wedge\\
&\quad \mathbf{snd}(\mathcal{E}xt_{\mathbf{snd}(\mathcal{E}xt_{K_{CA}}(m_2))}(\mathcal{D}ec_{K_C^{-1}}(m_1))) = N_i\\
&\quad \wedge\mathbf{thd}(\mathcal{E}\mathbf{xt}_{\mathbf{K_S}}(\mathcal{D}\mathbf{ec}_{\mathbf{K_C^{-1}}}(\mathbf{m_1}))) = \mathbf{K_C}\\
&\quad \mathbf{then}\ \overline{xchd}(\{s_i\}_{\mathbf{fst}(\mathcal{E}xt_{\mathbf{snd}(\mathcal{E}xt_{K_{CA}}(m_2))}(\mathcal{D}ec_{K_C^{-1}}(m_1)))}))\\
S \;&:=\; \mathbf{iter}_i(init(N :: K :: M).\\
&\quad \mathbf{if}\ \mathbf{snd}(\mathcal{E}xt_K(M)) = K\\
&\quad \mathbf{then}\ \overline{resp}(\{\mathcal{S}ign_{K_S^{-1}}(K_j :: N :: \mathbf{K}))\}_K ::\\
&\quad \mathcal{S}ign_{K_{CA}^{-1}}(S :: K(S))).xchd(s))
\end{aligned}$$

Security proof

Theorem. C||S preserves the secrecy of s against adversaries whose initial knowledge K satisfies the following.

$$(\{C.s_I, K_C^{-1}, K_S^{-1}\} \cup \{S.k_j : j \geq J\}$$
$$\cup\{\{\mathcal{S}ign_{K_S^{-1}}(X :: C.N_I :: K_C)\}_{K_C} : X \in \mathbf{Keys}\})$$
$$\cap\mathcal{K} = \emptyset$$

$$\mathcal{S}ign_{K_C^{-1}}(C :: X) \in \mathcal{K} \Rightarrow X = K_C$$

$$\mathcal{S}ign_{K_{CA}^{-1}}(S :: X) \in \mathcal{K} \Rightarrow X = K_S$$

Abstracting from Adversary Knowledge ?

Would like to say

- s protected by K in p
- K protected by K_S^{-1} in p
- K linked to N by K_S^{-1} in p or
- occurrence of K as fresh as N in p, guaranteed by K_S^{-1}
- …

Abstracting from Adversary Knowledge ?

Formalize „*s* protected by *K* in *p*“ as

8 *S*, *K*. (*S* ² *K*;*p*;*K*‘ Æ *s*2*K*‘) *K*2*K*).

Define function *L* to associate data with such formulas.

Get statements *S*,*L* ² *p*.

Give syntactic characterization (e.g. *S*,*L* ² *p* for $p = \overline{op}(\{m\}_K)$ where *L*(*s*) is the above formula) ?

Secure channel abstractions

So far, usually concentrated on specific properties of protocols in isolation.

Need to refine security properties so protocol is still secure in system context. Surprisingly problematic.

Motivates research towards providing secure channel abstractions to use security protocols securely in the system context.

Secure channel: approach

- Define a secure channel abstraction.
- Define concrete secure channel (protocol).
- Show simulates the abstraction.

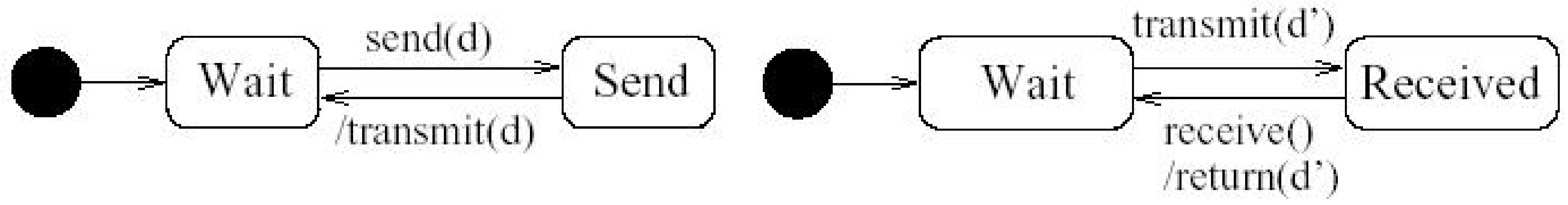
Give conditions under which it is secure to substitute channel abstractions by concrete protocols.

Secure channel abstraction

„Ideal“ of a secure channel:

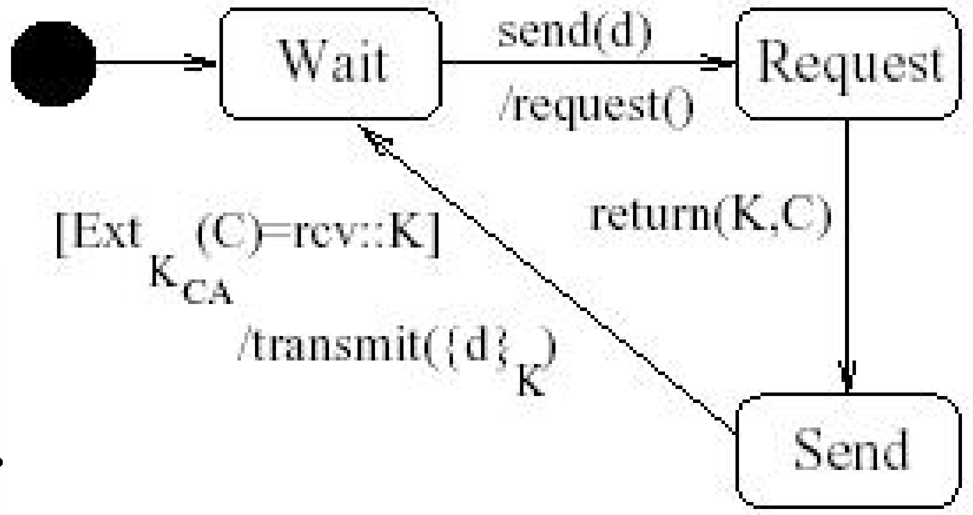
$$\begin{aligned} S &= send(d).\overline{transmit}(s).S \\ R &= transmit(d).\overline{receive}(d).R \end{aligned}$$

Take S - ^{I}R for I$:=\{send,receive\}$ as secure channel abstraction. Trivially secure in absence of adversaries.



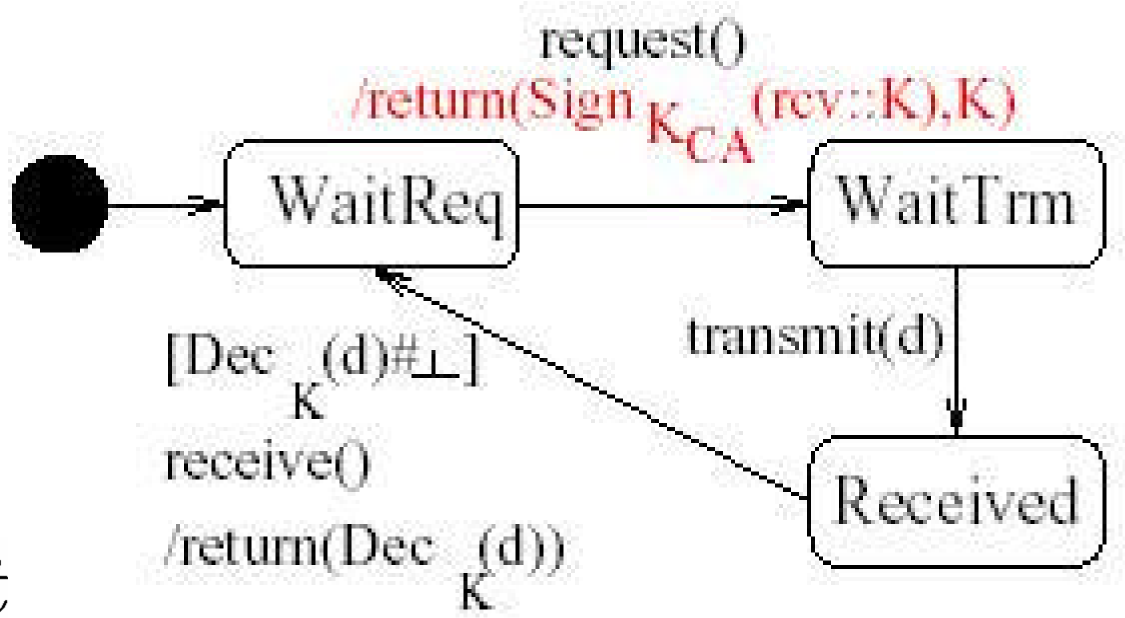
Concrete secure channel

Simple security protocol: encrypt under exchanged session key



$$
\begin{aligned}
S' \;:=\; & \mathbf{iter}_i(send(d).\\
& \overline{request}.return(C).\\
& \mathbf{if\ head}(\mathcal{E}xt_{K_R^{-1}}(\mathcal{D}ec_{K_S^{-1}}(C))) \in\\
& \mathbf{Keys} \wedge \mathbf{tail}(\mathcal{E}xt_{K_R}(\mathcal{D}ec_{K_S^{-1}}(C))) = j\\
& \mathbf{then}\ \overline{transmit}(\{d :: i\}_K)
\end{aligned}
$$

Concrete secure channel II



$$\begin{aligned} R' \;:=\; & \mathbf{iter}_j(\mathit{request} \\ & \overline{\mathit{return}}(\{\mathcal{S}\mathit{ign}_{K_R^{-1}}(K_j :: j)\}_{K_S}. \\ & \mathit{transmit}(E).\mathit{receive}. \\ & \mathbf{if\ tail}(\mathcal{D}\mathit{ec}_{K_j}(E)) = j \\ & \mathbf{then}\ \overline{\mathit{return}}(\mathbf{head}(\mathcal{D}\mathit{ec}_{K_j}(E))) \end{aligned}$$

Bisimulation

A binary relation *R* on processes is a bisimulation iff *(P RQ)* implies that for all actions α,

- if P ! $^{\alpha}$P‘ then exists Q ! $^{\alpha}$Q‘ with *P‘RQ‘* and
- if Q ! $^{\alpha}$Q‘ then exists P ! $^{\alpha}$P‘ with P‘*RQ‘.*

P, Q are bisimilar if there exists a bisimulation *R* with P*R*Q.

Faithful representation ?

Is *(R'||S') - 'A* bisimilar to *S - 'R* ?

No: delay possible. But:

Theorem. Suppose A does not contain the messages *send, receive* nor any value in *{K(S)*$^{-1}$*,K(R)*$^{-1}$*} [{K*$_{n}$*,{x::n}*$_{Kn}$*:x2 ExpÆ n2***N***}* nor *Sign*$_{K(R)}$$^{-1}$*(K'::n)* unless *K'=K*$_{n}$. Then *(R'||S') - 'A* is bisimilar to (*S - 'R*) - A$_{b}$.

Theorem. *(R'||S')* preserves secrecy of *d* against such A.

Roadmap

Rules of prudent security engineering

Saltzer, Schroeder (1975):

Design principles for security-critical systems.

Check how to enforce these with UMLsec.

Economy of mechanism

Keep the design as simple and small as possible.

Often systems made complicated to make them (look) secure.

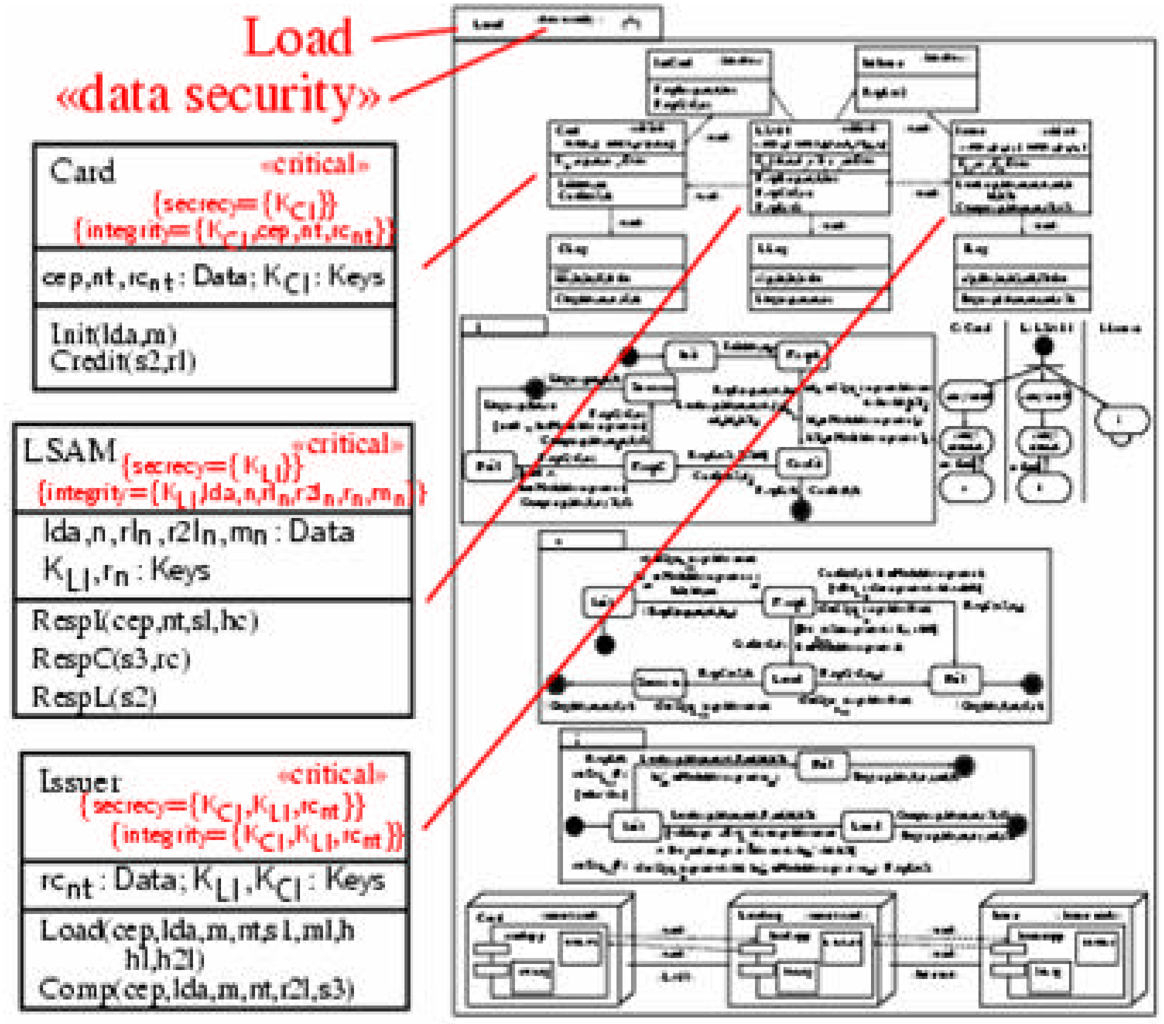
Method for reassurance may reduce this temptation.

Payoffs from formal evaluation may increase incentive for following the rule.

Fail-safe defaults

Base access decisions on permission rather than exclusion.

Example: secure log-keeping for audit control in Common Electronic Purse Specifications (CEPS).

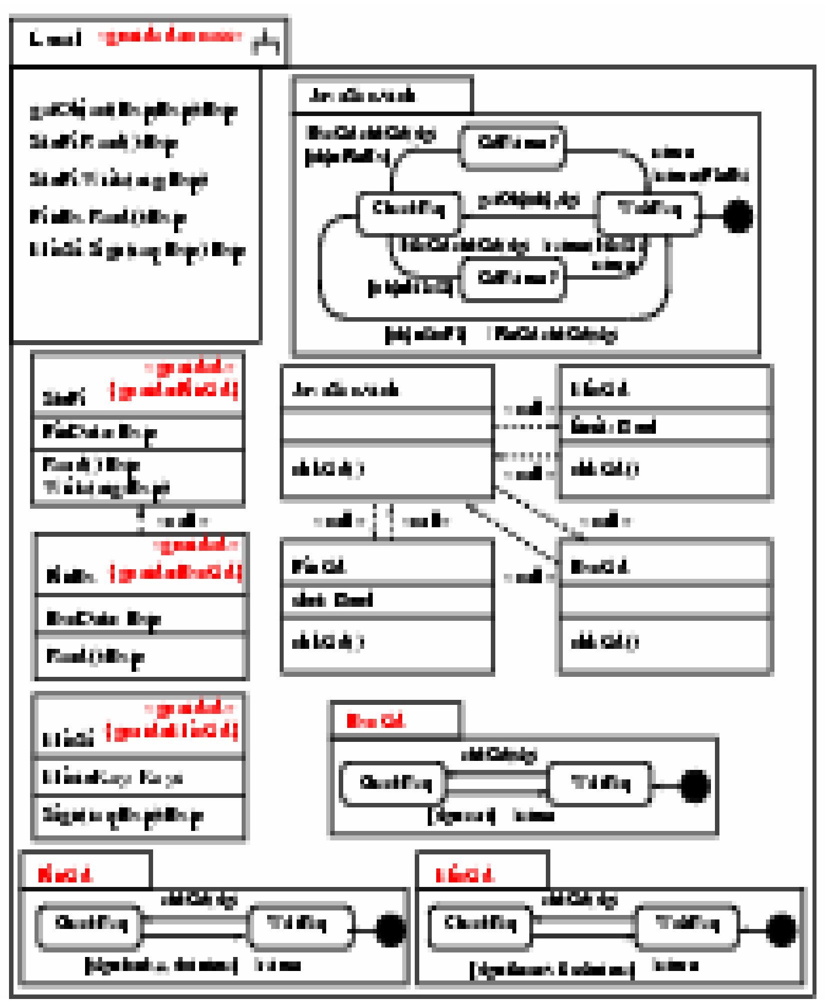

Load
«data security»
Card «critical»
{secrecy={K_CI}}
{integrity={K_CI,cep,nt,rc_nt}}
cep,nt,rc_nt : Data; K_CI : Keys
Init(lda,m)
Credit(s2,rl)
LSAM «critical»
{secrecy={K_LI}}
{integrity={K_LI,lda,n,rl_n,r2l_n,r_n,m_n}}
lda,n,rl_n,r2l_n,m_n : Data
K_LI,r_n : Keys
RespI(cep,nt,sl,hc)
RespC(s3,rc)
RespL(s2)
Issuer «critical»
{secrecy={K_CI,K_LI,rc_nt}}
{integrity={K_CI,K_LI,rc_nt}}
rc_nt : Data; K_LI,K_CI : Keys
Load(cep,lda,m,nt,s1,ml,h hl,h2l)
Comp(cep,lda,m,nt,r2l,s3)

Complete mediation

Every access to every object must be checked for authority.

E.g. in Java: use guarded objects. Use UMLsec to ensure proper use of guards.

More feasibly, mediation wrt. a set of sensitive objects.



Open design

The design should not be secret.

Method of reassurance may help to develop systems whose security does not rely on the secrecy of its design.

Separation of privilege

A protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.

Example: signature of two or more principals required for privilege. Formulate requirements with activity diagrams.

Verify behavioural specifications wrt. them.

Least privilege

Every program and every user of the system should operate using the least set of privileges necessary to complete the job.

Least privilege: every proper diminishing of privileges gives system not satisfying functionality requirements.

Can make precise and check this.

Least common mechanism

Minimize the amount of mechanism common to more than one user and depended on by all users.

Object-orientation:

- data encapsulation
- data sharing well-defined (keep at necessary minimum).

Psychological acceptability

Human interface must be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.

Wrt. development process: ease of use in development of secure systems.

User side: e.g. performance evaluation (acceptability of performance impact of security).

Discussion

No absolute rules, but warnings.

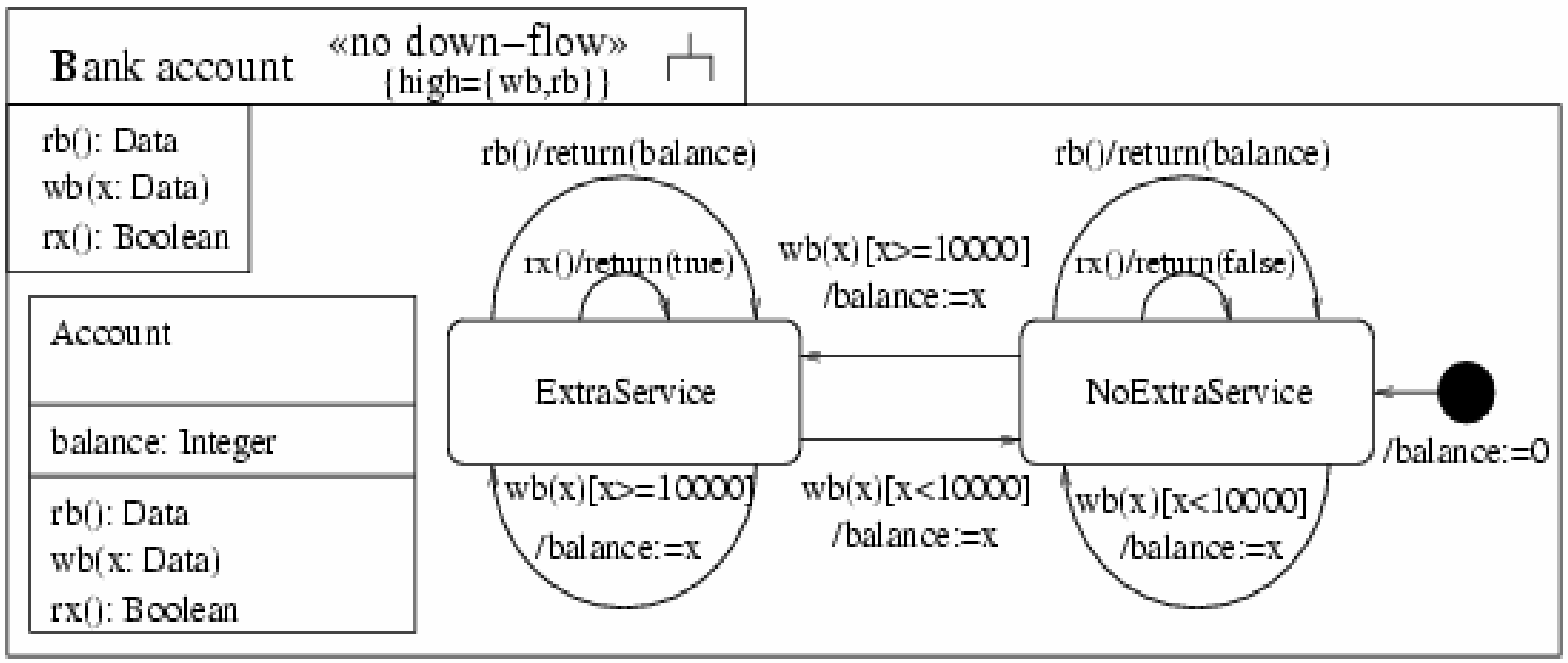
Violation of rules symptom of potential trouble; review design to be sure that trouble accounted for or unimportant.

Design principles reduce number and seriousness of flaws.

Security Patterns

Security patterns: use UML to encapsulate knowledge of prudent security engineering.

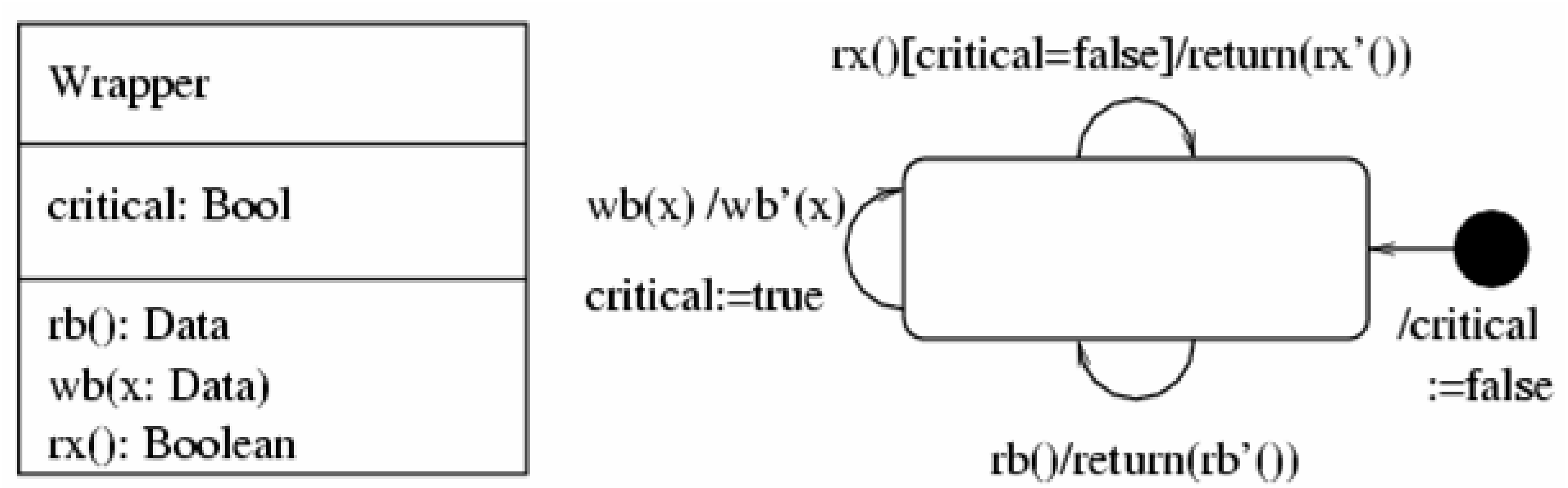
Example:



Does not preserve security of account balance.

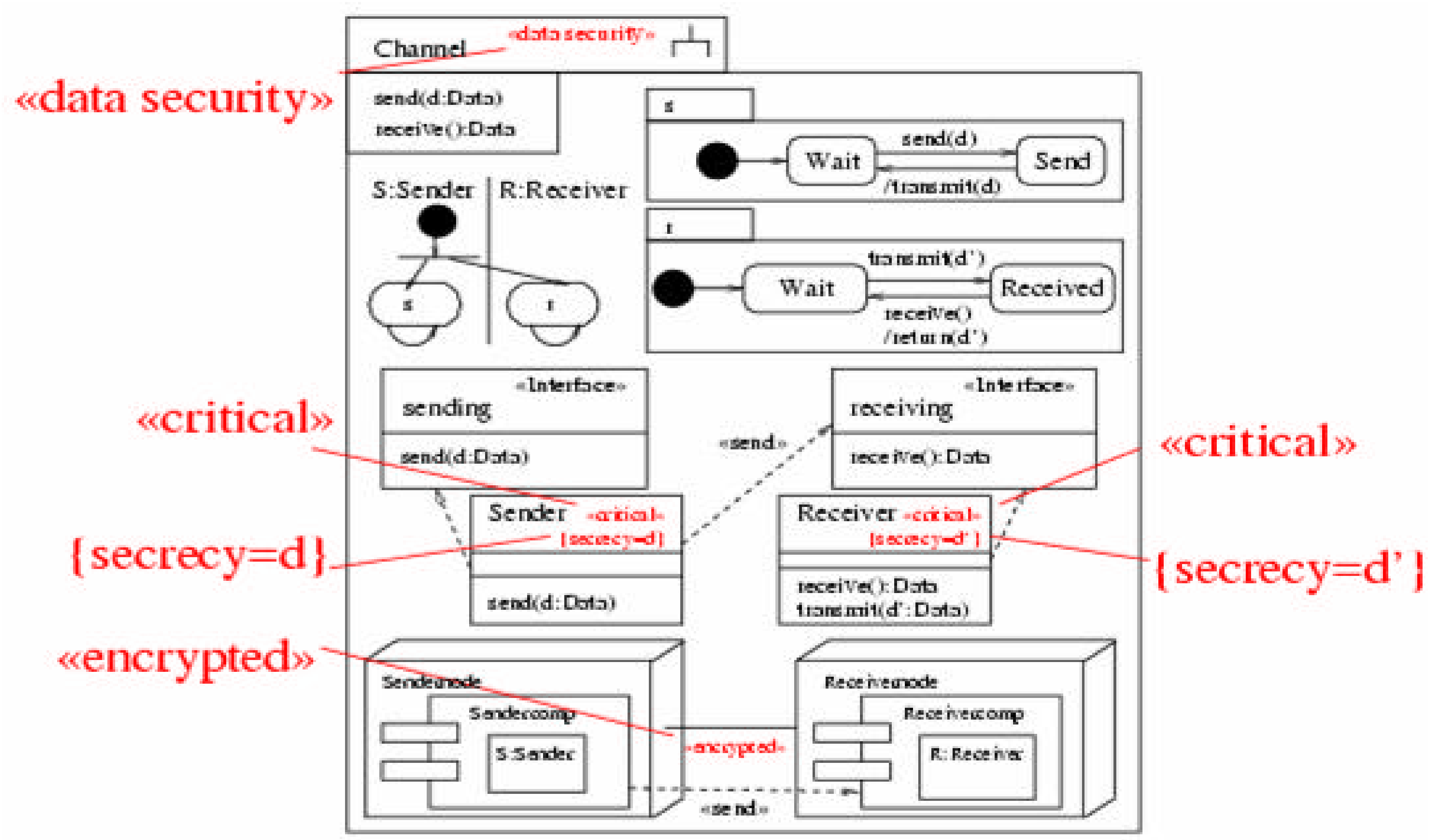
Solution: Wrapper Pattern

Technically, pattern application is transformation of specification.



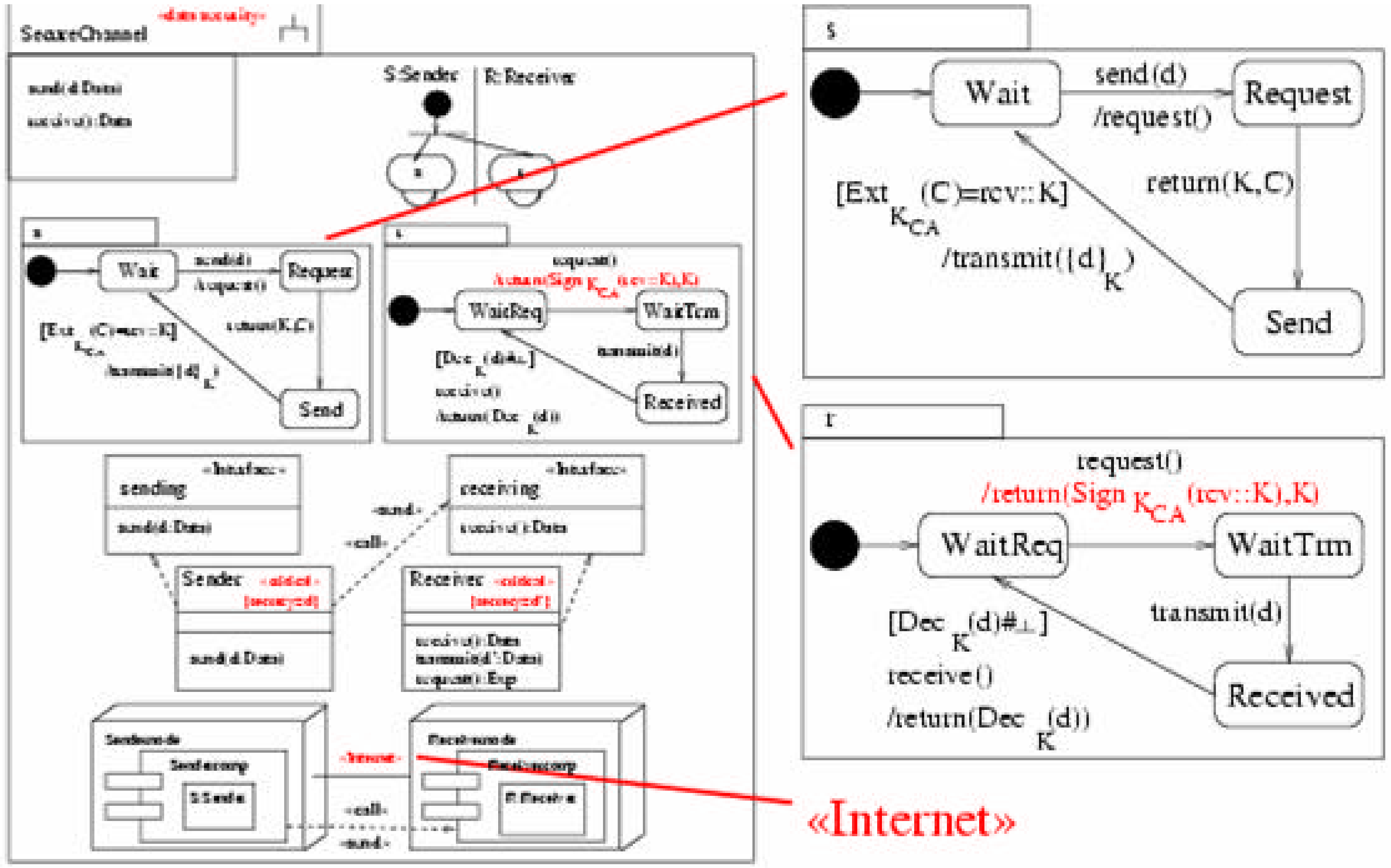
Use wrapper pattern to ensure that no low read after high write.
Can check this is secure (once and for all).

Secure channel pattern: problem



To keep *d* secret, must be sent encrypted.

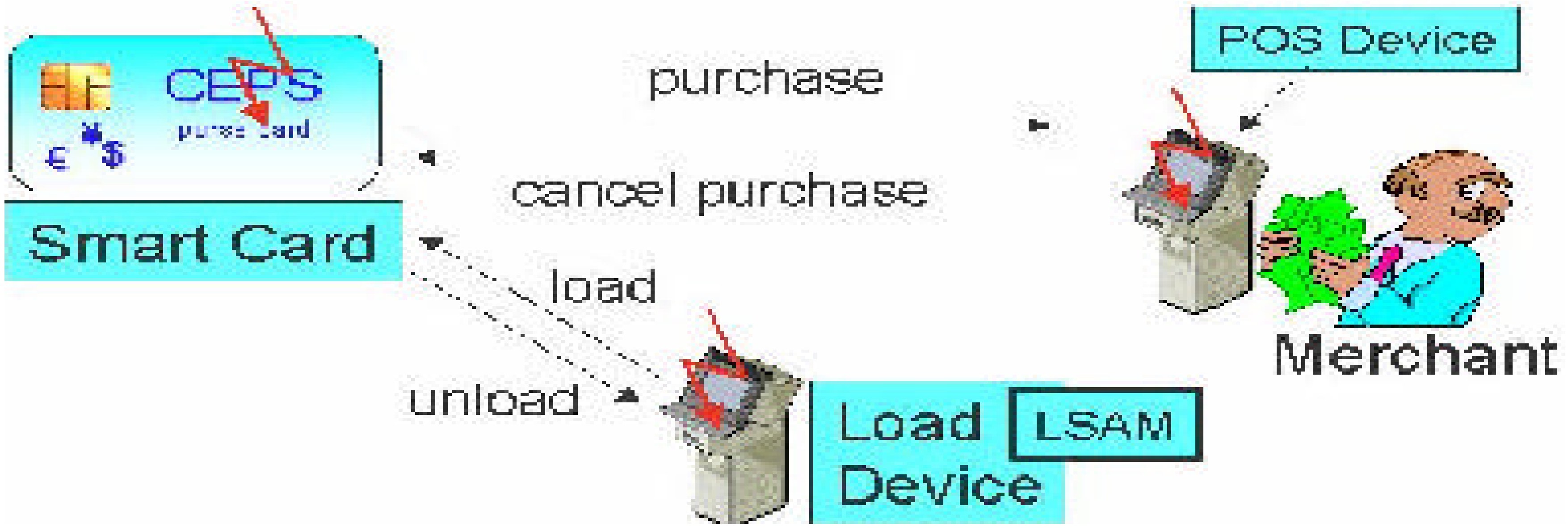
Secure channel pattern: (simple) solution



Exchange certificate and send encrypted data over Internet.

Roadmap

Common Electronic Purse Specifications



Global electronic purse standard (90% of market).

Smart card contains account balance. Chip performs cryptographic operations securing the transactions.

More fraud protection than credit cards (transaction-bound authorisation).

Load protocol

Unlinked, cash-based load transaction (on-line).

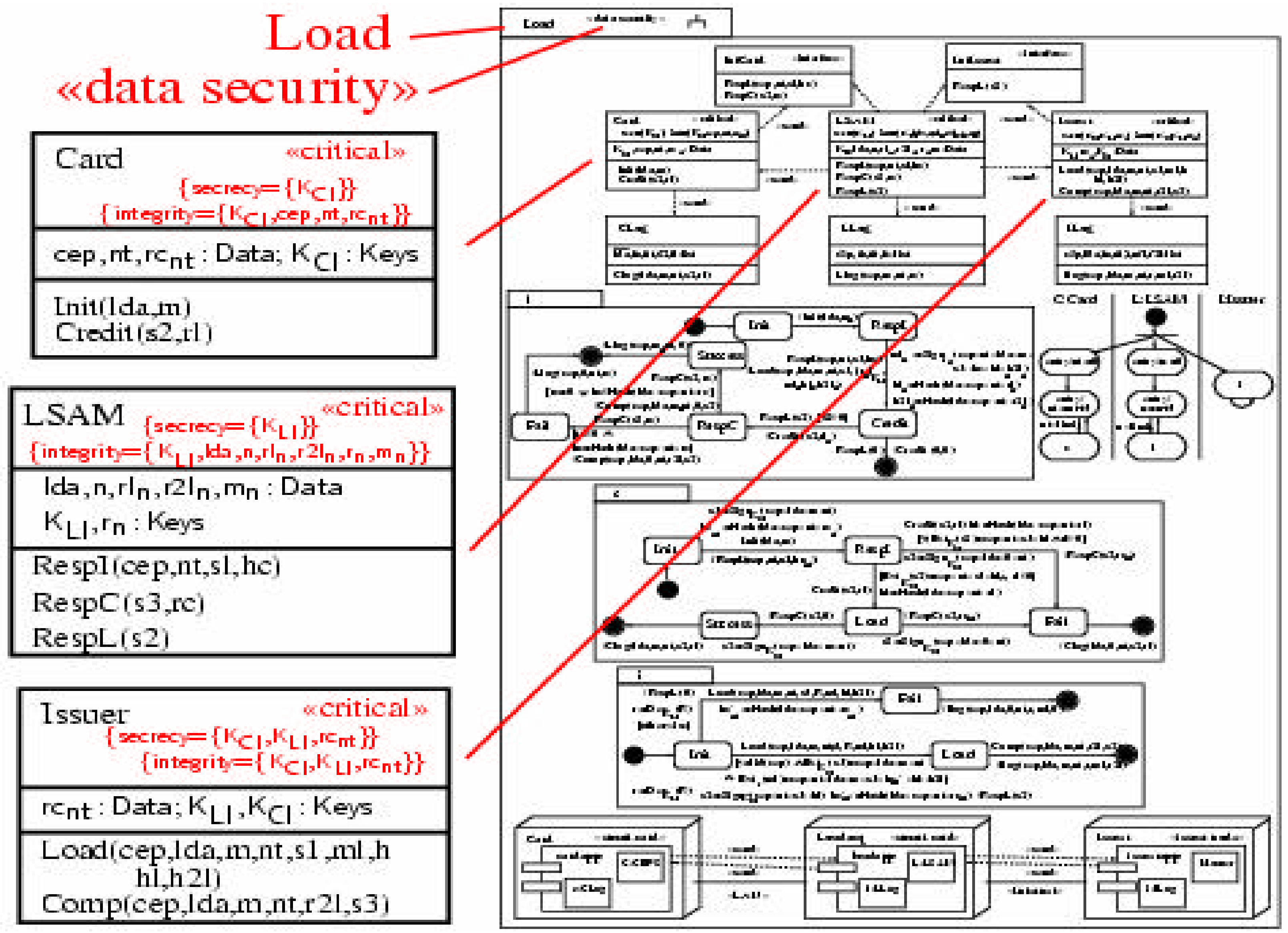
Load value onto card using cash at load device.

Load device contains Load Security Application Module (LSAM): secure data processing and storage.

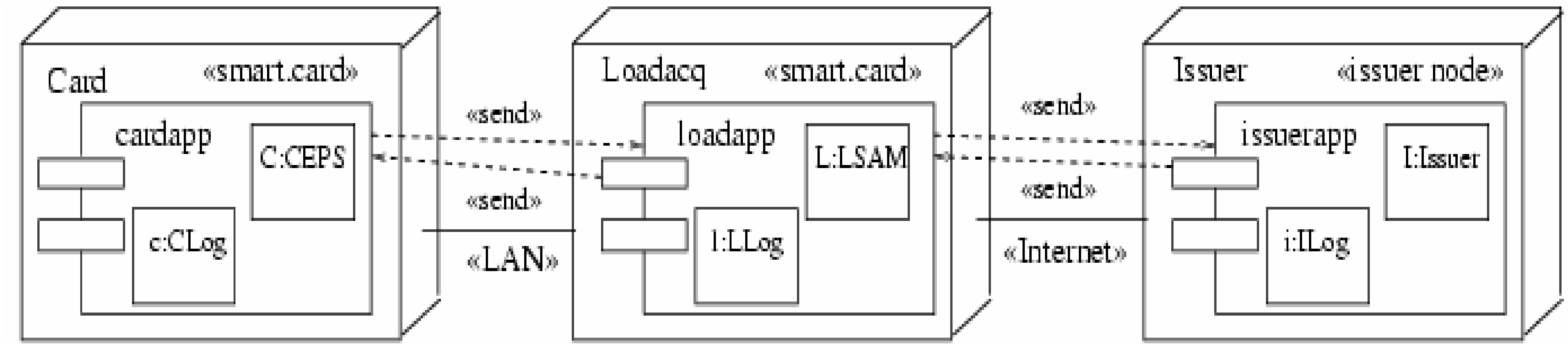
Card account balance adjusted; transaction data logged and sent to issuer for financial settlement.

Uses symmetric cryptography.

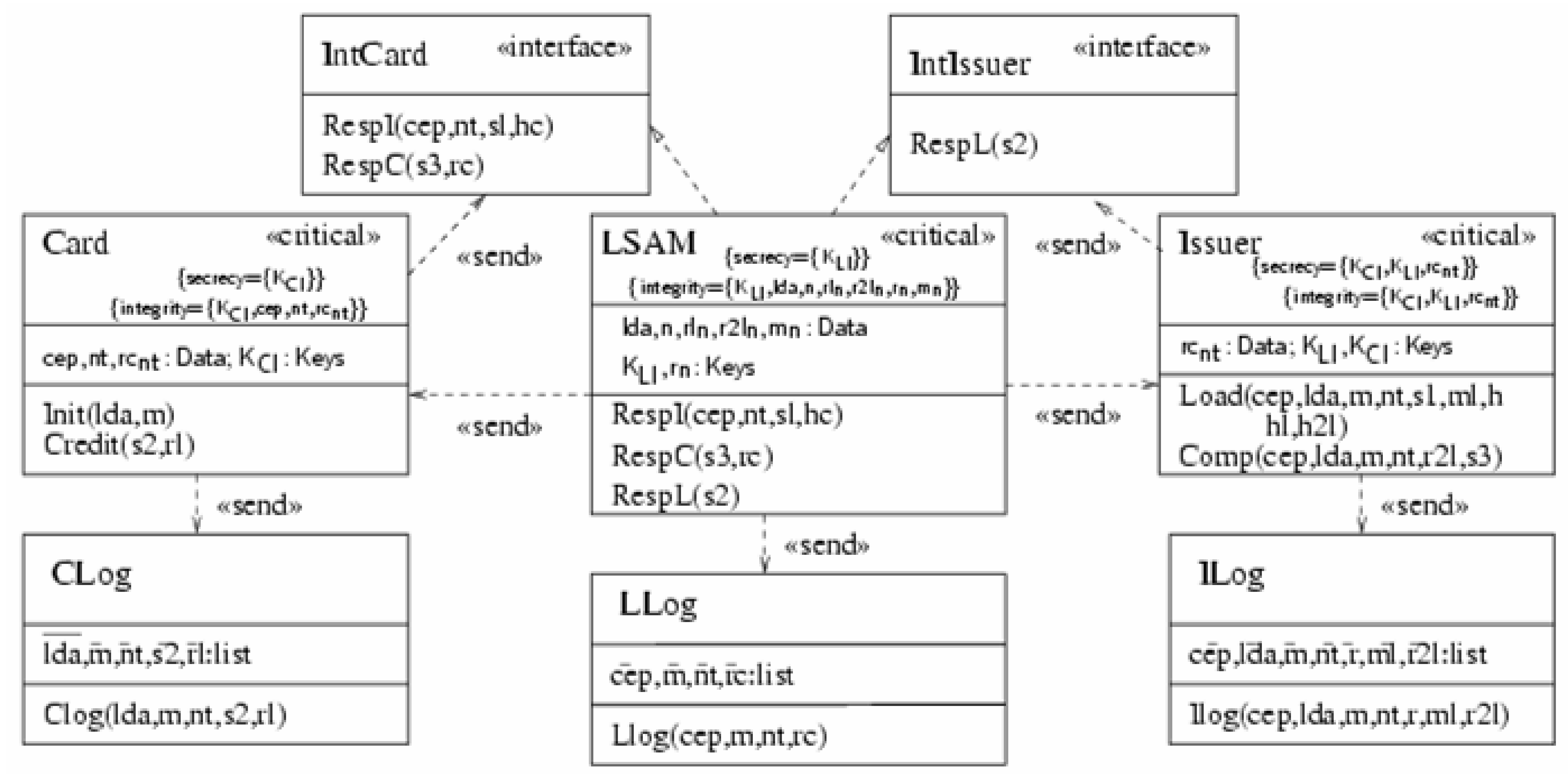
Load protocol


Load
«data security»
Card «critical»
{secrecy={K_{CI}}}
{integrity={K_{CI},cep,nt,rc_{nt}}}
cep,nt,rc_{nt} : Data; K_{CI} : Keys
Init(lda,m)
Credit(s2,rl)
LSAM «critical»
{secrecy={K_{LI}}}
{integrity={K_{LI},lda,n,rl_n,$r2l_n$,r_n,m_n}}
lda,n,rl_n,$r2l_n$,m_n : Data
K_{LI},r_n : Keys
RespI(cep,nt,sl,hc)
RespC(s3,rc)
RespL(s2)
Issuer «critical»
{secrecy={K_{CI},K_{LI},rc_{nt}}}
{integrity={K_{CI},K_{LI},rc_{nt}}}
rc_{nt} : Data; K_{LI},K_{CI} : Keys
Load(cep,lda,m,nt,s1,ml,h
hl,h2l)
Comp(cep,lda,m,nt,r2l,s3)

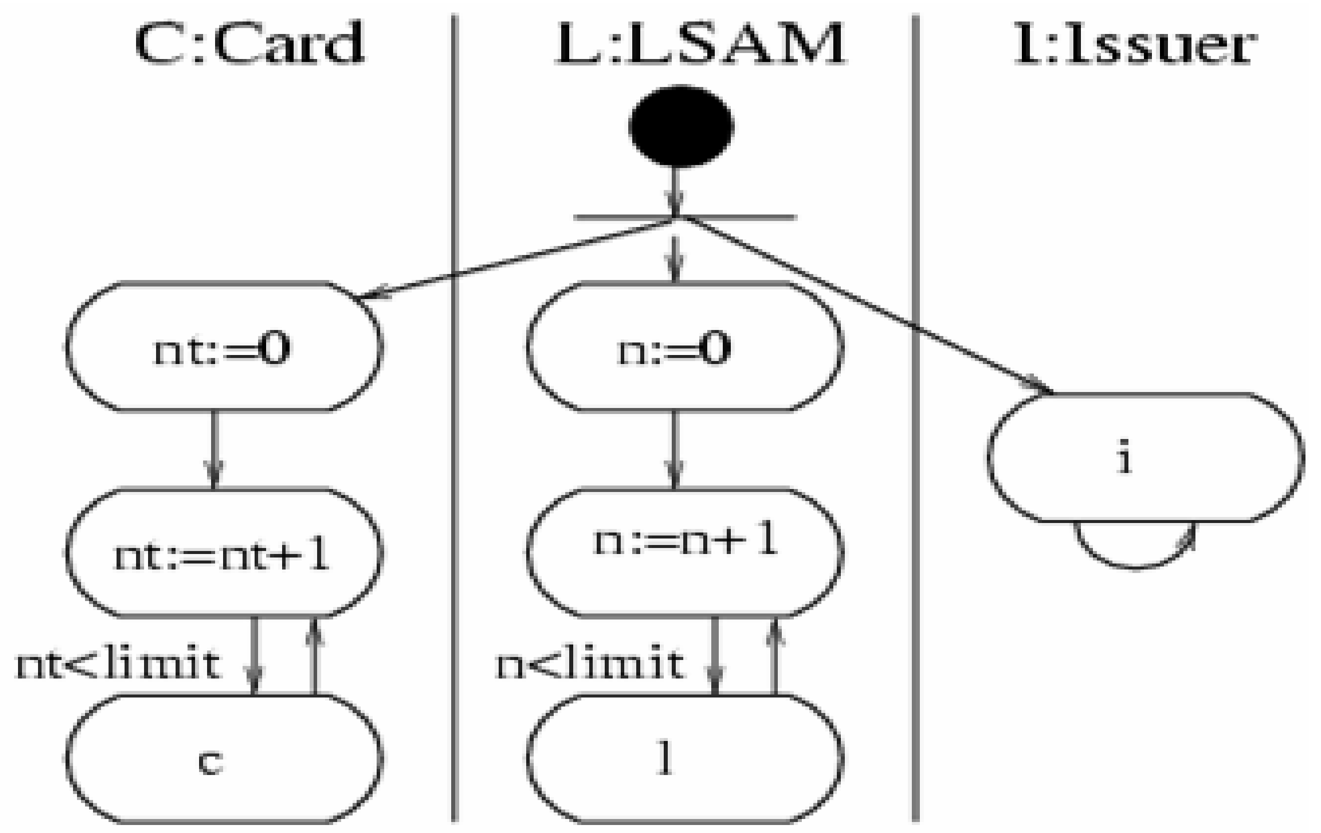
Load protocol: Physical view



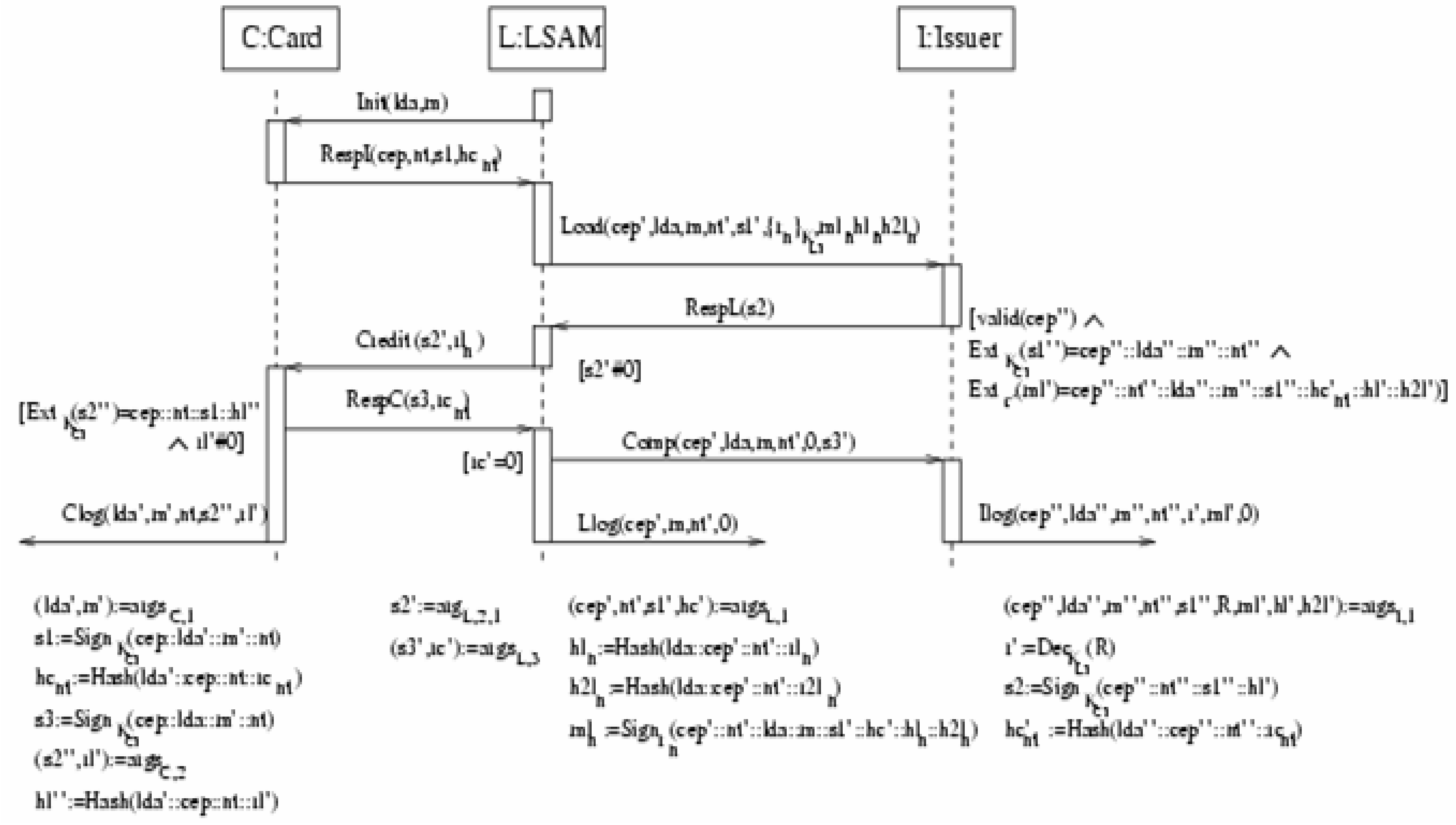
Load protocol: Structural view



Load protocol: Coordination view



Load protocol: Interaction view



C:Card
L:LSAM
I:Issuer
Init(lda,m)
$RespI(cep,nt,s1,hc_{nt})$
$Load(cep',lda,m,nt',s1',\{i_n\}_{K_{L1}},ml_n,hl_n,h2l_n)$
RespL(s2)
$[valid(cep'') \wedge Ext_{K_{C1}}(s1'')=cep''::lda''::m''::nt'' \wedge Ext_c(ml')=cep''::nt''::lda''::m''::s1''::hc'_{nt}::hl'::h2l')]$
$Credit(s2',il_n)$
$[s2'\neq0]$
$RespC(s3,ic_{nt})$
$[Ext_{K_{C1}}(s2'')=cep::nt::s1::hl'' \wedge il'\neq0]$
$Comp(cep',lda,m,nt',0,s3')$
$[ic'=0]$
Clog(lda',m',nt,s2'',il')
Llog(cep',m,nt',0)
Ilog(cep'',lda'',m'',nt'',i',ml',0)
$(lda',m'):=args_{C,1}$
$s1:=Sign_{K_{C1}}(cep::lda'::m'::nt)$
$hc_{nt}:=Hash(lda'::cep::nt::ic_{nt})$
$s3:=Sign_{K_{C1}}(cep::lda::m'::nt)$
$(s2'',il'):=args_{C,2}$
$hl'':=Hash(lda'::cep::nt::il')$
$s2':=arg_{L,2,1}$
$(s3',ic'):=args_{L,3}$
$(cep',nt',s1',hc'):=args_{L,1}$
$hl_n:=Hash(lda::cep'::nt'::il_n)$
$h2l_n:=Hash(lda::cep'::nt'::i2l_n)$
$ml_n:=Sign_{l_n}(cep'::nt'::lda::m::s1'::hc'::hl_n::h2l_n)$
$(cep'',lda'',m'',nt'',s1'',R,ml',hl',h2l'):=args_{I,1}$
$i':=Dec_{K_{L1}}(R)$
$s2:=Sign_{K_{C1}}(cep''::nt''::s1''::hl')$
$hc'_{nt}:=Hash(lda''::cep''::nt''::ic_{nt})$

Security Threat Model

Card, LSAM, issuer security module assumed tamper-resistant.

Intercept communication links, replace components.

Possible attack motivations:

- **Cardholder**: charge without pay
- **Load acquirer**: keep cardholder's money
- **Card issuer**: demand money from load acquirer

May coincide or collude.

Audit security

No direct communication between card and cardholder. Manipulate load device display.

Use post-transaction settlement scheme.

Relies on secure auditing.

Verify this here (only executions completed without exception).

Security conditions (informal)

Cardholder security If card appears to have been loaded with *m* according to its logs, cardholder can prove to card Issuer that a load acquirer owes *m* to card issuer.

Load acquirer security Load acquirer has to pay *m* to card issuer only if load acquirer has received *m* from cardholder.

Card issuer security Sum of balances of cardholder and load acquirer remains unchanged by transaction.

Load acquirer security

Suppose card issuer I possesses $ml_n = Sign_{rn}(cep::nt::lda::m_n::s1::hc_{nt}::hl_n::h2l_n)$ and card C possesses rl_n, where $hl_n = Hash(lda::cep::nt::rl_n)$.

Then after execution either of following hold:

- Llog(cep,lda,m_n,nt) has been sent to I:LLog (so load acquirer L has received and retains m_n in cash) or
- Llog $(cep, lda, 0, nt)$ has been sent to I : LLog (so L returns m_n to cardholder) and L has received rc_{nt} with $hc_{nt}=Hash(lda::cep::nt::rc_{nt})$ (negating ml_n).

"ml_n provides guarantee that load acquirer owes transaction amount to card issuer" (CEPS)

Flaw

Theorem. L does not provide load acquirer security against adversaries of type insider with $K_A^{fd} = \{cep, lda, m_n\}$.

Modification: use asymmetric key in ml_n, include signature certifying hc_{nt}.

Verify this version wrt. above conditions.

Further applications

- Analysis of multi-layer security protocol for web application of major German bank
- Tool for Analysis of SAP access control configuration
- Risk analysis of critical business processes for Basel II / KontraG
- …

Roadmap

Prologue
UML
UMLsafe
Security-critical systems
UMLsec: The profile
Security analysis

Security patterns
UMLsec case studies
Java security, CORBAsec
Tools
Model-based Testing

Java Security

Originally (JDK 1.0): sandbox.

Too simplistic and restrictive.

JDK 1.2/1.3: more fine-grained security control, signing, sealing, guarding objects, . . .)

BUT: complex, thus use is error-prone.

Java Security policies

Permission entries consist of:

- protection domains (i. e. URL's and keys)
- target resource (e.g. files on local machine)
- corresponding permissions (e.g. read, write, execute)

Signed and Sealed Objects

Need to protect integrity of objects used as authentication tokens or transported across JVMs.

A SignedObject contains an object and its signature.

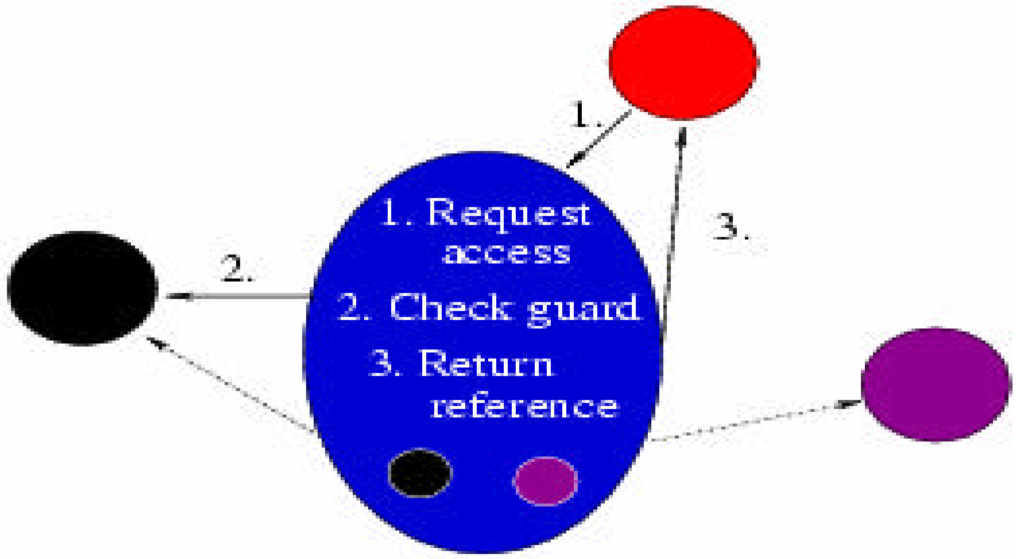
Similarly, need confidentiality.

A SealedObject is an encrypted object.

Guarded Objects

java.security.GuardedObject protects access to other objects.

- access controlled by getObject method
- invokes checkGuard method on the java.security.Guard that is guarding access
- If allowed: return reference. Otherwise: SecurityException



Problem: Complexity

- Granting of permission depends on execution context.
- Access control decisions may rely on multiple threads.
- A thread may involve several protection domains.
- Have method doPrivileged() overriding execution context.
- Guarded objects defer access control to run-time.
- Authentication in presence of adversaries can be subtle.
- Indirect granting of access with capabilities (keys).

→ Difficult to see which objects are granted permission.

⇒ use UMLsec

Design Process

(1) Formulate access control requirements for sensitive objects.

(2) Give guard objects with appropriate access control checks.

(3) Check that guard objects protect objects sufficiently.

(4) Check that access control is consistent with functionality.

(5) Check mobile objects are sufficiently protected.

Reasoning

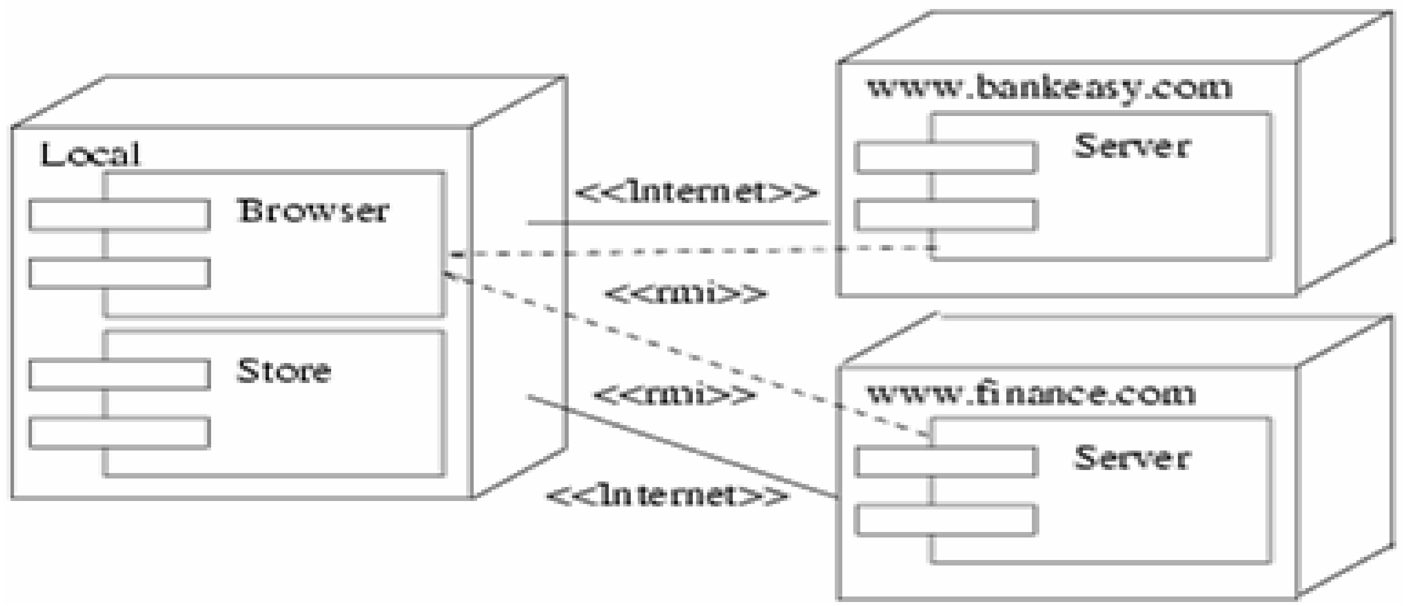
Theorem.

Suppose access to resource according to Guard object specifications granted only to objects signed with *K*.

Suppose all components keep secrecy of *K*.

Then only objects signed with *K* are granted access.

Example: Financial Application



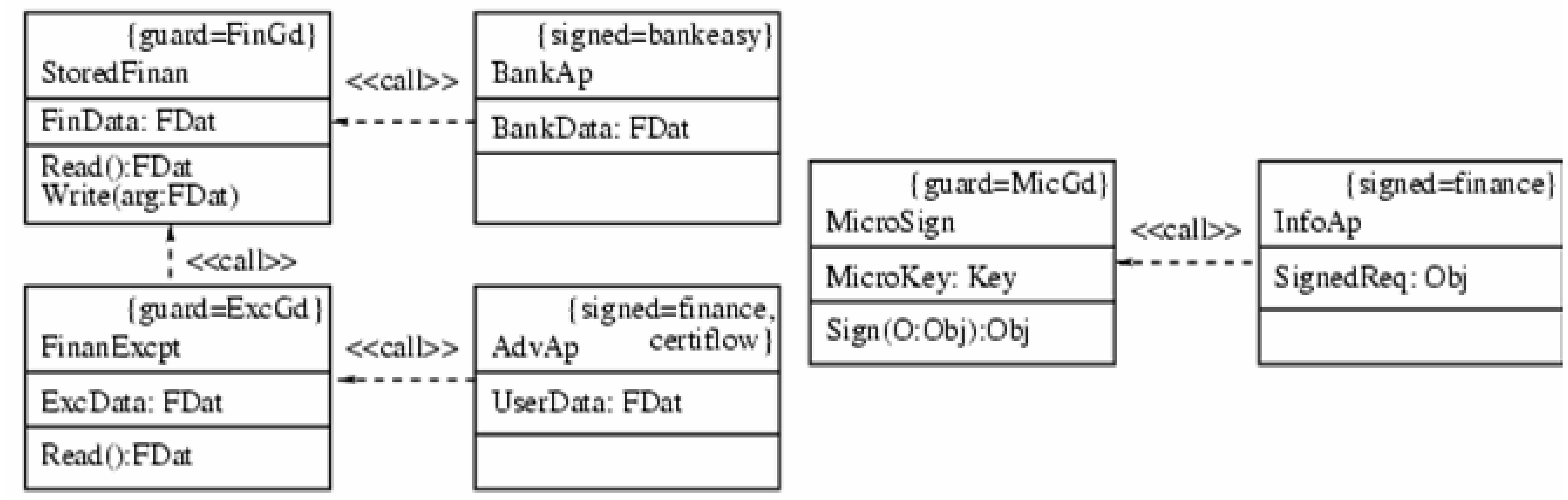
Internet bank, Bankeasy, and financial advisor, Finance, offer services to local user. Applets need certain Privileges (step1).

- Applets from and signed by bank read and write financial data between 1 pm and 2 pm.
- Applets from and signed by Finance use micropayment key five times a week.

Financial Application: Class diagram

Sign and seal objects sent over Internet for Integrity and confidentiality.

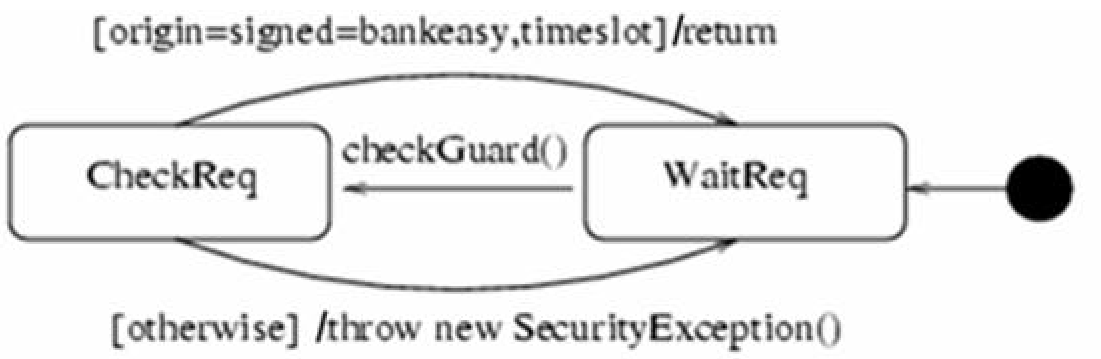
GuardedObjects control access.

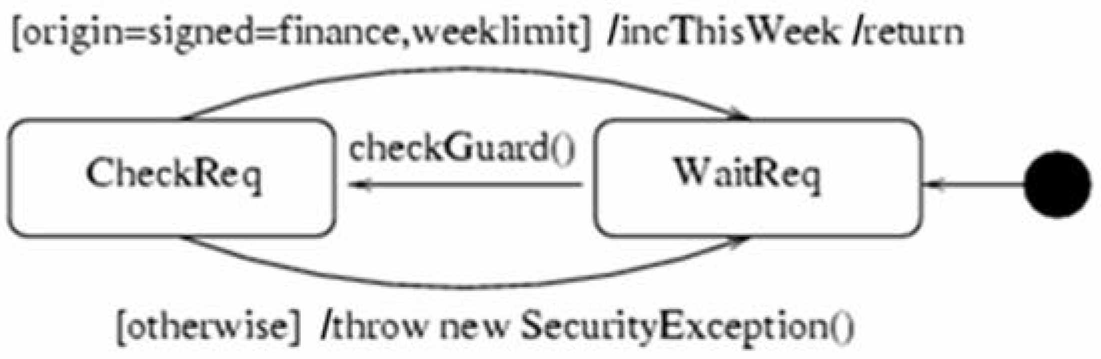


Financial Application: Guard objects (step 2)

timeslot true between 1pm and 2pm.

weeklimit true until access granted five times; inc ThisWeek increments counter.


[origin=signed=bankeasy,timeslot]/return
CheckReq
checkGuard()
WaitReq
[otherwise] /throw new SecurityException()


[origin=signed=finance,weeklimit] /incThisWeek /return
CheckReq
checkGuard()
WaitReq
[otherwise] /throw new SecurityException()

Financial Application: Validation

Guard objects give sufficient protection (step 3).

Proposition. UML specification for guard objects only grants permissions implied by access permission requirements.

Access control consistent with functionality (step 4). Includes:

Proposition. Suppose applet in current execution context originates from and signed by Finance. Use of micropayment key requested (and less than five times before). Then permission granted.

Mobile objects sufficiently protected (step 5), since objects sent over Internet are signed and sealed.

CORBA access control

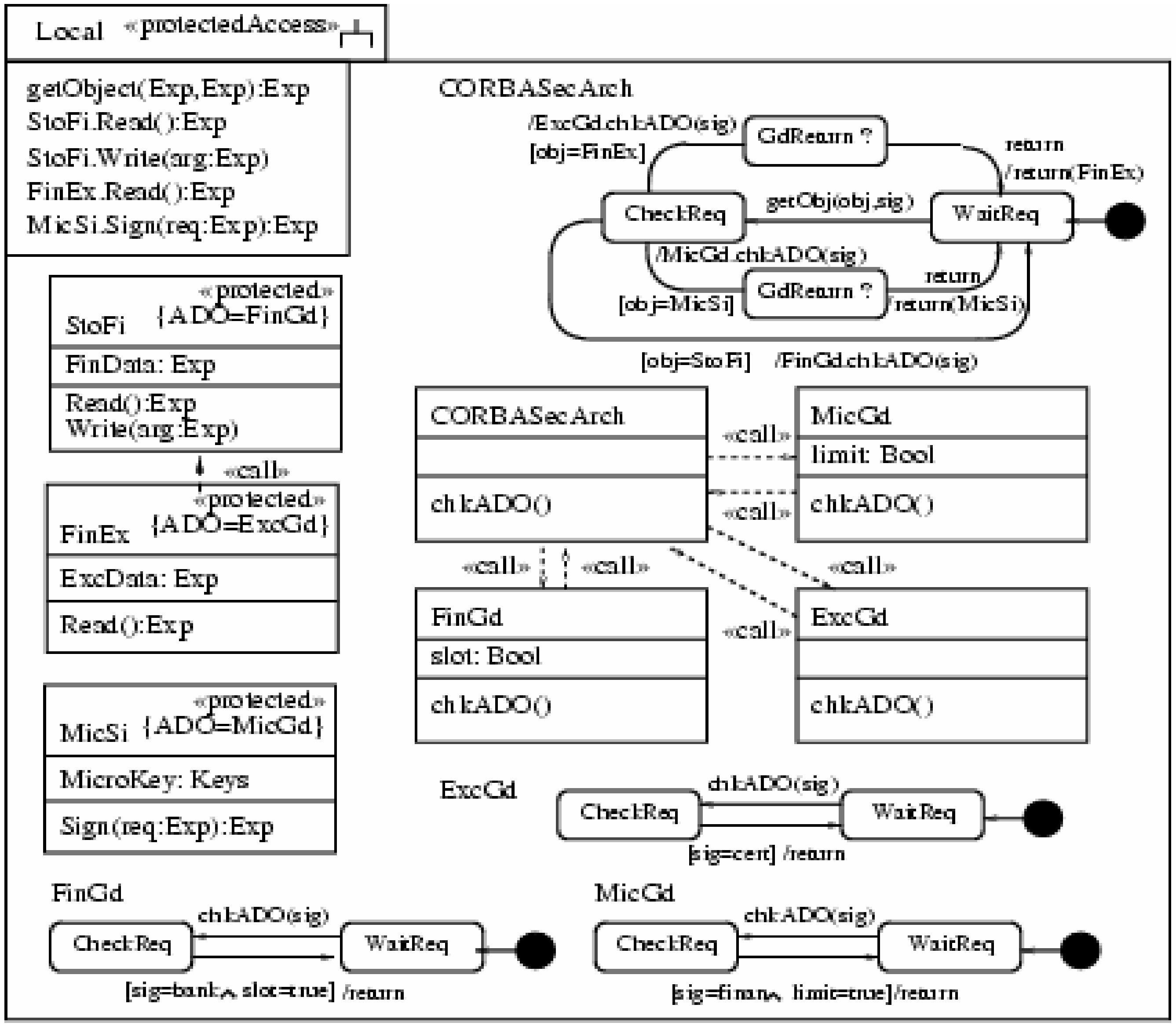
Object invocation access policy controls access of a client to a certain object via a certain method.

Realized by ORB and Security Service.

Use access decision functions to decide whether access permitted. Depends on

- called operation,
- privileges of the principals in whose account the client acts,
- control attributes of the target object.

Example: CORBA access control with UMLsec



Further Applications

- Analysis of multi-layer security protocol for web application of major German bank
- Analysis of SAP access control configurations for major German bank
- Risk analysis of critical business processes (for Basel II / KontraG)
- ...

Roadmap

Tool-support: Concepts

Meaning of diagrams stated informally in (OMG 2003).

Ambiguities problem for

- tool support
- establishing behavioral properties (safety, security)

Need precise semantics for used part of UML, especially to ensure security requirements.

Formal semantics for UML: How

Diagrams in context (using subsystems).

Model actions and internal activities explicitly.

Message exchange between objects or components (incl. event dispatching).

For UMLsec/safe: include adversary/failure model arising from threat scenario in deployment diagram.

Use Abstract State Machines (pseudo-code).

Tool-supported analysis

Choose drawing tool for UML specifications

Analyze specifications via XMI (XML Metadata Interchange)

skip compar.

UML Drawing Tools

Wide range of existing tools.

Consider some, selected under following criteria (Shabalin 2002):

- Support for all (UMLsec/safe-) relevant diagram types.
- Support for custom UML extensions.
- Availability (test version, etc).
- Prevalence on the market.

Selected Tools

- Rational Rose. Developed by major participant in development of UML; market leader.
- Visio for Enterprise Architect. Part of Microsoft Developer Studio .NET.
- Together. Often referenced as one of the best UML tools.
- ArgoUML. Open Source Project, therefore interesting for academic community. Commercial variant Poseidon.

Comparison

Evaluated features:

Support for custom UML extensions.

- Model export; standards support; tool interoperability.
- Ability to enforce model rules, detect errors, etc.
- User interface quality.
- Possibility to use the tool for free for academic institutions.

Rational Rose (Rational Software Corporation)

One of the oldest on the market.

+ Free academic license.

+ Widely used in the industry.

+ Export to different XMI versions.

- Insufficient support for UML extensions (custom stereotypes yes; tags and constraints no).

- Limited support for checking syntactic correctness.

- Very inconvenient user interface. Bad layout control.

- Lack of compatibility between versions and with other Rational products for UML modelling.

Together from TogetherSoft

Widely used in the development community. Very good round-trip engineering between the UML model and the code.

+ Free academic license.

+ Written in Java, therefore platform-independent.

+ Nice, intuitive user interface.

+ Export to different XMI versions; recommendations which for which tool.

- Insufficient support for UML extensions (custom stereotypes yes; tags and constraints no).

Visio from Microsoft Corporation

Has recently been extended with UML editing support

+ Good user interface

+ Full support for UML extensions

+ Very good correspondence to UML standard. Checks dynamically for syntactic correctness; suggestions for fixing errors

- No free academic license

- Proprietary, undocumented file format; very limited XMI export

- No round-trip engineering support. No way back after code generation

Choice: ArgoUML / Poseidon

ArgoUML: Open Source Project. Commercial extension Poseidon (Gentleware), same internal data format

+ Open Source
+ Written in Java, therefore platform-independent
+ XMI default model format
+ Poseidon: solid mature product with good UML specification support

Tool-supported analysis

Commercial modelling tools: so far mainly syntactic checks and code-generation.

Goal: more sophisticated analysis; connection to verification tools.

Several possibilities:

- General purpose language with integrated XML parser (Perl, ...)
- Special purpose XML parsing language (XSLT, ...)
- Data Binding (Castor; XMI: e.g. MDR)

Data-binding with MDR

MDR: MetaData Repository,
Netbeans library (www.netbeans.org)

Extracts data from XMI file into Java Objects, following UML 1.4 meta-model.

Access data via methods.

Advantage: No need to worry about XML.

MDR Standards

- MOF (Meta Object Facility)

  Abstract format for describing metamodels
- XMI (XML Metadata Interchange)

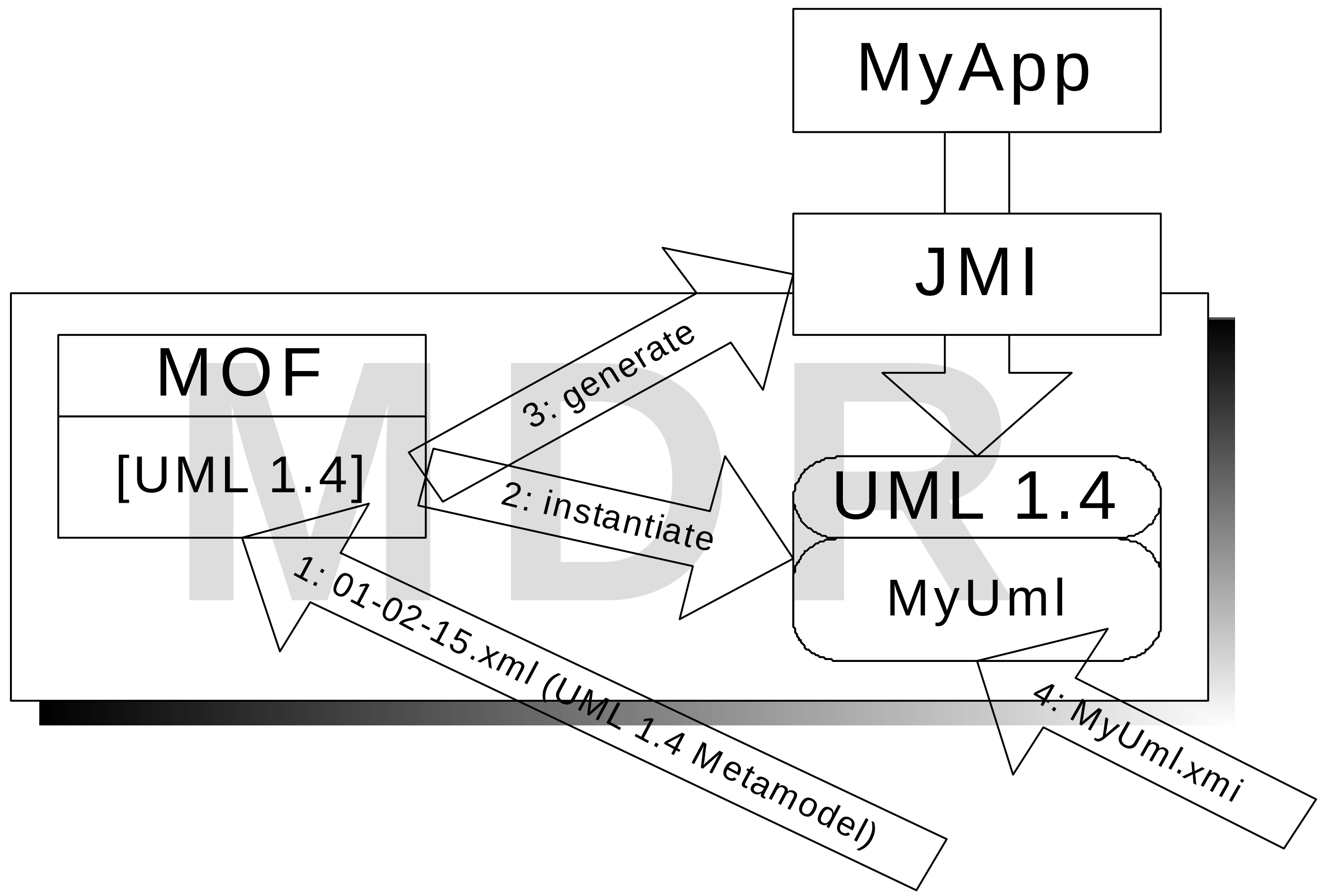
  Defines XML format for a MOF metamodel
- JMI (Java Metadata Interface)

  Defines mapping from MOF to Java

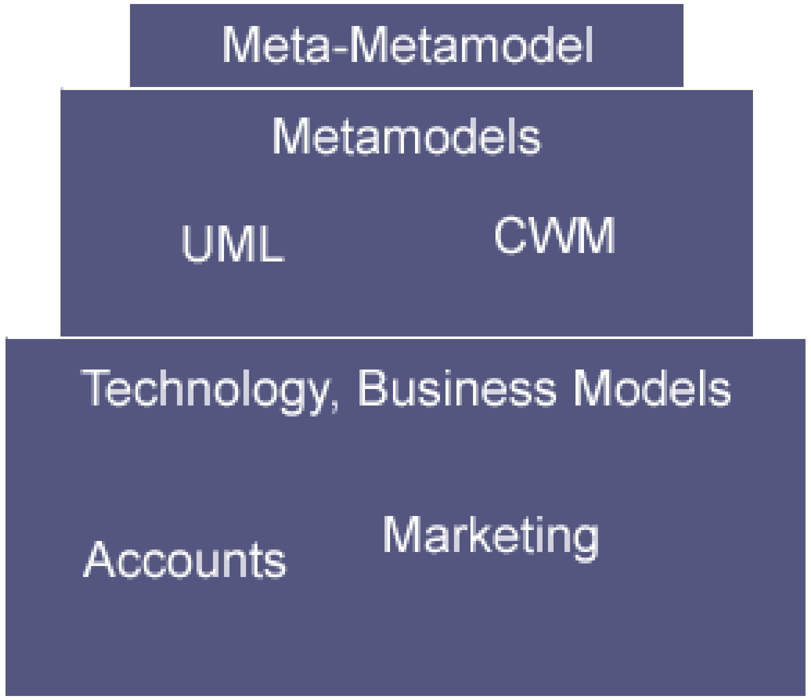
MDR Services

- Load and Store a MOF Metamodel
  (XMI format)
- Instantiate and Populate a Metamodel
  (XMI format)
- Generate a JMI (Java Metadata Interface) Definition for a Metamodel
- Access a Metamodel Instance

UML Processing



MOF Architecture



- Meta-Metamodel (M3)
  - defined by OMG
- Metamodels (M2)
  - user-defined
  - e.g. UML 1.5, MOF, CWM
  - can be created with uml2mof
- Business Model (M1)
  - instances of Metamodels
  - e.g. UML class diagram
- Information (M0)
  - instance of model
  - e.g. implementation of UML modelled classes in Java

MOF (Meta Object Facility)

skip details

OMG Standard for Metamodeling

Meta-Metamodel	MetaClass, MetaAssociation - MOF Model
Metamodel	Class, Attribute, Dependency - UML (as language), CWM
Model	Person, House, City - UML model
Data	(Bob Marley, 1975) (Bonn) - Running Program

JMI: MOF Interfaces

- IDL mapping for manipulating Metadata
  - API for manipulating information contained in an instance of a Metamodel
  - MOF is MOF compliant!
  - Metamodels can be manipulated by this IDL mapping
  - JMI is MOF to Java mapping
  - JMI has same functionality
- Reflective APIs
  - manipulation of complex information
  - can be used without generating the IDL mapping
  - MDR has implemented these interfaces

MDR Repository: Loading Models

- Metamodel is instance of another Metamodel
- Loading Model = Loading Metamodel
- Needed Objects:
  - MDRepository
  - MofPackage
  - XMISaxReaderImpl

- Java Code-Snippet:

```
MDRepository rep;
UmlPackage uml;
// Objekte erzeugen:
rep =

    MDRManager.getDefault().getDefaultRepository()
    ;
reader =
  (XMISaxReaderImpl)Lookup.getDefault().lookup(
            XmiReader.class);

// loading extent:
uml = (UmlPackage)rep.getExtent(„name“);

// creating Extent:
uml = (UmlPackage)rep.createExtent(„name“);

// loading XMI:
reader.read(„url“, MofPackage);,
```

MDR Repository: Reading Data

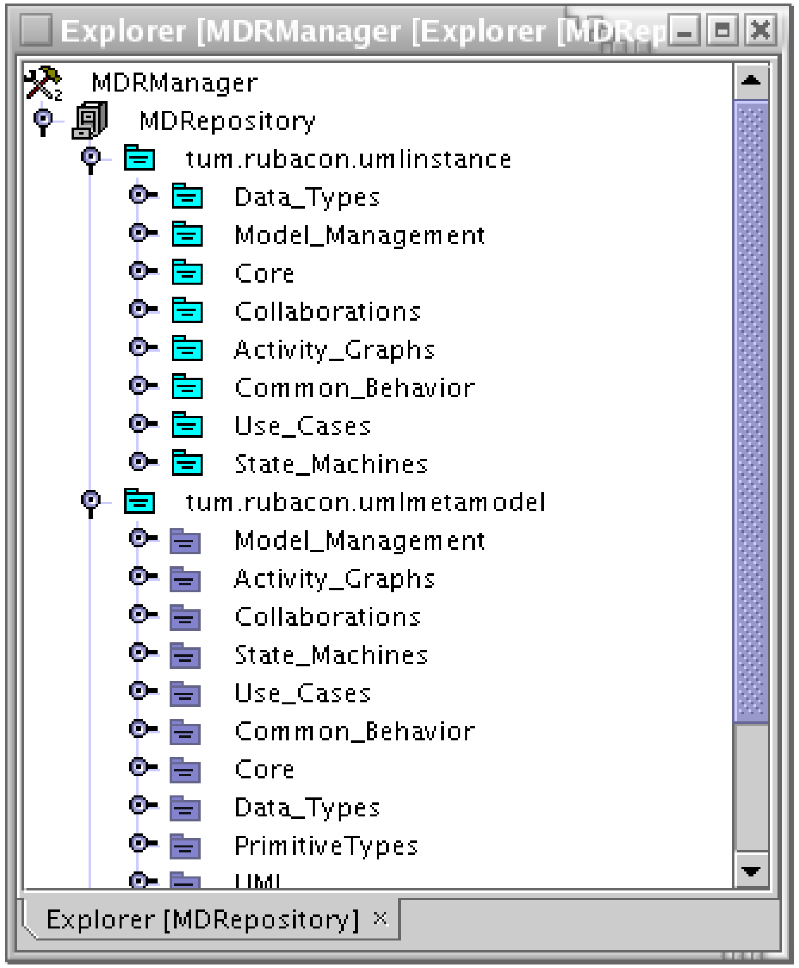
- Requires open Repository and Package
- Requires JMI Interfaces

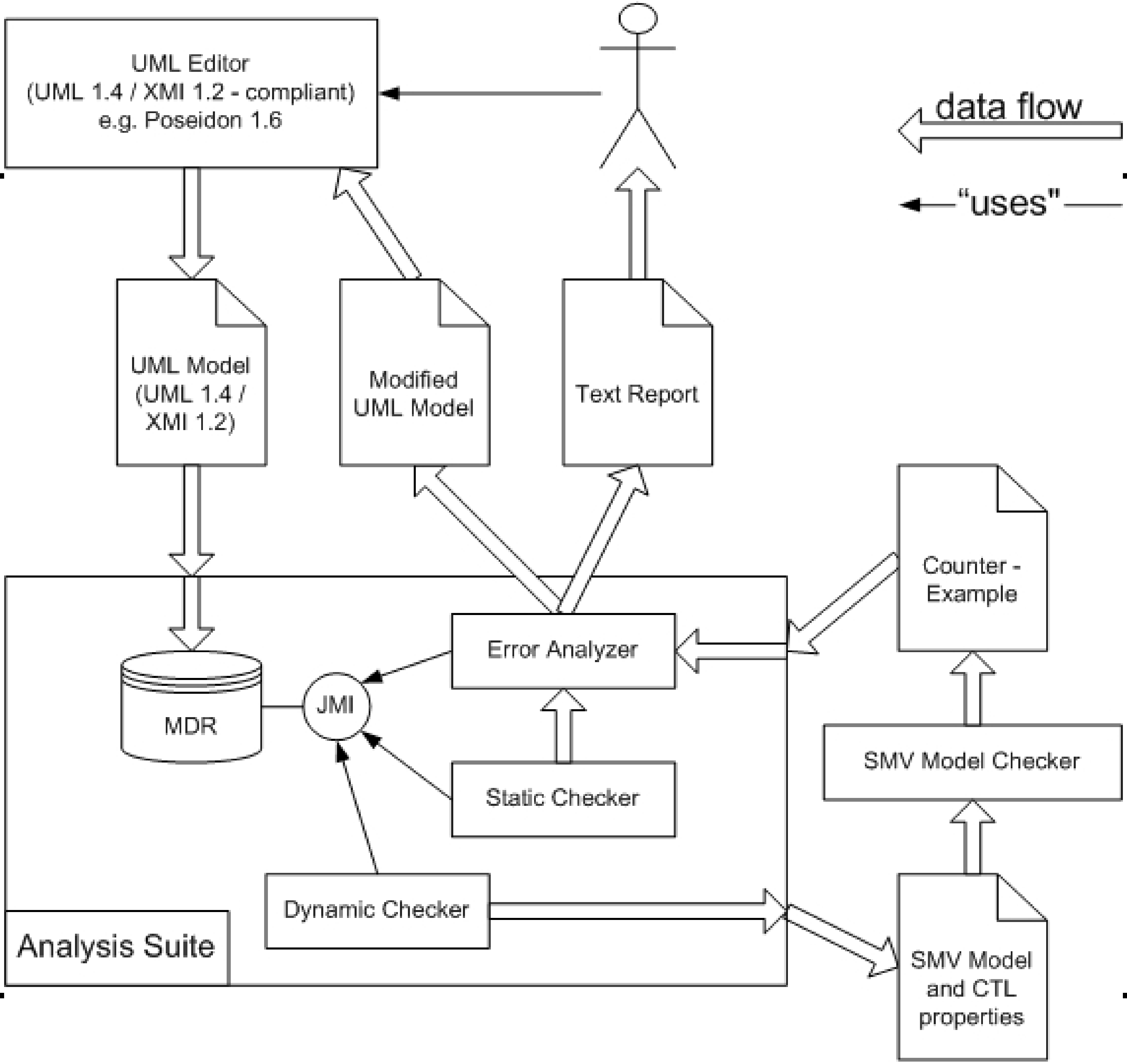
- Example: Loading UML Class:

```
Iterator it =
   uml.getCore().getUmlClass(
   ).refAllOfClass().iterator
   ();

while (it.hasNext()) {
    UmlClass uc =
   (umlClass)it.next();

    // .. do anything with
   UmlClass ..
}
```

Netbeans MDR Explorer

- Part of Netbeans IDE
- Browse Repositories
- Create Instances
- Load XMI Data
- Generate JMI Interfaces
- Shows
  - Extents
  - Metamodels
  - Instances




UML Editor
(UML 1.4 / XMI 1.2 - compliant)
e.g. Poseidon 1.6
data flow
"uses"
UML Model
(UML 1.4 /
XMI 1.2)
Modified
UML Model
Text Report
Counter -
Example
Error Analyzer
MDR
JMI
Static Checker
SMV Model Checker
Dynamic Checker
Analysis Suite
SMV Model
and CTL
properties

Tool

Currently implementing web-interface (see http://www4.in.tum.de/~umlsec and demo after this presentation).

Upload UML model (as .xmi file) on website. Tool analysis model for included criticality requirements. Download report and UML model with highlighted weaknesses.

Connection with analysis tool

Industrial CASE tool with UML-like notation: AUTOFOCUS (http://autofocus.informatik.tu-muenchen.de)

- Simulation
- Validation (Consistency, Testing, Model Checking)
- Code Generation (e.g. Java, C, Ada)
- Connection to Matlab

Connect UML tool to underlying analysis engine.

Roadmap

Prologue

UML

UMLsafe

Security-critical systems

UMLsec: The profile

Security analysis

Security patterns

UMLsec case studies

Java security, CORBAsec

Tools

Model-based Testing

Tool-support: Test-generation

Two complementary strategies:

- Conformance testing
- Testing for criticality requirements

Conformance testing

Classical approach in model-based test-generation (much literature).

Can be superfluous when using code-generation [except to check your code-generator, but probably once and for all]

Works independently of criticality requirements.

Conformance testing: Problems

- Complete test-coverage usually infeasible. Need to somehow select test-cases.
- Can only test code against what is contained in the behavioral model. Usually, model is more abstract than code. So may have „blind spots“ in the code.

For both reasons, may miss critical test-cases.

Criticality testing

Shortcoming of classical model-based test-generation (conformance testing) motivates „criticality testing“ (e.g., papers by Jürjens, Wimmel at PSI’01, ASE’01, ICFEM’02).

Goal: model-based test-generation adequate for (security-, safety-) critical systems.

Criticality testing: Strategies

Strategies:

- Ensure test-case selection from behavioral models does not miss critical cases: Select according to information on criticality („internal“ criticality testing).
- Test code against possible environment interaction generated from external parts of the model (e.g. deployment diagram with information on physical environment).

Internal Criticality Testing

Need behavioral semantics of used specification language (precise enough to be understood by a tool).

Here: semantics for simplified fragment of UML in „pseudo-code“ (ASMs).

Select test-cases according to criticality annotations in the class diagrams.

Test-cases: critical selections of intended behavior of the system.

External Criticality Testing

Generate test-sequences representing the environment behaviour from the criticality information in the deployment diagrams.

[For more details on criticality testing: can include talks mentioned above here.]

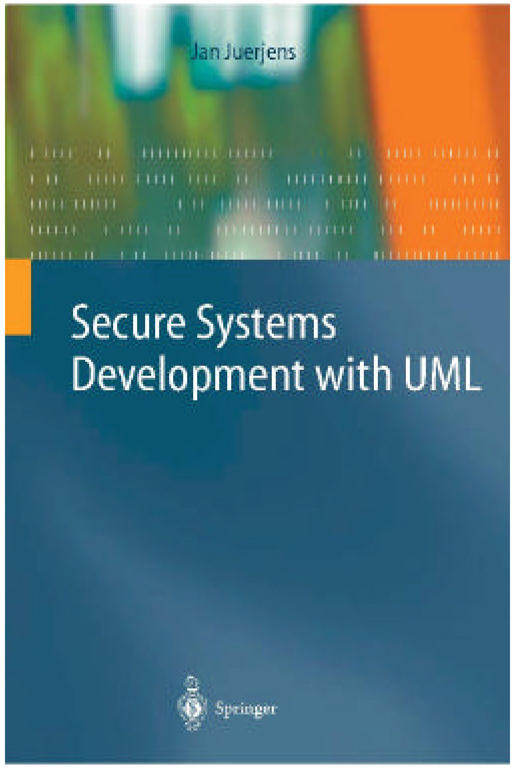
Some resources

Book: Jan Jürjens, Secure Systems Development with UML, Springer-Verlag, due 2003

Follow-on Tutorials: Sept: FORTE (BERLIN); Oct: Informatik (Frankfurt), ASE (Montreal), SNDP (Lübeck), LADC (Sao Paulo); Nov: WWW/Internet (Algarve), FMOODS (Paris), ICSTEST-E (Bilbao) …

Special SoSyM issue on Critical Systems Development with UML

CSDUML'03 @ UML'03 conference (Oct. in SFO)



More information (slides, tool etc.): http://www4.in.tum.de/~juerjens/csdumltut (user Participant, password Iwasthere)

Finally

We are always interested in industrial challenges for our tools, methods, and ideas to solve practical problems.

More info: http://www4.in.tum.de/~secse

Contact me here or via Internet.

Thanks for your attention !

BREAK !

Note:

We are always interested in industrial challenges for our tools, methods, and ideas to solve practical problems.
More info: http://www4.in.tum.de/~secse

Contact me here or via Internet.

Roadmap

Backup

IEC 61508 (1)

IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems

Strategy: derive safety requirements from a hazard and risk analysis and to design the system to meet those safety requirements, taking all possible causes of failure into account.

IEC 61508 (2)

- Concept: An understanding of the system and its environment is developed.
- Overall scope definition: The boundaries of the system and its environment are determined, and the scope of the hazard and risk analysis is specified.
- Hazard and risk analysis: Hazards and hazardous events of the system, the event sequences leading to the hazardous events, and the risks associated with the hazardous events are determined.
- Overall safety requirements: The specification for the overall safety requirements is developed in order to achieve the required functional safety.
- Safety requirements allocation: The safety functions contained in the overall safety requirements specification are allocated to the safety-related system, and a safety integrity level is allocated to each safety function.

IEC 61508 (3)

- Overall operation and maintenance planning: A plan is developed for operating and maintaining the system, and the required functional safety is ensured to be maintained during operation and maintenance.
- Overall safety validation planning: A plan for the overall safety validation of the system is developed.
- Overall installation and commissioning planning: Plans, ensuring that the required functional safety is achieved, are developed for the installation and commissioning of the system.
- Safety-related systems, E/E/PES: The E/E/PES safety-related system is created conforming to the safety requirements specification.
- Safety-related systems, other technology: Other technology safety-related systems are created to meet the requirements specified for such systems (outside scope of the standard).

IEC 61508 (4)

- External risk reduction facilities: External risk reduction facilities are created to meet the requirements specified for such facilities (outside scope of the standard).
- Overall installation and commissioning: The E/E/PES safety-related system is installed and commissioned.
- Overall safety validation: The E/E/PES safety-related system is validated to meet the overall safety requirements specification.
- Overall operation, maintenance and repair: The system is operated, maintained and repaired in order to ensure that the required functional safety is maintained.
- Overall modification and retrofit: The functional safety of the system is ensured to be appropriate both during and after modification and retrofit.

IEC 61508 (5)

- Decommissioning or disposal: The functional safety of the system is ensured to be appropriate during and after decommissioning or disposing of the system.