Security Engineering
Part I – Overview

Juan E. Tapiador

jestevez@inf.uc3m.es

Department of Computer Science, UC3M

Security Engineering – 4th year BSc in Computer Science, Fall 2011

So what's SE?

"SE is about building systems to remain dependable in the face of malice, error, or mischance."

Anderson, *Security Engineering, Chap. 1*

Why SE is hard:

- Cross-disciplinary expertise
- Its not just **safety**: key aspect is the analysis of **malice**:
  - *Dealing with* **strategic** *attackers is the domain of security*
- Many systems have critical assurance requirements
- Reality is very complex (we'll come back to this shortly)

Three short exercises

E1: Attacking combination door locks

E2: Forging a bank card

E3: Liars

Reality is very complex

1. Security requirements greatly differ from system to system.
2. Security provided through combination of many primitives and protocols.
3. Protecting the wrong things
4. Protecting the right things in the wrong way.
5. A chain is only as strong as its weakest link.
6. Security is a process, not a product.
7. Systems increasingly complex.
8. Systems increasingly interconnected and interdependent.
9. Unexpected behaviour: Unforeseen things happen.
10. Vulnerabilities are out there.

It's all about tradeoffs

The **project triangle** (engineering): *Your are given three options: Fast, Good, Cheap, and told to choose any two.*

Fact: You can't optimize everything simultaneously.

Q1: *Why not?*

In general we'll have tradeoffs involving:

- Cost
- Performance
- Usability
- **Security**

with $\uparrow$ security $\Rightarrow$ $\uparrow$ cost, $\downarrow$ performance, $\downarrow$ usability

Security all the way through

Traditional systems life cycle, in strict order:

1. Functionality
   - *Or, make it fly!*
2. Interoperability
   - *Or, make it work with everything else!*
3. Security (+Non-functional criteria: Quality, etc.)
   - *Or, make it "better"*

Now: Security across all life stages, from specification, analysis and design to implementation and evolution.

Ten SE principles

1. Economy: *Simplicity vs complexity*
2. Security by default: *Everything is forbidden unless explicitly stated otherwise*
3. Full mediation: *Every access must be checked against policy*
4. Open design: *No security through obscurity*
5. Separation of duty: *E.g., security admin. vs systems admin.*
6. Minimum privilege: *Always work on a need-to-know basis.*
7. Minimum common mechanisms: *Diversity!*
8. User aceptability: *From interfaces to psychology and HHRR*
9. Proporcionality: *Security cost vs Loss cost*
10. Audit: *As much as you can afford*

Assets

What things must be protected?

- Hardware
- Software
- Data

Q2: *Is that all?*

Data security (informal):

- Keep secret stuff secret $\Rightarrow$ **confidentiality**
- Prevent unauthorised modifications $\Rightarrow$ **integrity**
- Data should be accessible when needed $\Rightarrow$ **availability**

More terms

- Privacy
- Anonymity
- Vulnerability + Threat $\Rightarrow$ Security failure
- Attack
- Security policy

The threat within

The human factor: users, IT staff, security staff, ...

- **Negligency** / **stupidity** / **ignorance**

  > "There's no device known to mankind that will prevent people from being idiots"
  >
  > Mark Rasch, director of network security and privacy consulting for Falls Church

  > "There is more stupidity than hydrogen in the universe"
  >
  > Frank Zappa

- 2007 – A CCOO (Spanish union) employee inadvertely shares all the files in his computer through eMule, including DB with sensitive data about 20000+ union members.
- 2008 – Same story in an abortion practice: personal records of 4000+ patients are leaked out.

The threat within (cont.)

The human factor: users, IT staff, security staff, ...

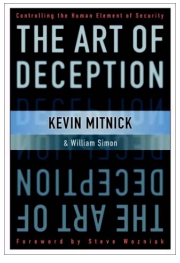
- **Insiders** – Diverse motivations:
  - Vengeance by resented / disgruntled employees
  - Financial problems
  - Bribed by adversaries / competitors
  - About to move to a new (though related) job
- This is one of the most serious threats!
- Insider Threat Study (US SS & CMU – sabotage across US critical infrastructures). Key findings:
  - 81% of organisations experienced negative financial impact, from $500 to tens of millions.
  - 75% had some impact in their business operations
  - 28% lost reputation

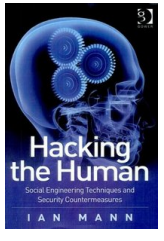
The threat within (cont.)

- Key findings (cont.):
  - 57%-92% attackers motivated by negative work-related event (disgruntled, termination, transfer, ...)
  - 80% exhibited concerning behaviour prior to the attack (tardiness, truancy, poor job performance, arguments with coworkers, ...)
  - 86% had technical positions. 90% had privileged system access when hired.
  - The majority attacked following termination, even if they no longer had authorised access:
    - → backdoor accounts
    - → ran a password cracker before leaving
    - → took advantage of inefective security controls in termination processess
    - → exploited gaps in the organisation's access controls

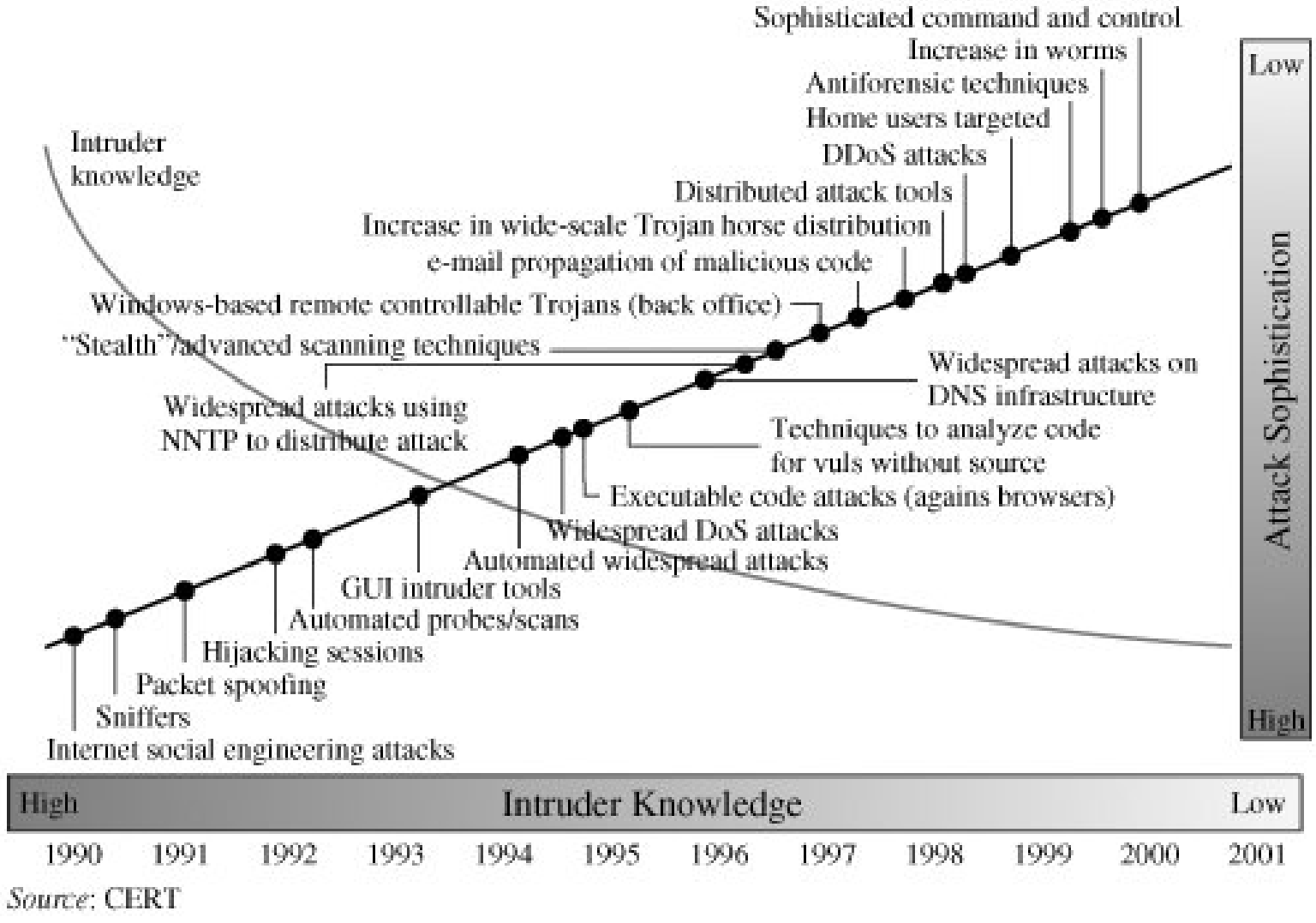
External adversaries

- **Q3**: *Who?*
- **Q4**: *Why?*
- How?
  - Tools:
    - → Scanners, sniffers, keyloggers, spoofers, password crackers, exploitation of vulnerabilities, spyware, session hijackers, rootkits, malware, ...
    - → Automated attacks
  - Social engineering.
    - → Phishing. See e.g.:
      `www.banksafeonline.org.uk/phishing_examples.html`
      `www.hmrc.gov.uk/security/examples.htm`
    - → Exploit security unawareness
    - → Exploit human (psychological) weaknesses





Attack sophistication vs Intruder knowledge



Source: CERT

Security measures

- Evolution:
  - Physical security
  - Technical measures
  - Security management / governance
    - → Externalisation
- Types:
  - Prevention • Detection • Correction
- Also legal measures:
  - Privacy / data protection
  - Identification and data retention

Technical measures

Security goals:

- Identification
- Autentication
- Information flow ("access") control
- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Audit

Security management

- When possible, run by a specific security department
  - Separate from IT staff!
- Functions:
  - Generate security and business continuity plans
  - Risk analysis
  - Security products – assess, buy/develop, configure
  - Penetration tests
  - Maintain security awareness