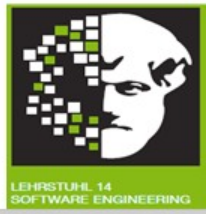

Willkommen zur Vorlesung

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

Security requirements: Secure Information Flow

- A traditional way of ensuring security in computer systems is to design **multi-level secure**[1] systems.
- In such systems, there are different levels of sensitivity of data.
- For simplicity, one usually considers two security levels: **high**, meaning highly sensitive or highly trusted, and **low**, meaning less sensitive or less trusted.
- Where trusted parts of a system interact with untrusted parts, one has to ensure that there is no indirect leakage of sensitive information from a trusted to an untrusted part.

[1] L. J. LaPadula and D. E. Bell. Secure computer systems: A mathematical model. Technical report, The MITRE Corporation, 1973. Reprinted in Journal of Computer Security, 4:239-263, 1996.

Fundamental aspects of security

- *security* is a comprehensive property
- *security* design reflects the *interests* of *participants*
- *conflicts* must be balanced
- *security requirements* identify *informational activities* and their *threats*
- *security mechanisms* aim at
  - *preventing* security violations
  - *limiting* the damage caused by violations
  - *compensating* their consequences

Information flow

- a transmitted message,
  seen as a string (of letters and, ultimately, of 0's and 1's),
  is not necessarily *meaningful* concerning content
  for a receiver or any other *observer*
- it may happen and can even be sensible that an observed string appears random and without information:
  from the point of view of the observer,
  the message transmission has *not* caused an information flow
- in other cases, an observer succeeds in
  assigning a meaning to the observed string,
  roughly in the following sense:
  he determines an assertion
  expressing the truth of some aspect of his considerations;
  if, additionally, the observer has newly learnt this truth,
  then the message transmission has caused
  an *information flow* from the observer's point of view

Information flow and message transmission

- a message transmission does not necessarily cause an information flow for any observer
- sometimes an observer has to infer implications in order to let a message transmission appear as an information flow from his point of view
- for such an inference, the observer can exploit a priori knowledge such as a previously acquired key
- for an actual inference, the observer needs appropriate computational means

Security interests: an expanded list

- availability
- integrity: correct content
- integrity: unmodified state
- integrity: detection of modification
- authenticity
- non-repudiation
- confidentiality
- non-observability
- anonymity
- accountability
- evidence
- integrity: temporal correctness
- separation of roles
- covert obligations
- fair exchange
- monitoring and eavesdropping

Basic security interests

- *availability* of data and activities
- *confidentiality* of information and actions
- *integrity* of the computing system
- *authenticity* of actors
- *non-repudiation* of their actions

Autonomy and cooperation: classification of security interests

Interest	Autonomy	Cooperation
availability	•,+	+,•
integrity: correct content	•	•
integrity: unmodified state	•	•
integrity: detection of modification	+	•
authenticity	+	•
non-repudiation	•,+	+
confidentiality	+	•
non-observability	+	•
anonymity	+	•
accountability	–,•	+
evidence	•,+	+
integrity: temporal correctness	+	•
separation of roles	+	•
covert obligations	+	•
fair exchange	+	•
monitoring and eavesdropping	–	+