Practical Security Analysis and Economics of Information Security

Jan Willemsen

September 12, 2007
What is Security?

- Definition 1: Security is a situation where nothing bad can happen

However, achieving such a situation would require potentially infinite amount of resources. Would you buy meteorite insurance? Thus we need to define security in economical terms.

- Definition 2: Security is a situation where all risks are taken down to the level where the expected loss is economically acceptable.
What is Security?

- Definition 1: Security is a situation where nothing bad can happen
- However, achieving such a situation would require potentially infinite amount of resources
  - Would you buy meteorite insurance?
What is Security?

- **Definition 1:** Security is a situation where nothing bad can happen.
- However, achieving such a situation would require potentially infinite amount of resources.
  - Would you buy meteorite insurance?
- Thus we need to define security in economical terms.
- **Definition 2:** Security is a situation where all risks are taken down to the level where the expected loss is economically acceptable.
Are We Secure?

- In order to take decisions about security, one needs to
  - evaluate the assets
  - write down possible attack scenarios
  - evaluate different parameters of the attacks (cost, probability, penalties, ...)
  - compute the expected result for the attacker
Are We Secure?

- In order to take decisions about security, one needs to
  - evaluate the assets
  - write down possible attack scenarios
  - evaluate different parameters of the attacks (cost, probability, penalties, ...)
  - compute the expected result for the attacker

- If this outcome is negative we can hope that a rational attacker would not attack
An Attack Tree

Forestalling
Release

The code is
stolen

The code is
completed
to product

FR via bribing
a programmer

FR via network
attack

FR via physical
robery

Bribe a
programmer

Programmer
obtains
the code

Employ a
hacker

Hacker
exploits
a bug

There is a
bug in the
computer
system

Employ a
robber

Robber
breaks into
the system,
obeing the
code
Possible Topics

▶ Developing the attack tree framework
  ▶ Introducing new types of nodes
  ▶ Developing the attacktree software further (node types, interval estimations, functional estimations)
  ▶ Studying the role of different parameters
  ▶ Studying the Mauw&Oodstijk framework

▶ Case study – working through some real examples and analyzing the trees