Introduction

Security:
Objectives

▷ Defense against non-authorized activities (adversaries)
  - Initiated by someone "from inside"
  - Initiated by someone "from outside"

▷ Types of illegal activities:
  - Access to information
  - Information modification
  - Resource usage
    - CPU, memory, printer, network, etc.
  - Denial of Service (DoS)
  - Vandalism
    - Interference with the normal system behavior without any benefit for the attacker

Security in computing systems: Complex problems

▷ Computers can do a lot of damage in a short time frame
  - They manage an always growing amount of data/information
  - They process and communicate very fast

▷ The number of weakness is always growing
  - Systems are getting more complex with time
  - Time-to-market is each time shorter

▷ Networks allow:
  - Anonymous (?) attacks from anywhere
  - Automatic propagation of cyberplagues
  - The existence and exploitation of hostile hosts and applications

▷ In general users are not careful
  - Because they are not aware of the problems and solutions
  - Because they take risks

Security: Pragmatic approach

▷ There will never be a 100% protection
  - Cost-efficiency balance

▷ Security is expensive
  - Dedicated technology, skilled people
  - Use only the minimum required

▷ Protection, value e punishment
  - Good protection for the most frequent attacks
  - Less interference with daily work than the damage caused by attackers
  - Police and courts for tracking and prosecuting attackers
    · It is critical to avoid the notion of total impunity

Security lexicon

▷ Vulnerability
  - A system weakness that makes it sensible to attacks
  - Design / development / installation

▷ Attack
  - A set of steps that lead to the execution of illegal activities
    - Usually exploiting vulnerabilities

▷ Risks / threats
  - Damage resulting from an attack

▷ Defense
  - Set of policies and mechanisms aiming at
    - Reducing the amount of vulnerabilities
    - Detect as fast as possible actual and past attacks
    - Reduce the risks of systems

Hackers, crackers and hats

▷ Hacker
  - Someone with high skills to overcome barriers and set complex things to work

▷ Cracker
  - Hacker that is an attacker, a malicious adversary

▷ Black hat
  - A hacker with a malicious goal

▷ White hat
  - A hacker that is payed for discovering problems

▷ Ethical hacker
  - A pro bono white hat

Security risks

▷ Information, time and money
  • Destruction or tampering of information

▷ Confidentiality
  • Non-authorized access to information

▷ Privacy
  • Non-authorized gathering of personal information
  • Data warehousing on personal information

▷ Resource availability
  • Disruption of computing systems / networks

▷ Impersonation
  • Of people / of services
  • Non-authorized exploitation of personal accounts / profiles

---

Main vulnerability sources

"Tech support says the problem is located somewhere between the keyboard and my chair."

▷ People
  • Ignorant or careless
  • Hostile

▷ Applications with bugs
  • Root kits help newcomers to exploit well-known vulnerabilities

▷ Malware
  • Trojan horses, worms, virus

▷ Defective administration
  • Systems get more complex as they evolve
  • Security restrictions vs. flexible operation
    · Most people cannot understand security jargon in order to manage security configurations
    · Default configurations may not be the most secure ones

▷ Communications over uncontrolled/unknown/unsafe network links

Security:
Dimensions to consider
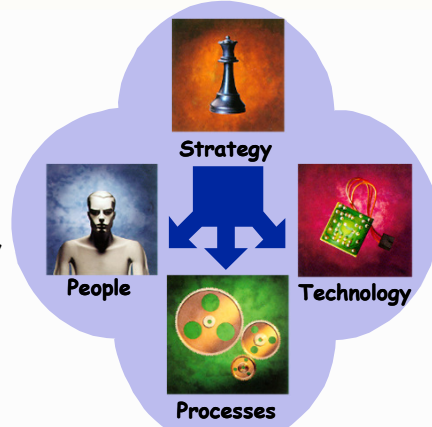

Strategy

People

Technology

Processes

- Training
- Awareness
- Organization of security

- Security policies
- Security administration processes
- Continues evolution of auditing and follow-up processes

- Vulnerability scanning
- Firewalls
- Authentication
- Access Control
- Auditing
- Cryptography
- Digital signatures
- Certification authorities
- Certification hierarchies
- Etc.

© André Zúquete /
João Paulo Barraca

Security

9

Security policies

▷ Define the power of each and every subject
  - Least privilege principle
  - Hardening

▷ Define security procedures
  - Who does what in which circumstances

▷ Define the minimum security requirements of a domain
  - Security levels
  - Authentication requirements
    - And related minimum authentication requirements
    - Strong/weak, single/multi-factor, remote/face-to-face

▷ Define defense strategies and fight-back tactics
  - Defensive architecture
  - Monitoring of critical activities or attack signs
  - Reaction against attacks or other abnormal scenarios

▷ Define the universe of legal and illegal activities
  - All that is not forbidden is allowed
 - All that is not allowed is forbidden

© André Zúquete /
João Paulo Barraca

Security

10

Security mechanisms

▷ Mechanisms implement policies
  - Policies define, at an higher level, what needs to be done
  - Mechanisms are used to deploy policies

▷ Generic security mechanisms
  - Confinement (sandboxing)
  - Authentication
  - Access control
  - Privileged execution
  - Filtering
  - Logging
  - Inspection
  - Auditing
  - Cryptographic algorithms
  - Cryptographic protocols

http://devhumor.com/media/human-error-dave
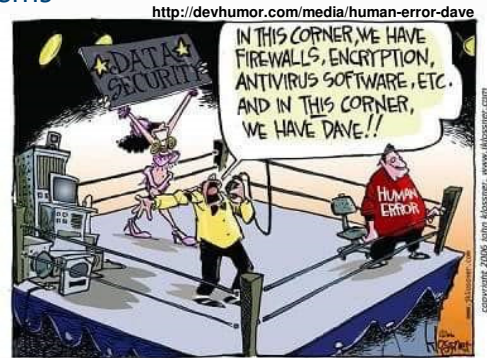
© André Zúquete /
João Paulo Barraca

Security

11

Security level offered by a computer

▷ Depends on:
  - Available security policies
  - Correctness and effectiveness of their specification / implementation

▷ Evaluation criteria:
  - NCSC Trusted Computer System Evaluation Criteria (TCSEC, Orange Book)
    - Classes: **D**, **C** (1, 2), **B** (1, 2, 3) e **A** (1)
    - D: insecure (minimum protection level)
    - A1: most secure
      - Very demanding and expensive protection policies
      - Formal validation of specification
      - Highly supervised implementation
  - EC Information Technology Security Evaluation Criteria (ITSEC)
    - Levels: **E1** to **E6**
      - Formal specification level
      - Correctness of implementation

© André Zúquete /
João Paulo Barraca

Security

12

Security policies for distributed systems

▷ Must encompass several hosts and networks
  - Security Domains
    - Definition of the set of hosts and networks of the domain
    - Definition of the set of accepted/authorized users
    - Definition of the set of accepted/not accepted activities
  - Security gateways
    - Definition of the set of allowed in-out interactions

▷ Perimeter defense vs. Defense in depth

Attacks to distributed systems

▷ Attacks to hosts
  - Stealing
  - Intrusion
  - Impersonation (of users)
  - Denial of service

▷ Attacks to networks
  - Packet inspection
  - Packet tampering / injection
  - Traffic interception
  - Traffic replaying
  - Host impersonation
  - Denial of service (jamming, flooding, deception, etc.)

▷ Other
  - Covert channels

"On the Internet, nobody knows you're a dog."

Attack models

▷ Generic, autonomous attacks
  - Conceived for exploiting well-known, common vulnerabilities
  - Coded for many scenarios and targets
    - e.g. phishing
  - Mean survivability time
    - Time between two consecutive automatic attacks
    - There are "network sensors" that help to compute it

▷ Target-specific attacks
  - Conceived for a particular person / host / network
    - e.g. spear-phishing
  - Idealized and conducted in real-time by specialists
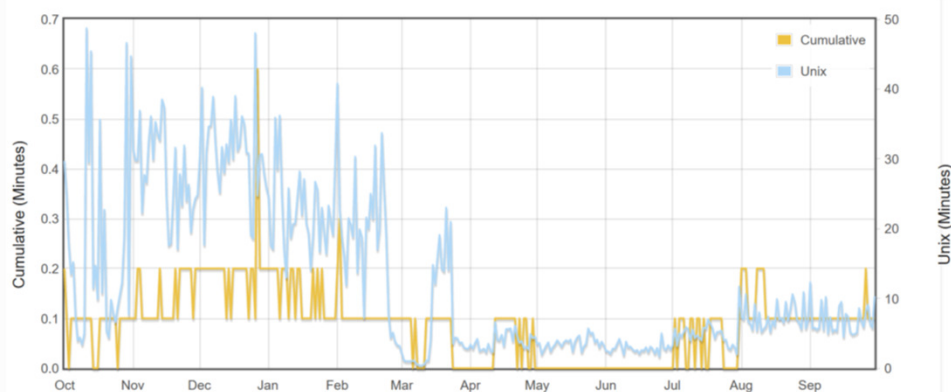
Mean survival time
(http://isc.sans.org/survivaltime.html)
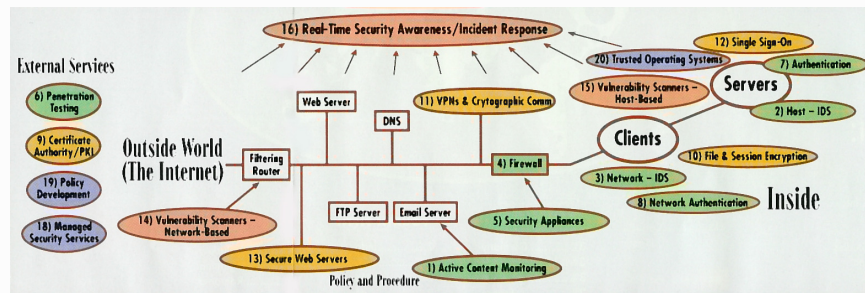
Security:
Mechanisms for distributed systems (1/5)

Security:
Mechanisms for distributed systems (2/5)

▷ Trusted Operating Systems
- Security levels, certification
- Secure execution environments for servers
- Sandboxing / virtual machines

▷ Firewalls & Security Appliances
- Traffic control between networks
- Monitoring (traffic load, etc.)

▷ Secure communications / VPNs
- Secure channels over insecure, public networks
- Secure extension of organizational networks

Security:
Mechanisms for distributed systems (3/5)

▷ Authentication
  - Local
  - Remote (network authentication)
  - Single Sign-On

▷ Certification Authorities / PKI
  - Management of public key certificates

▷ Encryption of files and sessions
  - Privacy / confidentiality of network data
  - Privacy / confidentiality of long-term stored data

Security:
Mechanisms for distributed systems (4/5)

▷ Intrusion detection
  - Detention of forbidden / abnormal activities
  - Network-Based / Host-based

▷ Vulnerability scanners
  - Scanning for problem fixing or exploitation
  - Network-based / Host-based

▷ Penetration testing
  - Vulnerability assessment
  - Demo penetration attempts
  - Testing of installed security mechanisms
  - Assessment of badly implemented security policies

Security:
Mechanisms for distributed systems (5/5)

▷ Content monitoring
  ◆ Detection of virus, worms or other cyber plagues

▷ Security administration
  ◆ Development of security policies
  ◆ Distributed enforcement of policies
  ◆ Co-administration / outsourcing of security services

▷ Real-Time Security Awareness / Incident Response
  ◆ Capacity to detect and react to security incidents in real-time
  ◆ Means for a rapid and effective incident reaction

Security

21

11