Willkommen zur Vorlesung

Sicherheit: Fragen und Lösungsansätze

im Wintersemester 2012 / 2013

Prof. Dr. Jan Jürjens

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Vorlesungswebseite (bitte notieren):

http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ws12-13/sfl/index_de.shtml

Agenda

- Organisatorisches
- Vorstellung des Fachgebietes
- Vorlesungsinhalte

Organisatorisches – Agenda

Studienordnung:
- Einordnung / Kompetenzen / Struktur / Prüfung

Vorlesung:
- Bildungsvertrag, Termine, Feedback

Übung:
- Konzept / Termine

Klausur

Studienordnung
Einordnung

Bachelor Informatik / Angewandte Informatik

- Wahlmodul

Diplom Informatik

- Spezialvorlesung, Schwerpunktgebiete: 1 (Software-Konstruktion), 3 (Verteilte Systeme), 5 (Sicherheit und Verifikation)

Master of Science „Datenwissenschaft“

- Exportveranstaltung

Verteilung (Handzeichen) ?

Teilnahmevoraussetzungen

- Erfolgreich abgeschlossen: –keine–
- Vorausgesetzte Kenntnisse: alle Module des 1. und 2. Studienjahres

Studienordnung
vermittelte Kompetenzen

Die Studierenden sollen die Fragen zur Sicherheit umfassend verstehen und gängige Lösungsansätze mitsamt der Nachweise ihrer Wirksamkeit kennen und anwenden können.

Darüber hinaus sollen sie weitergehende Lösungsvorschläge im Hinblick auf die Sicherheitseigenschaften eigenständig untersuchen und bewerten können.

Studienordnung
Struktur laut Modulhandbuch (Bachelor)

3 SWS:

- 2 SWS Vorlesung
- 1 SWS Übung

4 Credits

- 3 Credits Vorlesung
- 1 Credits Übung

Aufwand 120 Stunden

- 45 Stunden Präsenz (15*(2+1))
- 75 Stunden Vor-/Nachbereitung und Hausübungen (15*5)

Veranstaltungssprache Deutsch; Folien in Englisch

Modulprüfung: Klausur (90 Minuten) oder mündliche Prüfung (20 Minuten) gemäß Ankündigung nach Beginn der Veranstaltung.

Leistungsnachweise:

- Diplom-Studierende nach DPO 2001 erhalten einen unbenoteten Schein durch erfolgreiche Teilnahme an der Abschlussklausur.
  - Die Teilnahme an den Übungen und die Abgabe von Hausübungen sind freiwillig.
- Bachelor-Studierende benötigen für die Zulassung zur Prüfung/Klausur einen Leistungsnachweis über die erfolgreiche Teilnahme an den Übungen.

Bildungsvertrag
Wir bieten ...

- Fachliche Einführung in das Thema Softwaresicherheit
- Engagierte Betreuung
- Interessante Vorlesung
- Regelmäßige Sprechstunden
- Betreute Übungen
- Korrigierte Hausübungen
- Transparente Anforderungen
- Möglichkeiten zum direkten Feedback
- Möglichkeit zum Erwerb des Scheins

Bildungsvertrag
Wir erwarten ...

- Aktives Auseinandersetzen mit den Vorlesungsinhalten
- Aktive Teilnahme an der Vorlesung
- Vor- und Nachbereitung der Vorlesung
- Aktive Teilnahme an den Übungen
- Bearbeitung der Hausübungen

Termine:

- Di. 10:15 bis 12:00 Otto-Hahn-Str. 14 – 304
  10-min. Pause ca. um 11:00

- Aktuelle Informationen zur Vorlesung:

(Bitte regelmäßig beachten wegen möglicher Vorlesungs-ausfälle o.ä..)
http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ws12/sfl/index_de.shtml

Vorlesungsfolien werden auf o.g. Webseite zur Verfügung gestellt (spätestens Mitternacht des Vorabends der jeweiligen Vorlesung).

Vorlesung
Feedback

Wir haben besonderes Interesse an vorlesungsbegleitendem Feedback, um etwaige Verbesserungsvorschläge ggf. schon während des Semesters zu berücksichtigen.

Übliche Kontaktmöglichkeiten:

- E-mail jan.jurjens@cs.tu-dortmund.de
- Tel.: 0231 755-7208
- Sprechstunde: Dienstags 12.00-13.00 Uhr
- Anonymes Kontaktformular: Link von Vorlesungswebseite

Darüberhinaus: Vorlesungsbegleitendes Feedback über Fragebögen in unregelmäßigen Abständen.

Termine (**14 tägig**):

- Gruppe 1: Di 8:30 bis 10:00, OH-14, Raum 304
- Gruppe 2: Di 12:15 bis 13:45, MSW-16, Raum E31
- 1. Übung am 30. Okt. 2012

Kontakt

- Bei Fragen zu den Übungen und ihrer Durchführung:
  - Tutor der jeweiligen Gruppe
  - Dr. Thomas P. Ruhroth:
    thomas.ruhroth@cs.tu-dortmund.de

Übung
Termine

HÜ	Übung
1	30. Okt 12
2	13. Nov 12
3	27. Nov 12
4	11. Dec 12
5	8. Jan 13
6	22. Jan 13

Anmeldung:

- Via AsSESS
- http://ess.cs.uni-dortmund.de/ASSESS/index.php?do=lecturelist

- Anmeldung nach der heutigen Vorlesung möglich
- Verteilung wird am 22.10.2012 bekannt gegeben

Übung
Ablauf Präsenzübung

Übungsmodus

- Die Übung wird als Präsenzübung durchgeführt.
- Die Übungszettel werden während der Übung alleine oder in Gruppen bearbeitet.
- Der anwesende Tutor steht für Fragen zur Verfügung.
- Am Ende der Übung werden von den Studierenden Lösungen vorgeschlagen und die Aufgaben besprochen.
- Ein Lösungsvorschlag zur Präsenzübung wird dann über unsere Webseite veröffentlicht.

Übung
Hausübungen

Übungskonzept:

- Insgesamt werden 6 Übungszettel veröffentlicht.
- 6 davon enthalten eine Hausübung (für 5 gibt es Punkte)
- Hausübungen sollen bis zum entsprechenden Termin gelöst und abgegeben werden. (Mehr dazu gleich.)
- Die Aufgaben sollen (inhaltlich, konzeptionell) in Gruppen von min. 2 und max. 3 Studierenden bearbeitet werden. Inhaltliche und konzeptionelle Zusammenarbeit sind entsprechend auf den Abgaben zu vermerken.
- Abgabe im Briefkasten 1 in der OH20 jeweils bis folgenden Dienstag. Übungsblätter auf der Homepage.
- Die Abgaben werden korrigiert und die Gruppe erhält die korrigierte Lösung zurück.

Übung
Leistungsnachweis

Übungskonzept:

- Bei jeder Hausübung gibt es 10 Punkte.
- Diplom-Studierende nach DPO 2001
  - erhalten einen unbenoteten Schein durch erfolgreiche Teilnahme an der Abschlussklausur.
  - Teilnahme an den Übungen und Hausübungen ist freiwillig.
- Bachelor-Studierende
  - benötigen für die Zulassung zur Klausur einen Leistungs-nachweis über die erfolgreiche Teilnahme an den Übungen
  - 50% der Punkte aus den Hausübungen (25 von 50)
  - UND mindestens jeweils 30% der Punkte aus den Aufgaben 2+3 und 4+5+6
  - UND aktive Teilnahme an den Übungen

Übung
Hausübungen – Zeitschema

Woche	Mo	Di	Mi	Do	Fr	Sa	So
x		Ausgabe Übung letzte HÜ					
x+1		Abgabe					
x+2 =X		Ausgabe nächste HÜ Übung					

Übung
Hausübungen – Termine

HÜ	Ausgabe	Abgabe	Übung
1	16. Okt 12	23. Okt 12 13:00	30. Okt 12
2	30. Okt 12	6. Nov 12 13:00	13. Nov 12
3	13. Nov 12	20. Nov 13:00	27. Nov 12
4	27. Nov	4. Dec 12 13:00	11. Dec 12
5	11. Dec 12	18. Dec 12 13:00	8. Jan 13
6	8. Jan 13	15. Jan 13 13:00	22. Jan 13

Inpud-Forum

Ziel: Diskussion der Studierenden untereinander

Keine Kommunikation mit den Veranstaltern dort

- Keine garantierten Antwortzeiten
- Für dringendes: Mail oder Sprechstunde nutzen

Organisatorische + inhaltliche FAQ

- Für Fragen von Studierenden, die auch für andere interessant sein könnten

Moderation durch die Veranstalter

Prüfung
Termine

Prüfung: Klausur bei großer Vorlesungsgröße

- schriftlich
- 90 Minuten

Klausurtermine: Achtung: Daten noch nicht bestätigt!

- **18.02**.13: 12:30 bis 14:30 Uhr, HS1, Emil-Figge-Str. 50
- **18.03.**13: 13:30 bis 15:30 Uhr, HS1, Emil-Figge-Str. 50

Prüfung: münd. Prüfung bei sehr kleiner Vorlesungsgröße

- Details werden später bekanntgegeben

Kontakt

Jan Jürjens:

- http://www-jj.cs.tu-dortmund.de/staff/jurjens

Thomas Ruhroth:

- http://www-jj.cs.tu-dortmund.de/staff/ruhroth

Vorlesungsseite:

- http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ws12-13/sfl/index_de.shtml

Inpud-Forum:

- http://inpud.cs.tu-dortmund.de/phpbb/viewforum.php?f=332

Übungsanmeldung

- http://ess.cs.uni-dortmund.de/ASSESS

Vorstellung des Fachgebietes

- Forschung
- Abschlussarbeiten und Hiwi-Jobs
- Weitere Lehrveranstaltungen

Wer bin ich?

- Professor für Software Engineering an der TU Dortmund
- Wissenschaftskoordinator „Enterprise Engineering“ am Fraunhofer ISST
- Leiter der Fraunhofer-Attract-Projektgruppe „Architectures for Auditable Business Process Execution (Apex)“

Vorher u.a.:

- Royal Society Industrial Fellow bei Microsoft Research Cambridge
- Research Fellow am Robinson College (Univ. Cambridge)
- Postdoc an der TU München
- Promotion zu „Principles for Secure Systems Design“ (Univ. Oxford)
- Forschungsaufenthalte am LFCS (Univ. Edinburgh) und Bell Labs (Palo Alto)
- Studium an Univ. Bremen und Univ. Cambridge

Wer ist meine Forschungsgruppe?

- Misha Aizatulin (Microsoft Research Cambridge)
- H. Selcuk Beyhan (Logica (Germany))
- Francois Dupressoir (Microsoft Research Cambridge)
- Michael Giddings (Open University)
- Thorsten Humberg (Fraunhofer ISST)
- Christopher McLaughlin (Gartner)
- Sebastian Pape (TUD)
- **Dr. Thomas P. Ruhroth (TUD) => Übungsbetreuung**
- Andreas Schmitz (Fraunhofer ISST)
- Stefan Taubenberger (Münchener Rückversicherung)
- Daniel Warzecha (Fraunhofer ISST)
- Dr. Sven Wenzel (TUD)
- Christian Wessel (TUD)

Vertrauenswürdige IT-Systeme

IT Systeme durchziehen heute fast alle Funktionen in Wirtschaft und Gesellschaft. IT hat direkten (oft invasiven) Einfluss auf fast alle Aspekte menschlichen Lebens.

Die Erwartungen an die Vertrauenswürdigkeit dieser Systeme sind daher in den letzten 10 Jahren stark gestiegen. Diese Erwartungen werden oft nicht erfüllt. Teil des Problems ist, dass die bislang verwendeten System- und Software-Entwicklungsmethoden mit den gestiegenen Erwartungen bei gleichzeitig steigender Systemkomplexität nicht mithalten konnten.

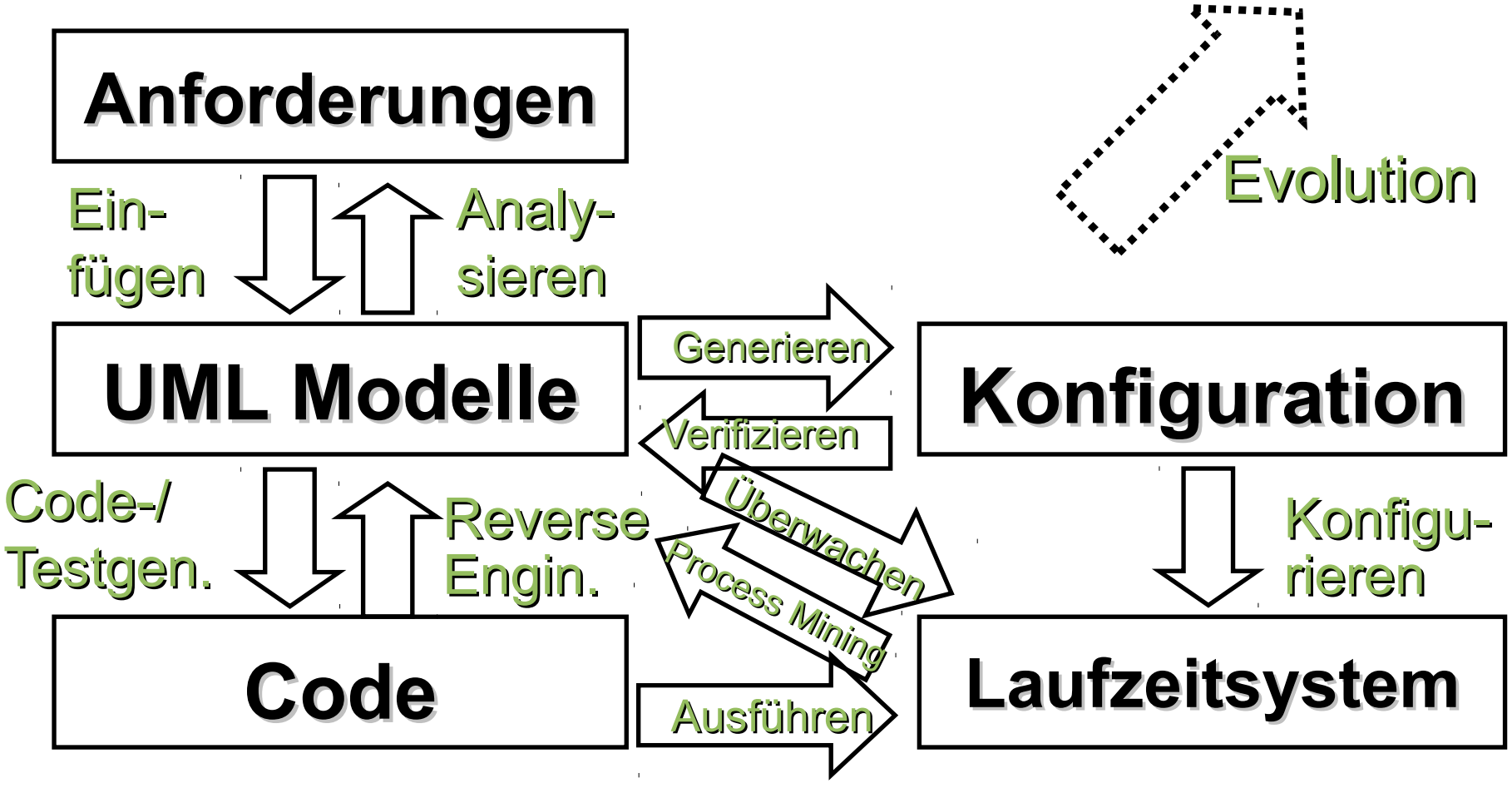
Offene Systeme

Aus Flexibiliäts- und Kostengründen sind moderne IT Systeme meist über offene Infrastrukturen realisiert, zum Beispiel:

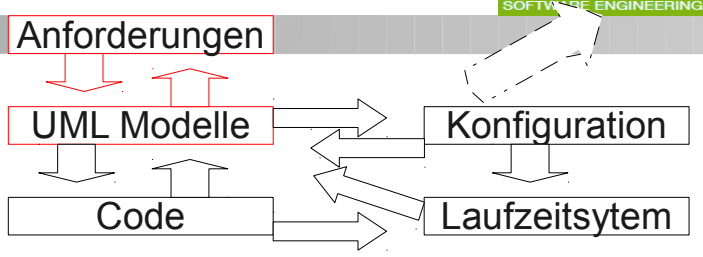
- Internet
- Mobile Netze

Aufgrund ihrer Offenheit sind sie dem Zugriff von Personen ausgesetzt, die in verschiedenem Maße vertrauenswürdig sind. Dieser Zugriff muss daher systemseitig reguliert werden. Aus Flexibiliäts- und Kostengründen wird dies oft auf der Softwareebene gelöst. Eine vertrauenswürdige IT braucht also sichere Software.

Modellbasierte Entwicklung



Modellierung mit UMLsec

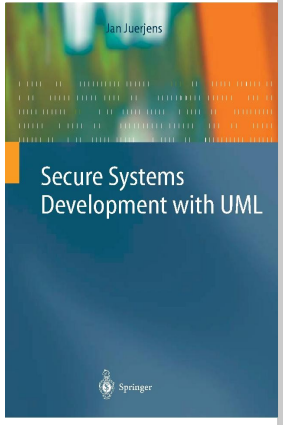


Ziel:

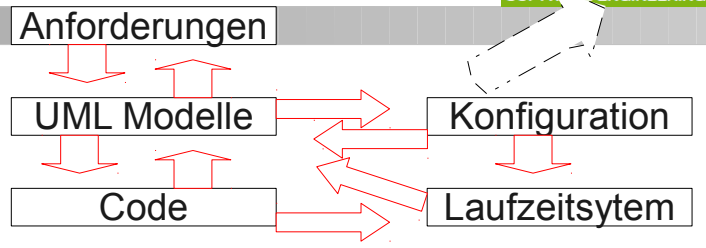
- Dokumentation und automatische Analyse von sicherheits-relevanten Informationen (z.B. Sicherheits-Eigenschaften und -Anforderungen) als Teil der Systemspezifikation.

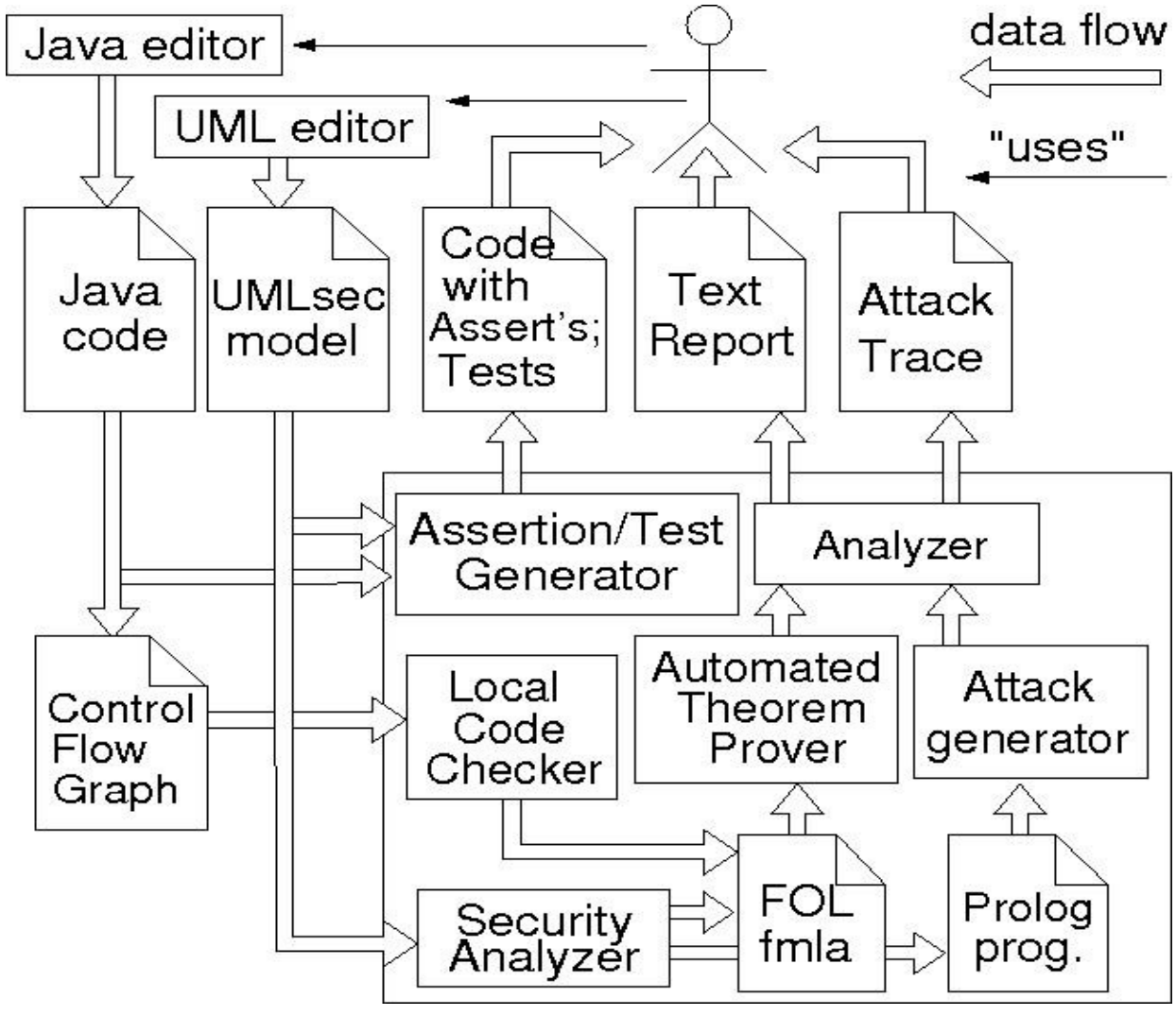
Idee:

- UML für System-Modellierung.
- Sicherheitsrelevante Informationen als Markierungen (Stereotypen) einfügen. Definiere dazu UML-Erweiterung UMLsec.
- Formale Semantik mit stromverarbeitenden Funktionen als Grundlage für Verifikation.



Werkzeugunterstützung

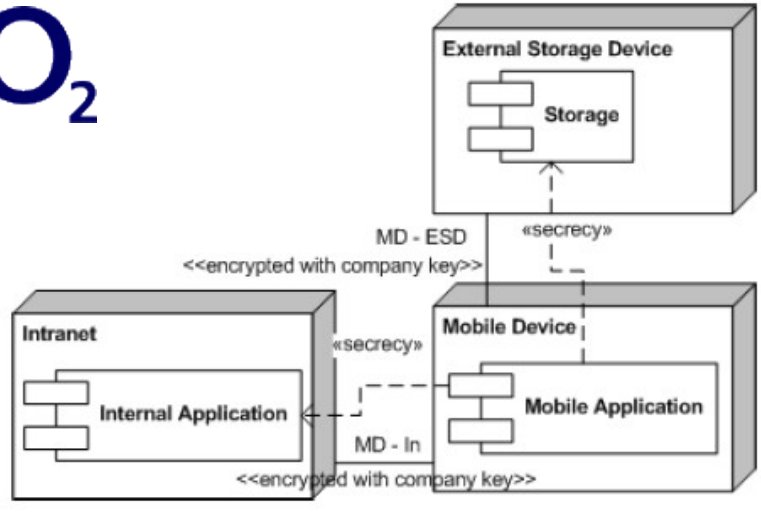




Mobile Informationssysteme bei O_2

- Anwendung von UMLsec auf mobile Kommunikations-Architekturen bei O_2 (Germany).
- Alle 62 Sicherheitsanforderungen aus der Security Policy erfolgreich verifiziert.
- Modellbasierte Techniken bringen Zusatzaufwand.
- Macht sich bezahlt bei wichtigen Sicherheitsanforderungen und Konzentration auf kritische Architekturanteile (auch im Vergleich mit anderen Qualitätssicherungs-Ansätzen mit vergleichbarer Verlässlichkeit).
- UMLsec adäquat für mobile Architekturen.

O_2



Internes Informationssystem bei BMW

MetaSearch Engine: Personalisierte Suche im Firmen-Intranet (passwort-geschützt).

BMW Group

Einige Dokumente sehr sicherheitskritisch.

Über 1.000 potentielle Benutzer, 280.000 Dokumente, 20.000 Anfragen pro Tag.

Nahtlos in unternehmensweite Sicherheitsarchitektur integriert. Bietet Sicherheitsdienste für Anwendungen (Benutzerauthentisierung, rollenbasierte Zugangskontrolle, globales Single-Sign-On), Ansatzpunkte für weitere Sicherheitsdienste.

Erfolgreich mit UMLsec analysiert.

Bank-Informationssystem bei der HypoVereinsbank

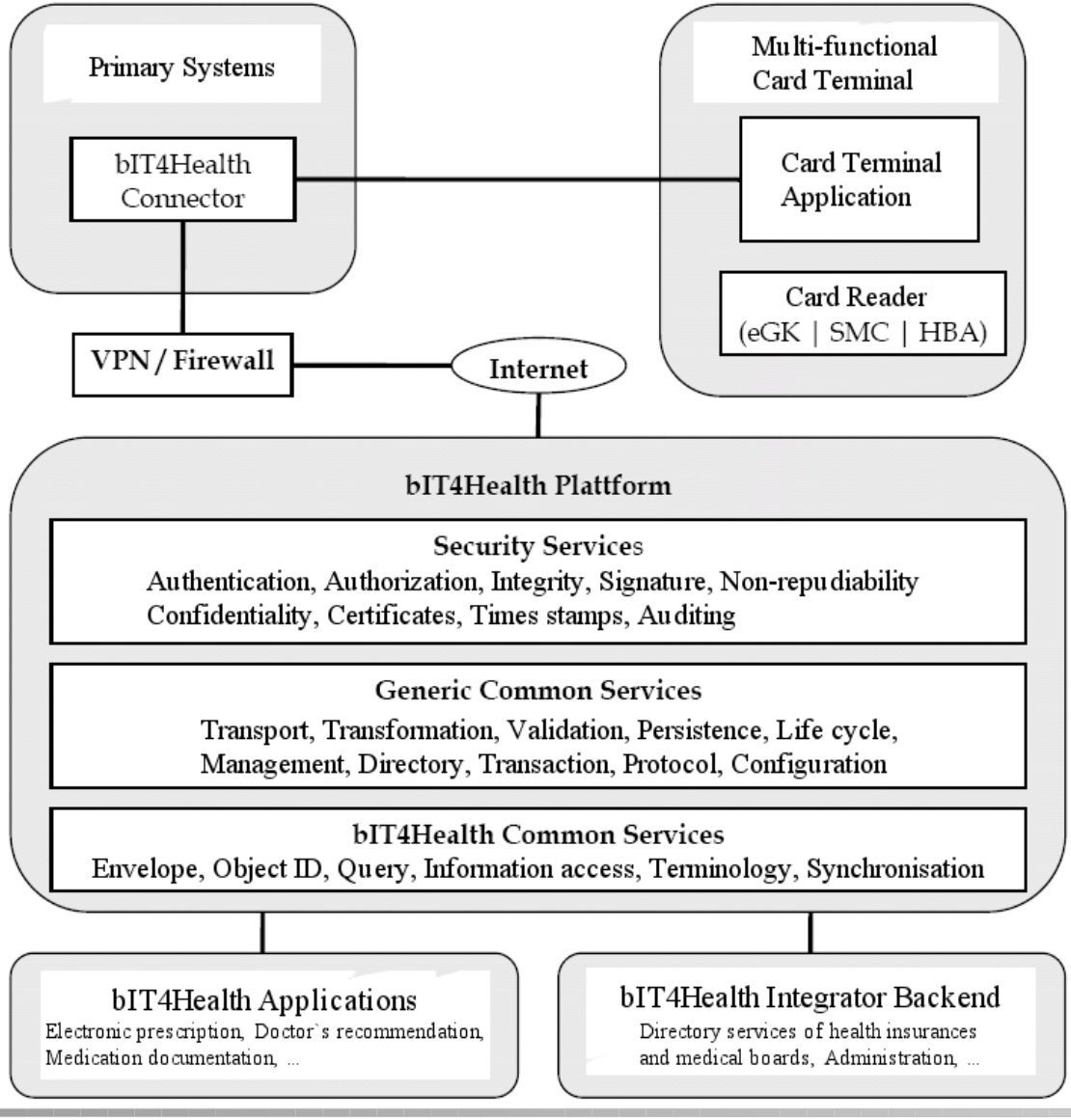
Modellbasierte Sicherheitsanalyse von webbasierter Bankanwendung ("digitaler Formularschrank").

Geschichtete Architektur (SSL Protokoll, darauf Client Authentisierungs-Protokoll)

Anforderungen:

- Vertraulichkeit
- Authentisierung

- Architektur mit UMLsec analysiert.
- Einige Schwachstellen aufgedeckt (fehlender Vertraulichkeitsschutz für digitale Rezepte).

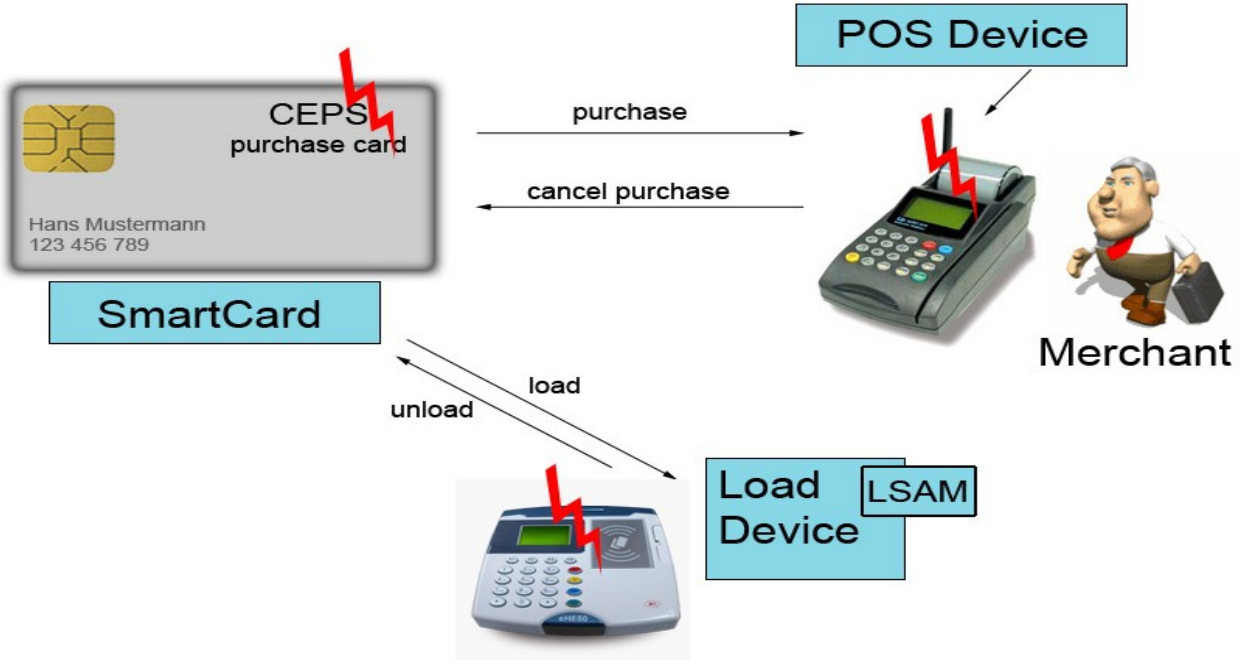


Mobiles Bezahlsystem

Common Electronic Purse Specifications:
Globaler Standard für e-Geldbörsen (Visa et al.).

Smartcard enthält Kontostand, sichert Transaktionen mithilfe Krypto.

Formale Analyse von Load und Purchase Protokollen: signifikante Schwachstellen: Kauf-Umleitung, Betrug Ladegerätbetreiber vs. Bank.



Biometrische Authentisierung

Smartcard-basiertes System.

Analysiert mit UMLsec parallel zur Entwicklung durch Firma in gemeinsamem Projekt.

Entdeckten drei signifikante Schwachstellen in verschiedenen Versionen (Fehlbedienungszähler umgangen durch Löschen / Wiederholen von Nachrichten; Smartcard unzureichend authentisiert durch Mischen von Sitzungen).

Endgültig entwickelte Version sicher.

Governance, Risk & Compliance auf Geschäftsprozessen

- Idee: Automatische Analyse von Geschäftsprozessmodellen auf operationale Risiken, z.B. gegenüber Benutzerberechtigungen zur Laufzeit, sowie der Benutzer-berechtigungen gegenüber der Sicherheitspolitik.
- Automatische Risiko-Identifikation und -Bewertung.
- Laufendes Projekt (Fraunhofer Attract): Architekturen für auditierbare Geschäftsprozessausführung (Apex).
- Insbesondere aktuell: Cloud-Sicherheit & -Compliance

Hiwi-Tätigkeiten

Es gibt verschiedene Möglichkeiten für eine Beschäftigung als Hiwi am Fraunhofer ISST oder am LS 14 / TUD:

- Unterstützung der folgenden Projekte (bespielsweise durch Java-Programmierung eines UML-Analyse Werkzeuges oder konzeptuelle Arbeiten im Bereich modell-basierte Sicherheitsanalyse): "Architectures for Auditable Business Process Execution (APEX)", „SecureClouds“, „ClouDAT“
- Unterstützung in der Lehre (Tutorien, Folienerstellung etc)

Informationen unter:

http://www-jj.cs.tu-dortmund.de/secse/pages/home/jobs_de.shtml

Abschlussarbeiten (z.B. Bachelor)

Abschlussarbeiten können in inhaltlicher Beziehung zu einer Hiwi-Tätigkeit am Fraunhofer ISST oder LS 14 / TUD durchgeführt werden (oder auch unabhängig davon).

Sie können insbesondere in Zusammenhang mit Anwendungsprojekten am ISST durchgeführt werden, wodurch sich vielfältige Möglichkeiten zu Kooperation mit Unternehmen ergeben, zB:

- Apex: Versicherungen / Banken (Münchener Rückversicherung, Signal Iduna, Wüstenrot), Softwarehersteller (SAP, IDS Scheer)
- Secure Clouds / ClouDAT: Cloud-Software-Anbieter (LinogistiX), IT-Berater (Admeritia, ITESYS, TÜV-IT)

Informationen unter:

http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/thesis/index_de.shtml

Vorstellung offener Abschlussarbeiten: Mo 5. Nov. 2012, 16:00 Uhr in Raum OH14 / E23

Einige Beispiel-Themen für Abschlussarbeiten

- Formale Abbildung von regulatorischer Compliance auf Security Policies
- Modellierung und Automatische Sicherheits-Analyse für Cloud Computing Systems
- Business Process Mining
- Spezifikation von IT-Sicherheitszielen für die Geschäftsprozessmodellierung und deren Integration in die Ausführung im Workflow
- Design und Entwicklung einer Schnittstelle zwischen der Business Prozess Management Suite ARIS und dem Sicherheitsanalysetool UMLsec zur Compliance Analyse in der Versicherungsdomäne
- Generierung von Geschäftprozessen mit OpenArchitectureWare unter Berücksichtigung von Sicherheitseigenschaften
- Werkzeuggestützte Modell-basierte Sicherheitsanalyse
- Werkzeugunterstützte Analyse von sicherheitskritischen SAP-Berechtigungen im Finanzbereich
- Modell-basiertes Return on Security Investment (ROSI) im IT-Sicherheitsmanagement

Weitere relevante Lehrveranstaltungen

Dieses Semester:

- Seminar „Ausgewählte Themen des Modell-basierten Sicherheits-Engineerings“. http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ws12-13/mbse-sem/index_de.shtml
- Vorlesung „Softwarekonstruktion“ (Bachelor Wahl-Pflicht). http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/ws12-13/swk/index_de.shtml

SS 2013:

- Fachprojekt „Softwaretechniken für sichere Cloud-Computing-Systeme” (4 SWS)
- Methodische Grundlagen des Software Engineering (Master-Basismodul Software) (4+2 SWS)
- Seminar „Ausgewählte Themen des Modell-basierten Sicherheits-Engineerings“.

Zuordnung der Wahlveranstaltungen zu Schwerpunktgebieten (Diplom):

- Sicherheit und Verifikation
- Software-Konstruktion

Forschungsbereich Master: Software, Sicherheit und Verifikation

Informationen unter:
http://www-jj.cs.tu-dortmund.de/secse/pages/teaching/index_de.shtml

Und danach ?

[http://www.fraunhofer.de/de/presse/presseinformationen/2012/april/ertraege-aus-der-wirtschaft.html]

"**Die Fraunhofer-Gesellschaft ist auch im Jahr 2011 weiter gewachsen.** Das Finanzvolumen stieg um 12 Prozent auf 1,85 Milliarden Euro an.

Im Vorjahr hat Fraunhofer 1300 neue Beschäftigte eingestellt. Damit stieg die Zahl der Mitarbeiterinnen und Mitarbeiter auf mehr als 20 000 an. »Um die wachsende Anzahl an Forschungsprojekten und das steigende Auftragsvolumen bearbeiten zu können, benötigen wir auch künftig weitere neue qualifizierte Mitarbeiterinnen und Mitarbeiter«, betont der Personalvorstand der Fraunhofer-Gesellschaft.

Fraunhofer ist ein beliebter Arbeitgeber. Das hat die Mitarbeiter-Befragung im Vorjahr ergeben. 86 Prozent der Mitarbeiterinnen und Mitarbeiter sind stolz darauf, bei Fraunhofer zu arbeiten. Im Durchschnitt sagen das in Deutschland nur 60 Prozent über ihren Arbeitgeber."

http://www.randstad-award.de/randstad-award-deutschland/presse/news/news/items/349.html

"**Der Randstad Award für den attraktivsten Arbeitgeber geht in diesem Jahr an die Fraunhofer-Gesellschaft.** Auf Platz 2 schaffte es EADS, dicht gefolgt von BMW auf Platz 3."

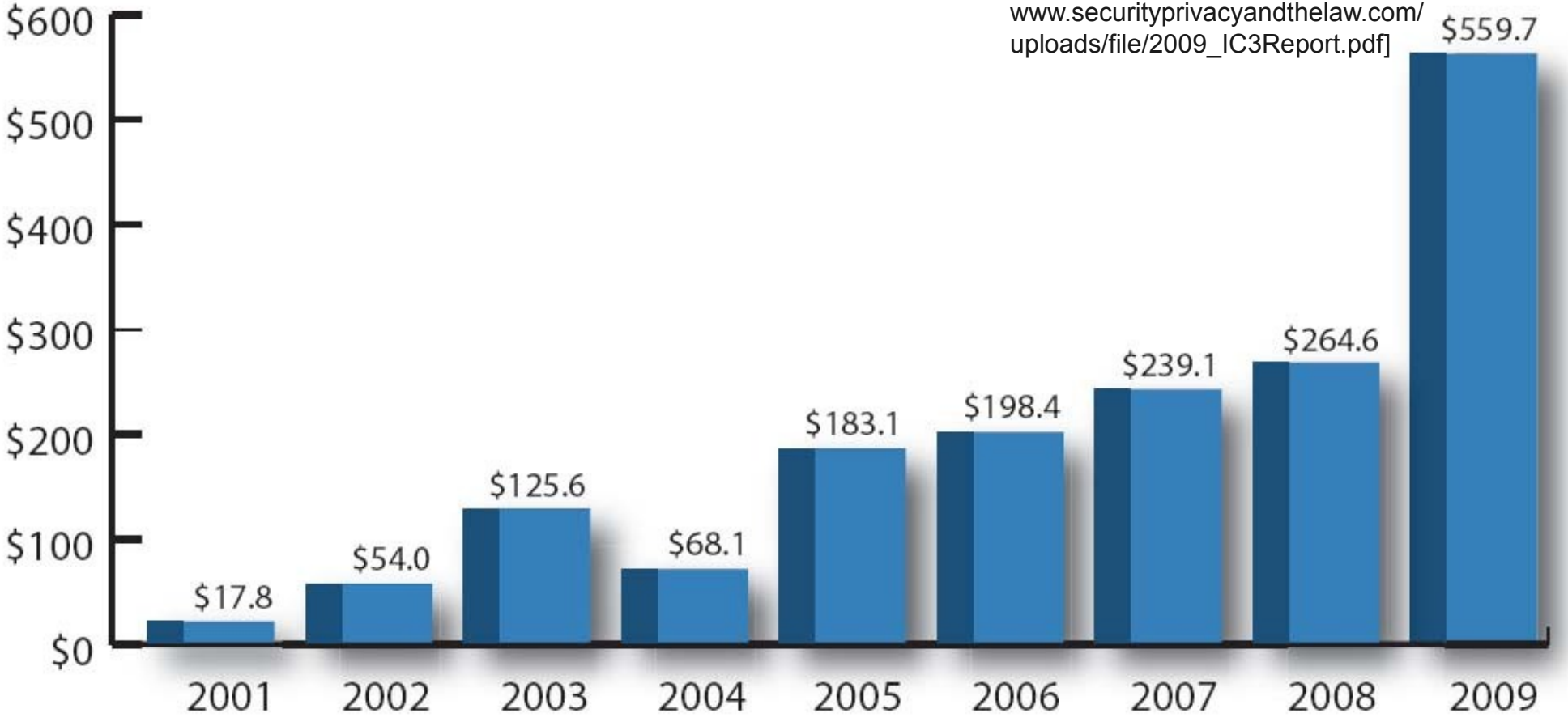
Und: Promotion projekt-begleitend möglich.

Kontakt: http://jan.jurjens.de

Warum ist dies Ihre wichtigste Vorlesung in diesem Semester ?

Figure 2: Yearly Dollar Loss (in millions) of Referred Complaints

[2009 Internet Crime Report, US Dep. Of Justice
www.securityprivacyandthelaw.com/
uploads/file/2009_IC3Report.pdf]



Beispiel (2010): Virusangriff auf Iranisches Nuclearprogramm

http://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAInEy6U_story.html

Stuxnet was work of U.S. and Israeli experts, officials say

A damaging cyberattack against Iran's nuclear program was the work of U.S. and Israeli experts and proceeded under the secret orders of President Obama, who was eager to slow that nation's apparent progress toward building an atomic bomb without launching a traditional military attack, say current and former U.S. officials.

The origins of the cyberweapon, which outside analysts dubbed Stuxnet after it was inadvertently discovered in 2010, have long been debated, with most experts concluding that the United States and Israel probably collaborated on the effort. The current and former U.S. officials confirmed that long-standing suspicion Friday, after a New York Times report on the program. […]

Overall, the attack destroyed nearly 1,000 of Iran's 6,000 centrifuges — fast-spinning machines that enrich uranium, an essential step toward building an atomic bomb. The National Security Agency developed the cyberweapon with help of Israel.

Beispiel (2011): Hacker attackieren den Währungsfond

http://www.zeit.de/digital/datenschutz/2011-06/hacker-iwf-wirtschaftsdaten

Hacker haben den Internationalen Währungsfonds angegriffen und offenbar Daten gestohlen. Der IWF geht von Spionage aus und macht eine "bestimmte Regierung" verantwortlich.

Der Internationale Währungsfonds (IWF) ist Opfer einer Attacke auf seine Computer geworden. Nach einem Bericht von Bloomberg News wurden bei dem Angriff E-Mails und weitere Dokumente gestohlen. Der Fonds habe Ermittlungen eingeleitet, wie es zu dem Hacker-Angriff kommen konnte, erklärte ein IWF-Sprecher. Die Arbeit der Organisation sei durch den Angriff aber nicht beeinträchtigt. Über das Ausmaß des Schadens machte der Sprecher keine Angaben. [...]
Nach Angaben des Internet-Sicherheitsexperten Tom Kellermann, der in dieser Funktion auch für den IWF und die Weltbank gearbeitet hat, zielte der Hackerangriff darauf, heimlich eine Software zu installieren, um einer bestimmten Regierung Zugang zu Insider-Informationen des IWF über andere Länder zu verschaffen. Um welche Regierung es sich handle sei noch unklar.

Mehr Beispiele: Einige der größten Schäden durch Cyber-Angriffe

http://www.businesspundit.com/10-most-costly-cyber-attacks-in-history

2011: Exposure of over 100 million PlayStation Network and Sony Online Entertainment accounts is forging a new chapter in the history of cyber-attacks. The personal information — including credit and debit card data — of tens of millions of users was stolen by an as yet unknown group of assailants. Experts predict that the damage may range from $1 to $2bn, making it possibly the costliest cyber-hack ever to have been pulled off.
2008: Trusted payments processor Heartland Payment Systems fell victim to a plot to steal credit and debit card numbers. By secretly infesting the company's computer network with spyware, the criminal gang responsible were able to steal over 100 million individual card numbers. The episode ended up costing around $140m.
2007: Grocery retailer Hannaford Bros suffered a four-month long breach of their security from the winter of 2007 to the spring of 2008. During this period, over 4.2 million credit and debit card numbers were exposed, along with other sensitive information. Experts table the costs incurred at an estimated $252m.
2005: Massachusetts-based retailing company TJX was attacked by a gang able to get their hands on over 45 million credit and debit card numbers, a selection of which they then used to fund a multi-million dollar spending spree from Wal-Mart's stock of electronics equipment. The damage from the data-breach ended up costing over $250m in total.
2004: Sven Jaschan unleashed a virus which infected millions of computers around the world, reaching its highest degree of destruction when it comprehensively disabled the Delta Air Lines computer system, causing the cancellation of several transatlantic flights. Jaschan was eventually arrested after a three-month hunt, during which Mircosoft placed a $250,000 bounty on the hacker's head. An estimated $500 million worth of damage was generated.
2000: 15-year-old Michael Calce conducted notorious attacks against huge companies with high levels of security. Amongst those attacked were computer manufacturer Dell, media giant CNN, and shopping sites Amazon and Ebay. Prosecution for the estimated $1.2bn worth of damage caused went pretty smoothly, from Calce's perspective. He ended up with a sentence of eight months open custody.

Ziele dieser Vorlesung

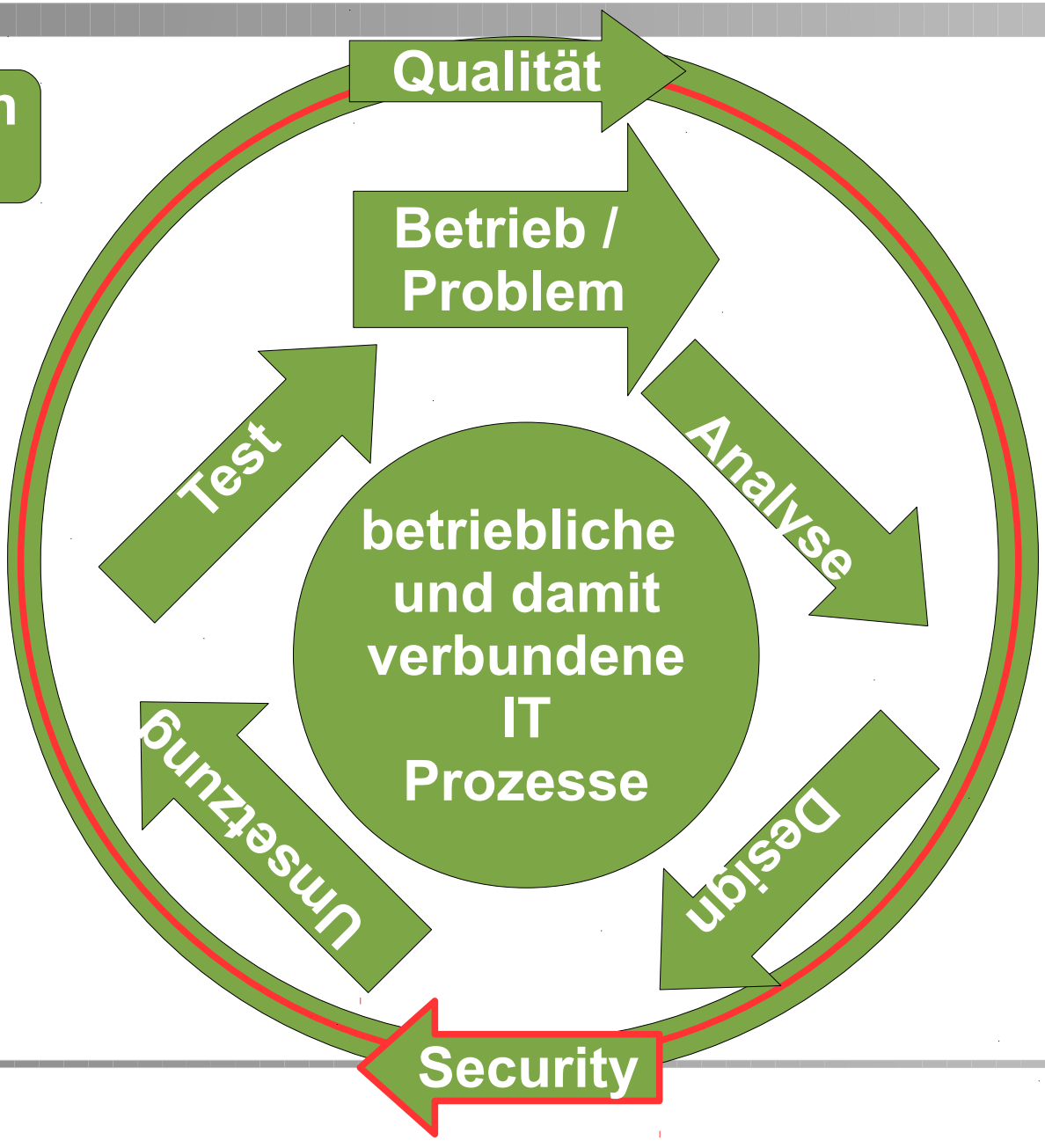
Es sollen die folgenden Fragen behandelt werden:

- Welche und wessen Interessen nach Sicherheit sollen gewahrt werden ?
- Welche technischen und organisatorischen Anforderungen ergeben sich aus den Sicherheitsinteressen ?
- Welche technischen Sicherheitsmaßnahmen können welche inhaltlichen Sicherheitsanforderungen unterstützen ?
- In welche organisatorischen Strukturen müssen die technischen Maßnahmen eingebettet werden ?
- Wie kann ein Rechensystem unter dem Gesichtspunkt der Sicherheit entworfen, verwirklicht und betrieben werden ?
- Wie kann man sich vergewissern, welche Art und welchen Grad von Sicherheit man tatsächlich erreicht hat ?

Es wird ein Überblick über derartige Fragen und eine Einführung in die möglichen Lösungsansätze gegeben. Dabei werden insbesondere die folgende Einzelthemen behandelt: Sicherheitsinteressen und ihre Wechselwirkungen, Informationsflüsse und Inferenzkontrolle, Kontrolle und Überwachung, Kryptographie.

Vorlesungsüberblick
Inhaltlicher Zusammenhang

Sicherheit von IT-Systemen



Themen der Vorlesung (1)

Part I: Challenges and Basic Approaches

1) Interests, Requirements, Challenges, and Vulnerabilities

2) Key Ideas and Combined Techniques

Part II: Control and Monitoring

3) Fundamentals of Control and Monitoring

4) Case Study: UNIX

Part III: Cryptography

5) Fundamentals of Cryptography

6) Case Studies: PGP and Kerberos

7) Symmetric Encryption

8) Asymmetric Encryption and Digital Signatures with RSA

9) Some Further Cryptographic Protocols

Themen der Vorlesung (2)

Part IV: Access Control

10) Discretionary Access Control and Privileges

11) Mandatory Access Control and Security Levels

Part V: Security Architecture

12) Layered Design Including Certificates and Credentials

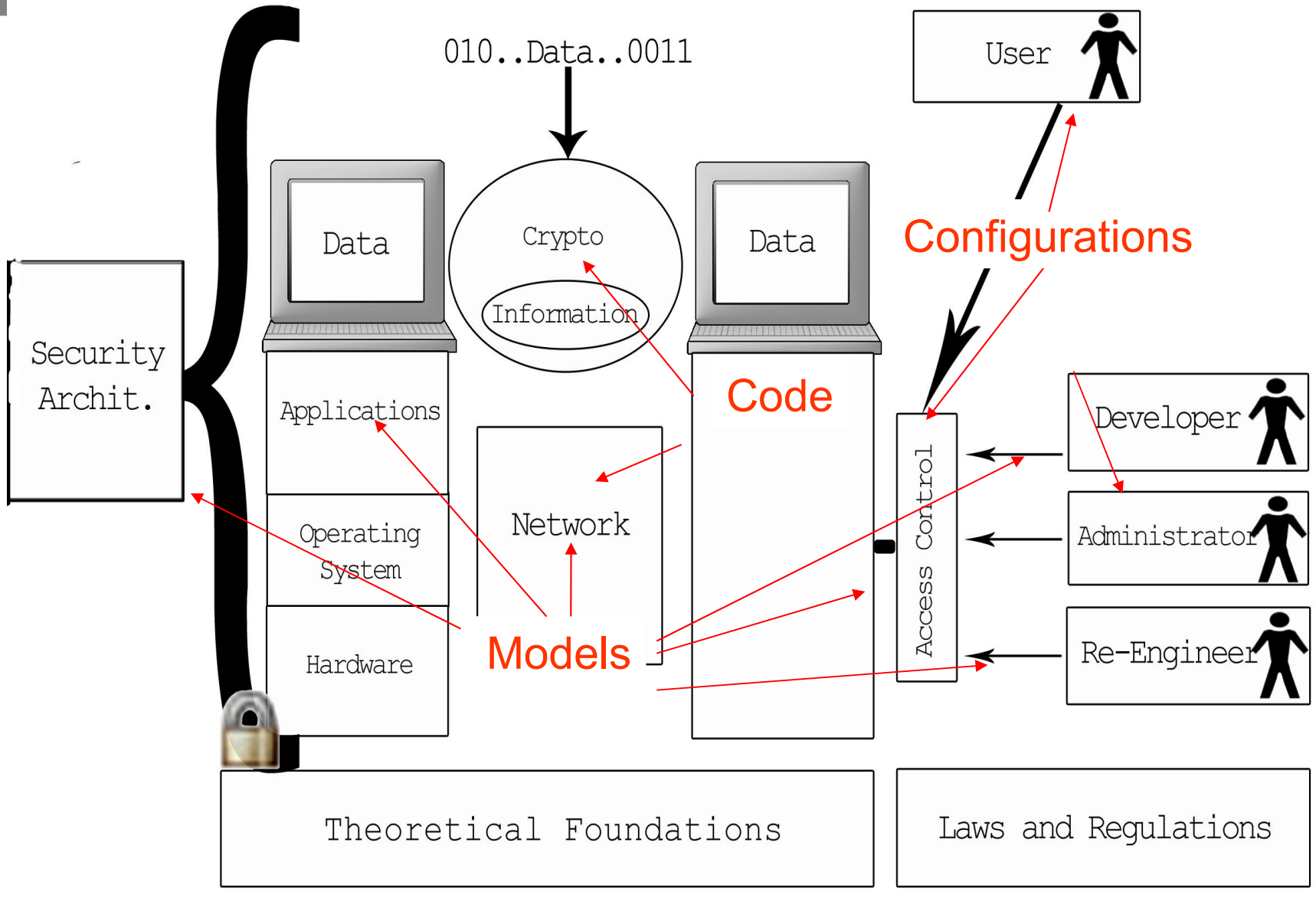
13) Intrusion Detection and Reaction

Part VI: Model-based Security

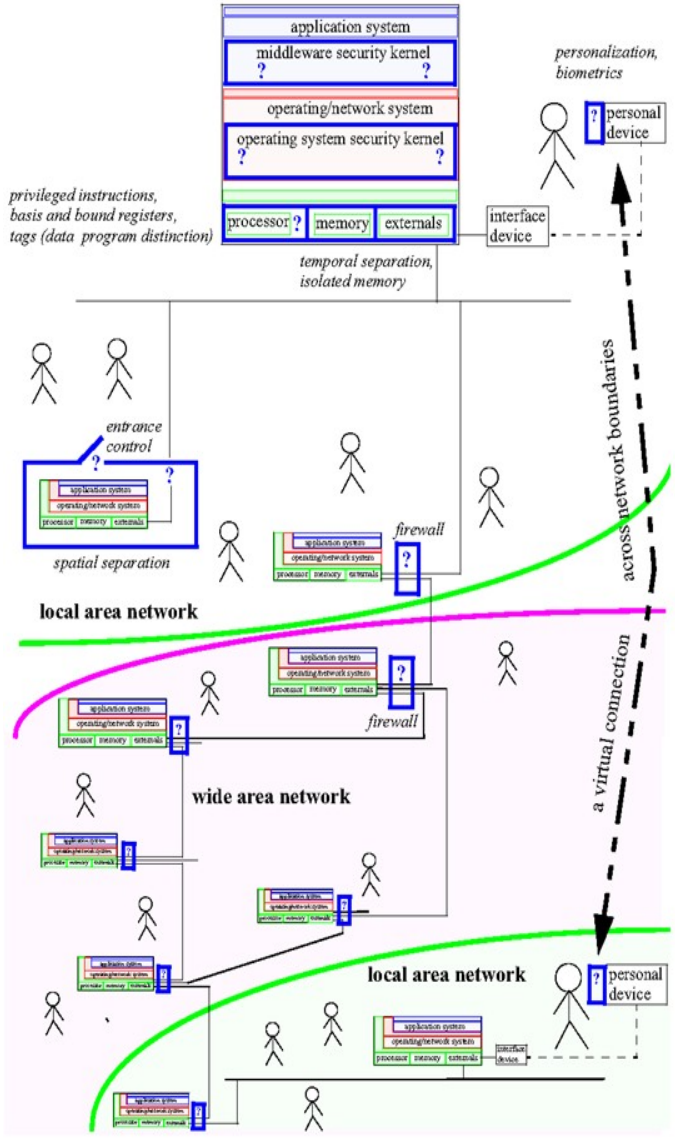
14) Model-based Security

15) Practical applications

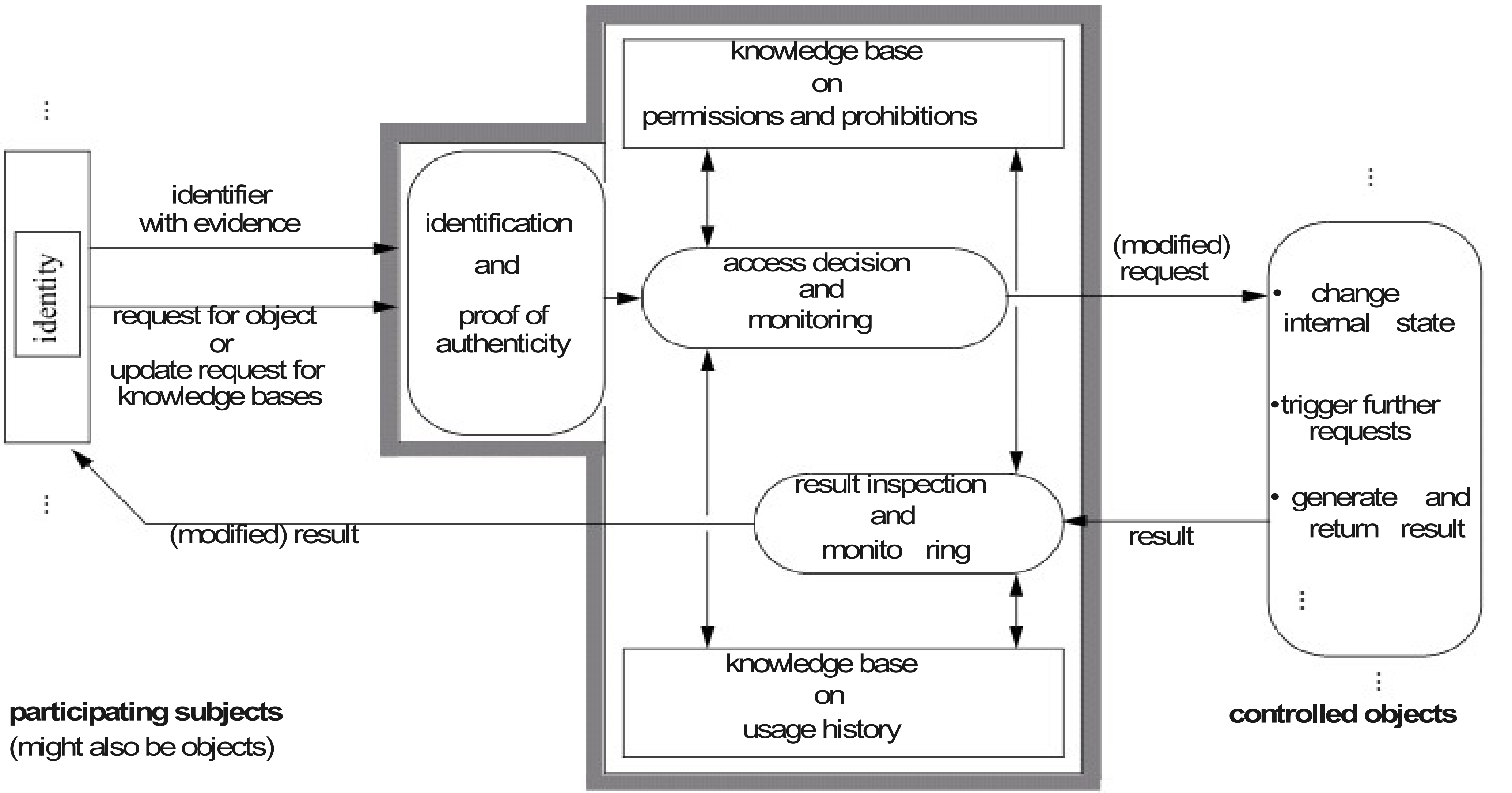
1) Interests, Requirements, Challenges, and Vulnerabilities



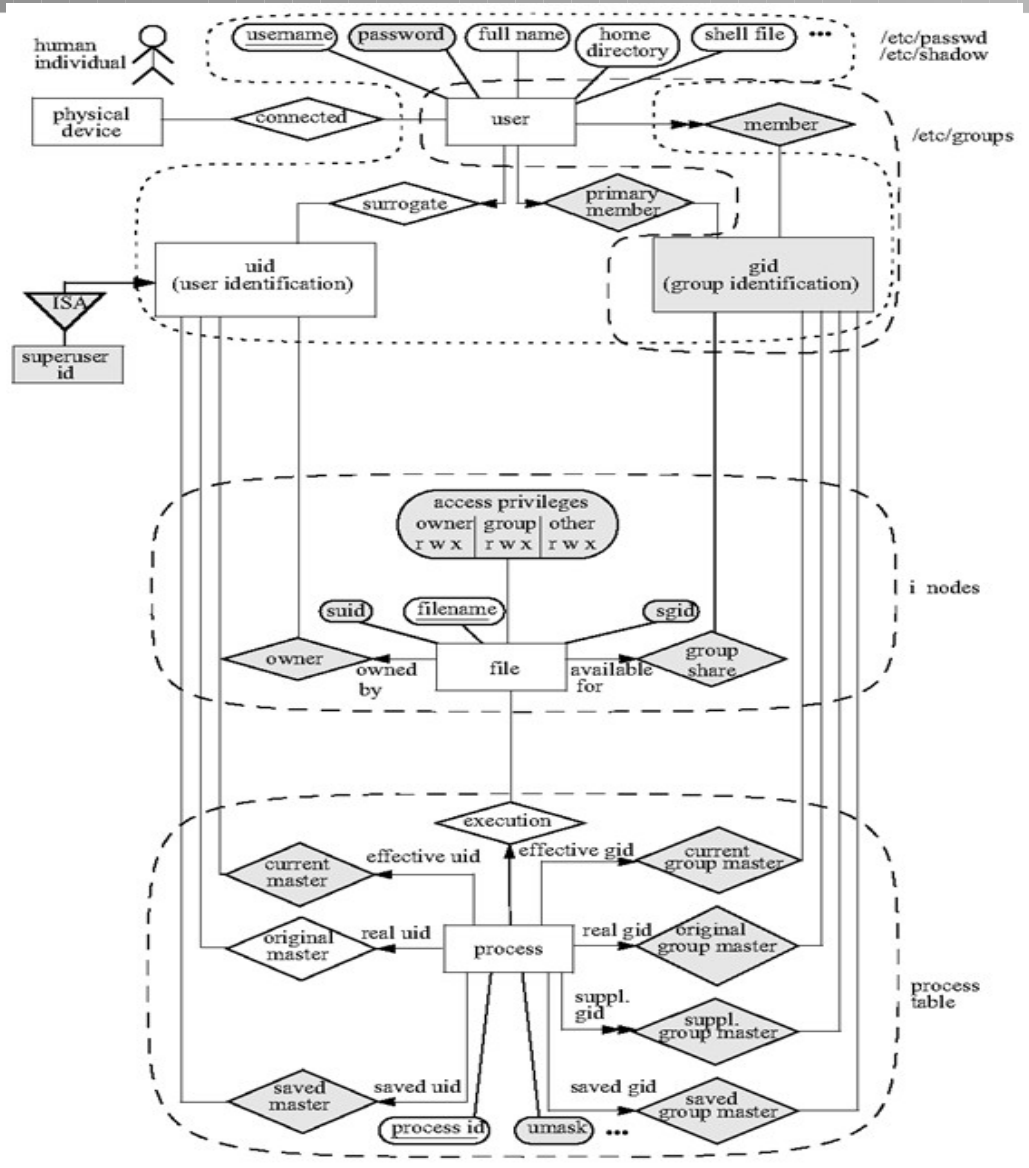
2) Key Ideas and Combined Techniques



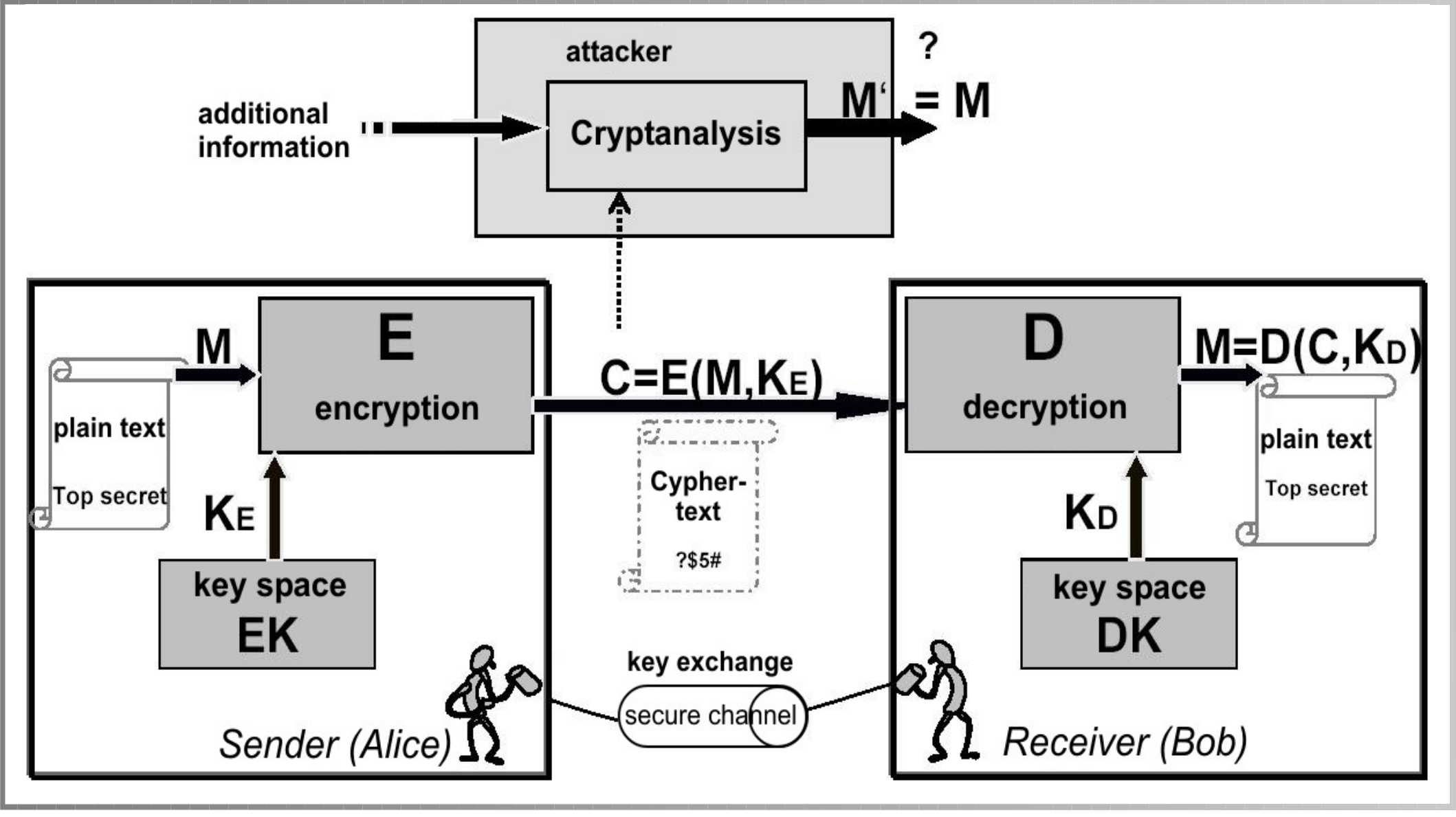
3) Fundamentals of Control and Monitoring



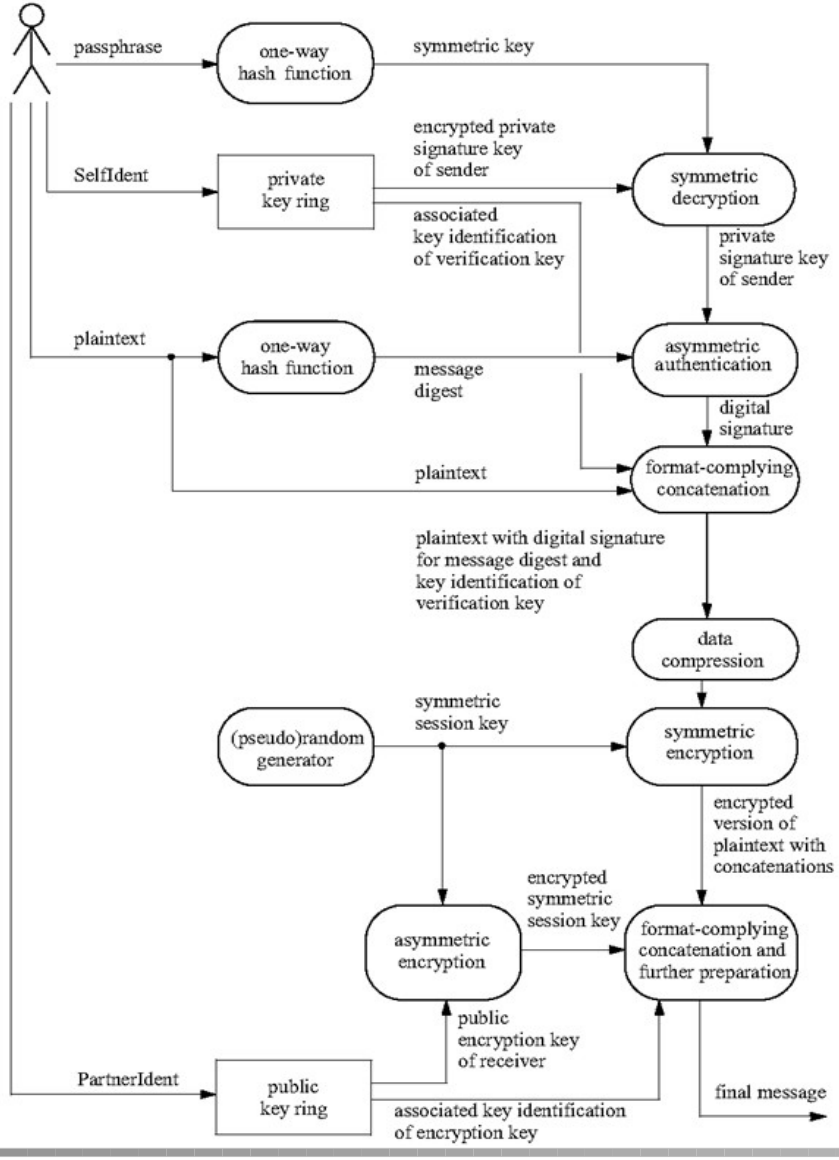
4) Case Study: UNIX



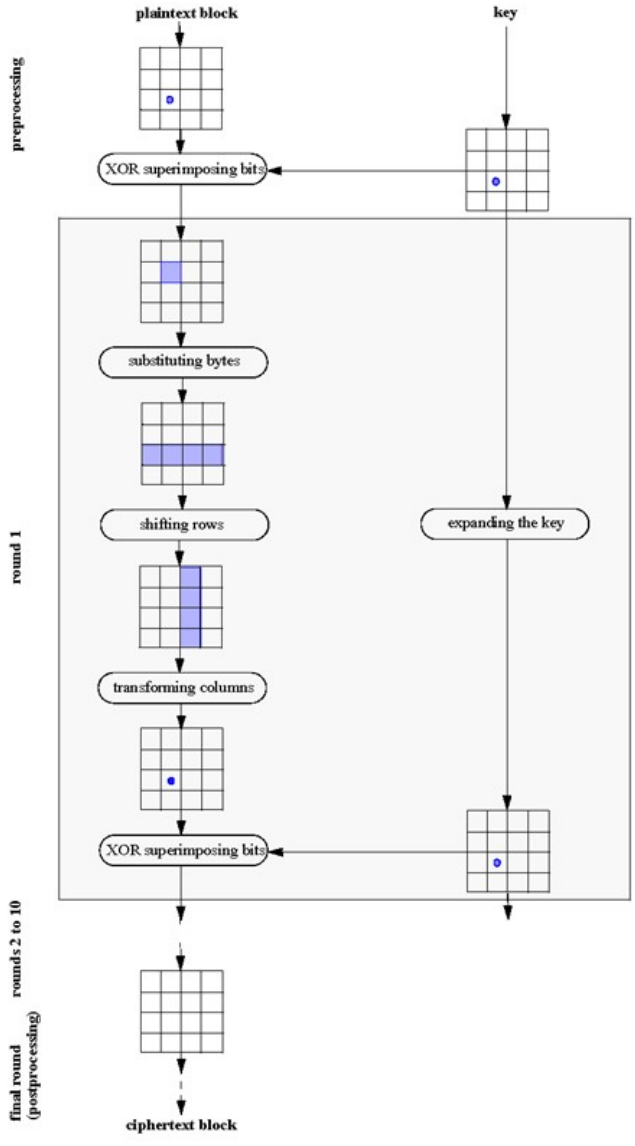
5) Fundamentals of Cryptography



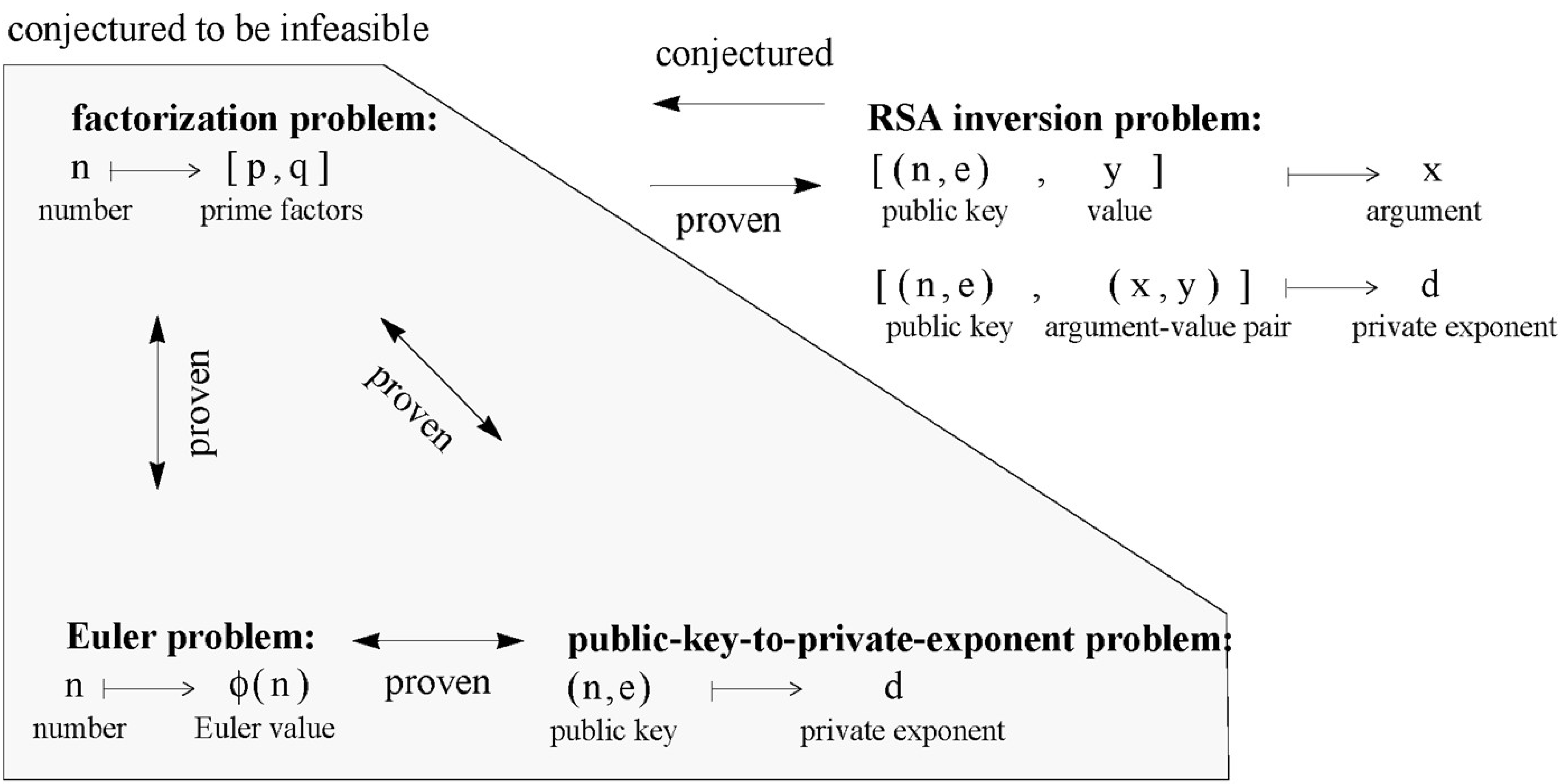
6) Case Studies: PGP and Kerberos



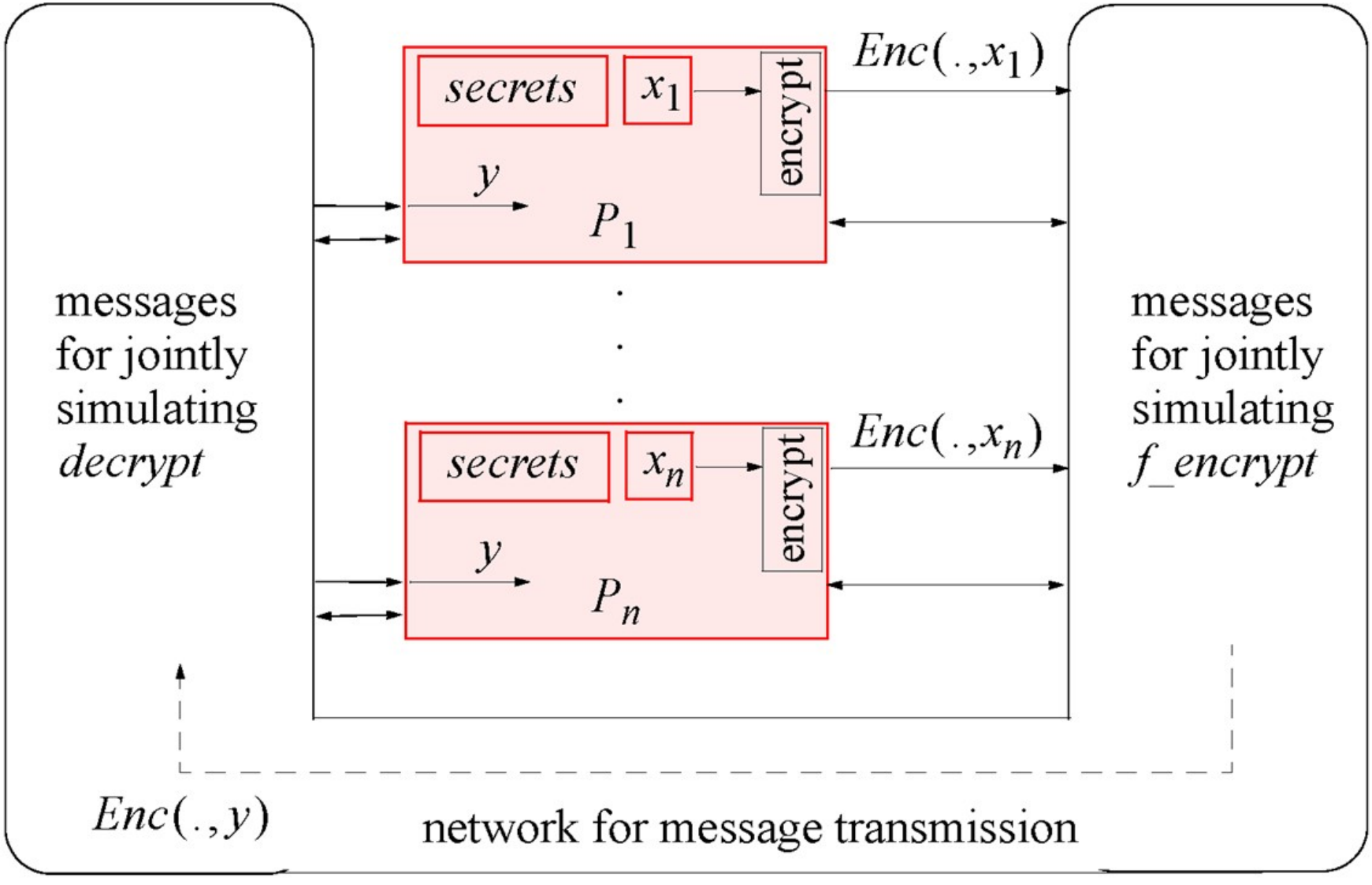
7) Symmetric Encryption



8) Asymmetric Encryption and Digital Signatures with RSA



9) Some Further Cryptographic Protocols

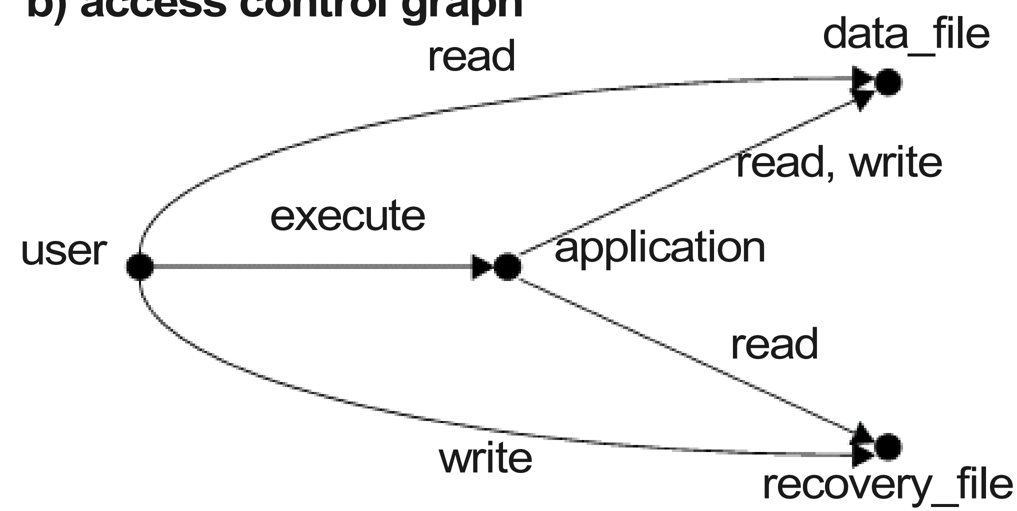


10) Discretionary Access Control and Privileges

a) access control matrix

	application	data_ file	recovery_ file
user	execute	read	write
application		read, write	read

b) access control graph



c) privilege lists

Cl(user) = { [application,execute], [data_file,read], [recovery_file,write] }

Cl(application) = { [data_file,read], [data_file,write], [recovery_file,read]
}

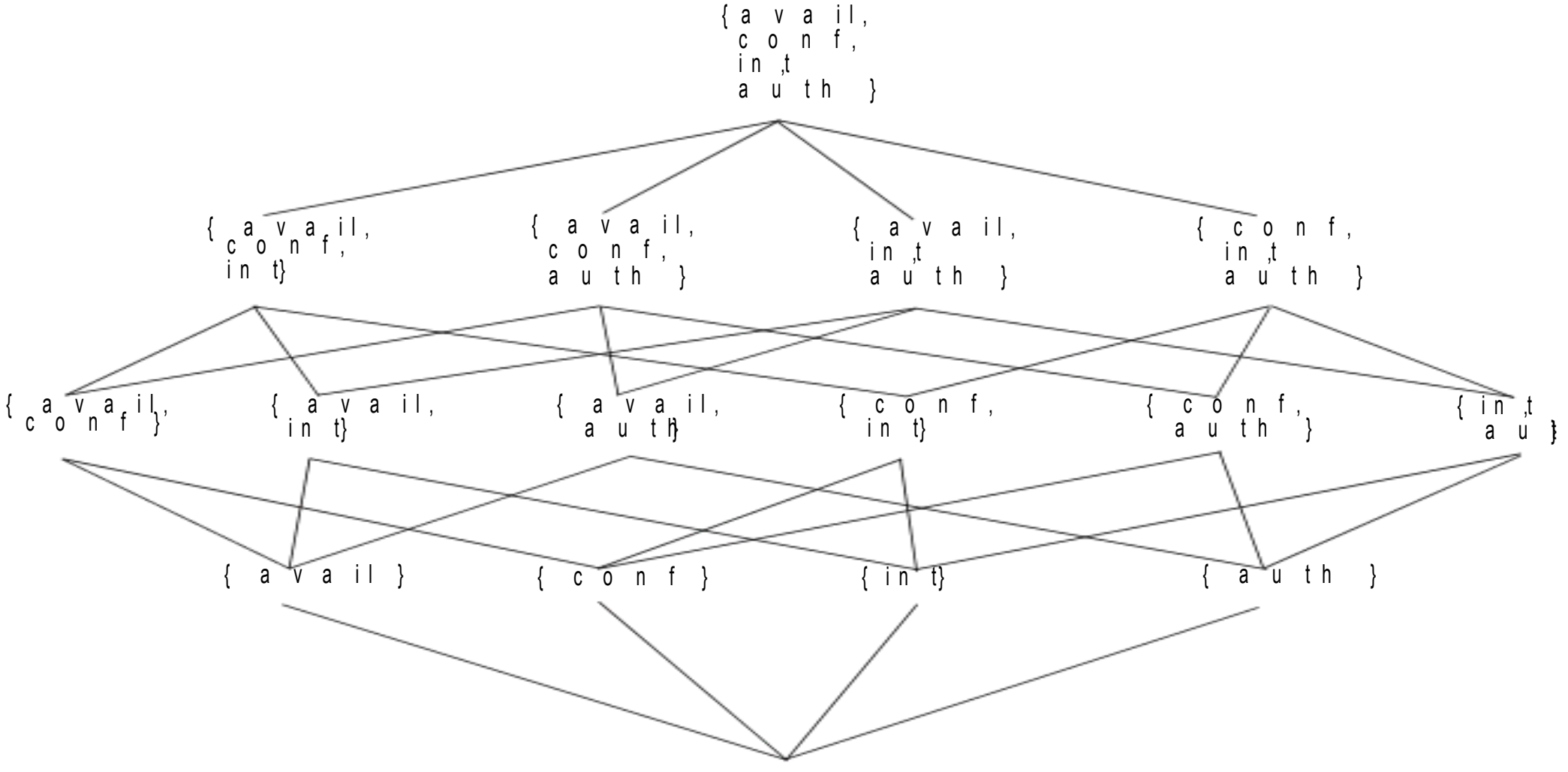
d) access control lists

Acl(application) = { [user,execute] }

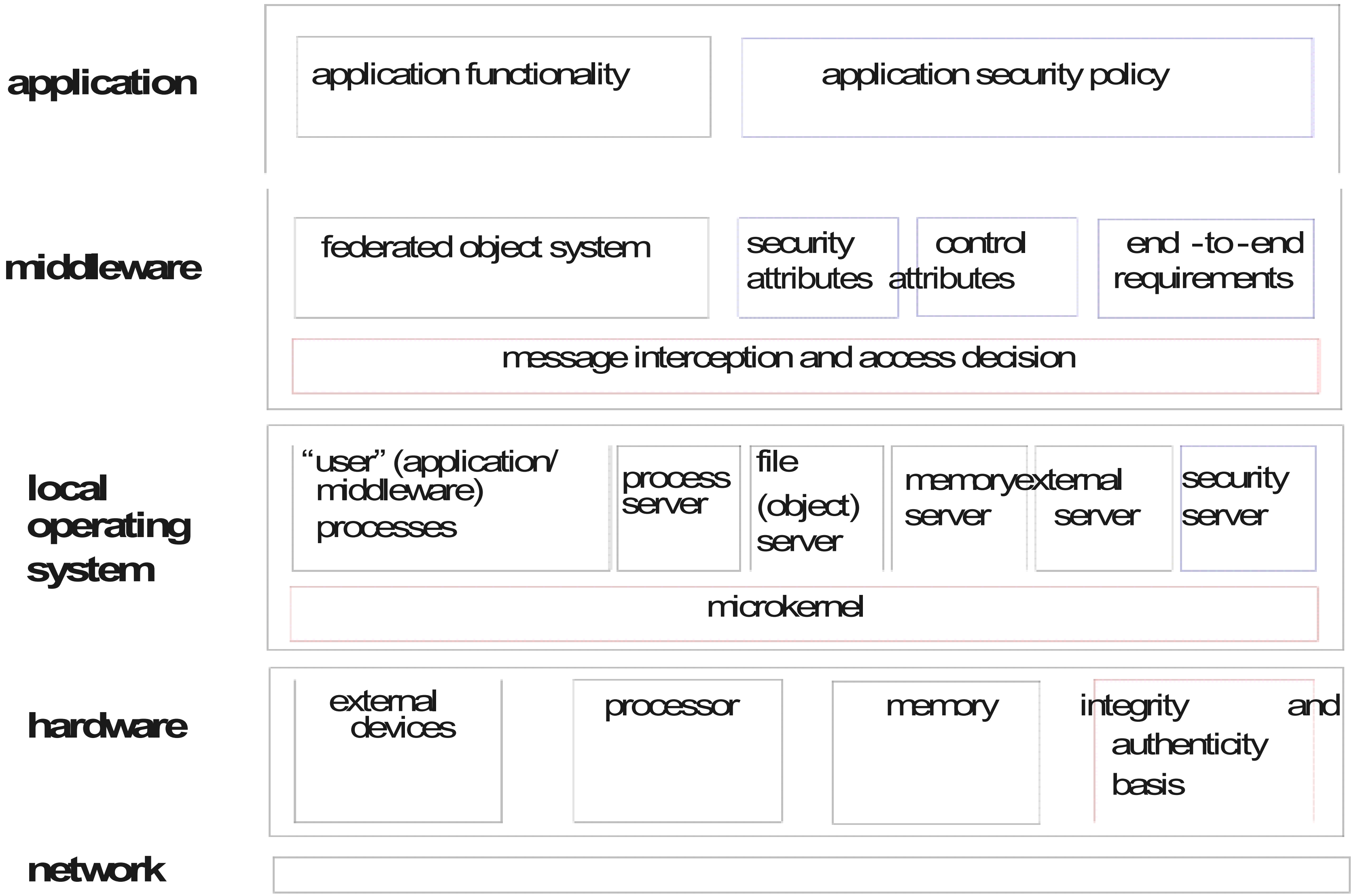
Acl(data_file) = { [user,read], [application,read], [application,write] }

Acl(recovery_file) = { [user,write], [application,read] }

11) Mandatory Access Control and Security Levels



12) Layered Design Including Certificates and Credentials



application:
- permissions
- prohibitions

session:
- fault-tolerance
- authenticity
- access rights
- non-repudiation
- accountability
- confidentiality

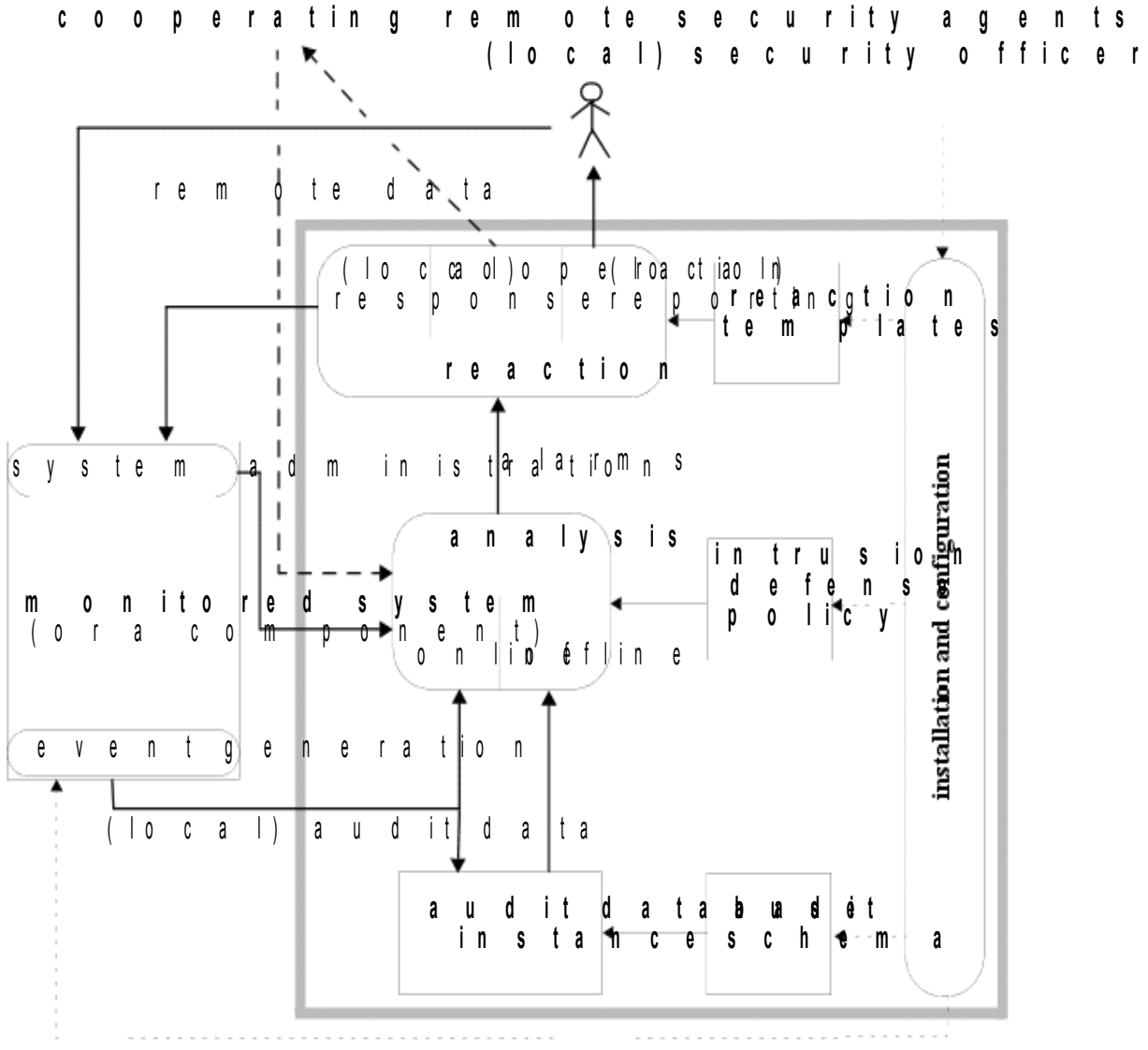
transport:
- packets

network:
- routing

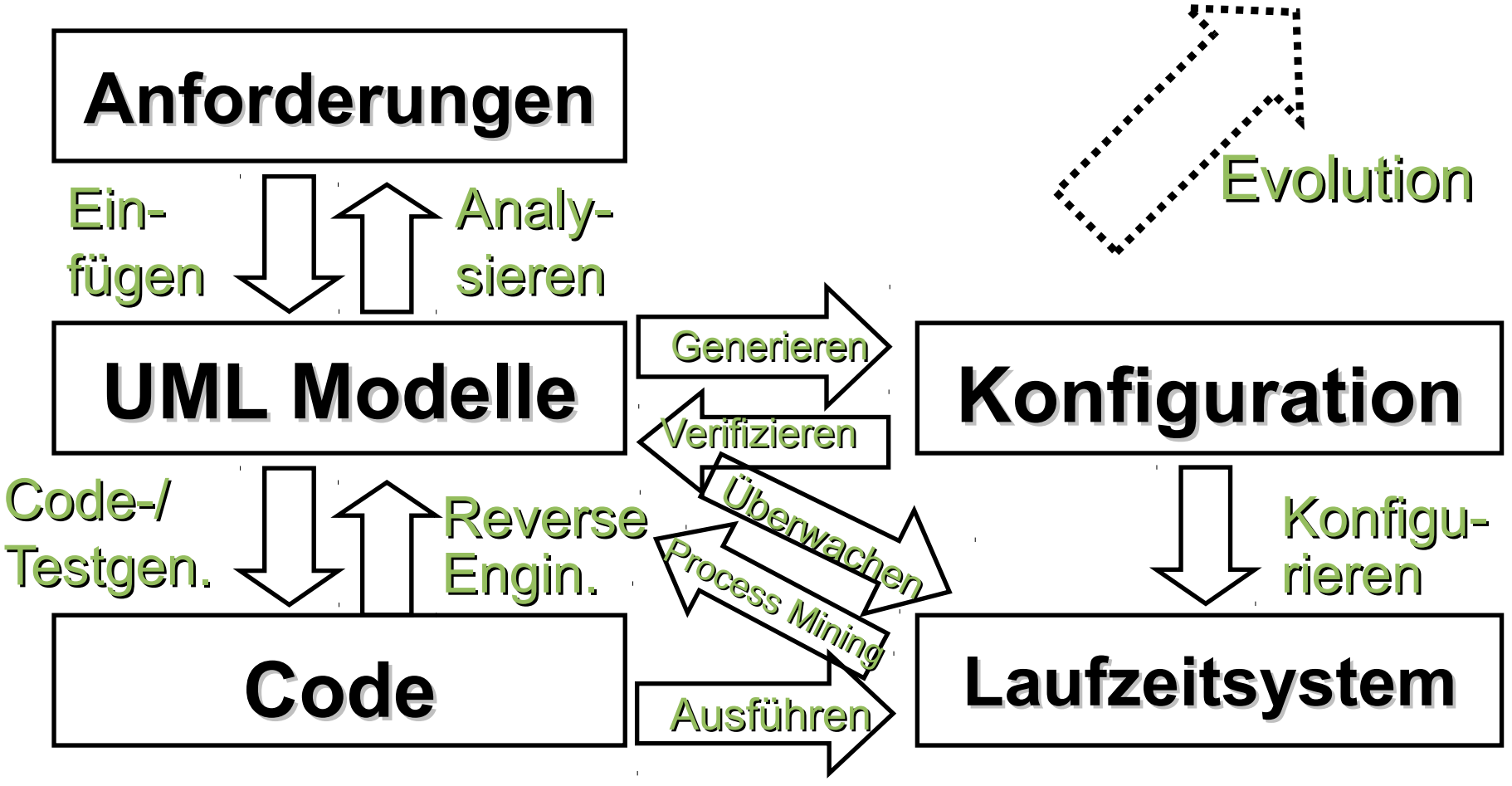
datalink:
- frames

physical:
- bits

13) Intrusion Detection and Reaction



14) Modellbasierte Sicherheit



15) Praxisbeispiele

Wie oben erwähnt:

- Elektronische Geldbörse (Visa)
- Biometrische Authentifikation (xxx)
- Mobile Kommunikation (O2)
- Informationssystem (BMW)
- Internetbank-Architektur (HypoVereinsbank)
- Gesundheitskarte
- Clouds

Literatur

Teil 1-13):

- Joachim Biskup: „Security in Computing Systems: Challenges, Approaches and Solutions“, Springer-Verlag 2009

Teil 14-15):

- Jan Jürjens: „Secure Systems Development with UML“, Springer-Verlag 2005

Beide Lehrbücher sind in ausreichender Anzahl in der Uni-Bibliothek vorhanden (inkl. Lehrbuchsammlung); bitte informieren Sie mich, falls sich ein Engpass in der Ausleihe ergeben sollte (ggf. können relevante Auszüge zur Verfügung gestellt werden).