

Computer System Security and Management

D0004E

Lecture 1: Introduction [ch.1 & 2]
Paweł Pietrzak



Administrative Details

Teachers

- Paweł Pietrzak
 - Office: A2304
 - Email: pawel.pietrzak@lth.se
- Rumen Kyusakov
 - Office: A2307
 - Email: rumen.kyusakov@lth.se
- Örjan Tjernström (labs Skellefteå)
 - E-mail: ortje@lth.se

D0004E, 2011-12

Course Homepage

<http://www.sm.luth.se/csee/courses/d0004e>

or google for D0004E

D0004E, 2011-12

Lectures

- Currently scheduled
 - (not quite) "evenly" spaced throughout the quarter
 - 12 + 1 in total, including one for repetition

D0004E, 2011-12

Methods of Assessment

- Written exam
 - 3hp
- Lab work
 - 4.5hp
 - deadlines
 - Sept 15, Oct 4, Oct 19
 - final lab examination Oct 24-25

D0004E, 2011-12

Grading

- Grade requirements:
 - 3) Mandatory lab assignments + written exam
 - 4) Everything for 3) and 3 extras
 - 5) Everything for 3) and 6 extras
- ECTS grades: see the lab page

D0004E, 2011-12

Lab Assignments

- Work in pairs
- Each group has 3 machines
- Dedicated lab setups in A1203

D0004E, 2011-12

Lab setup

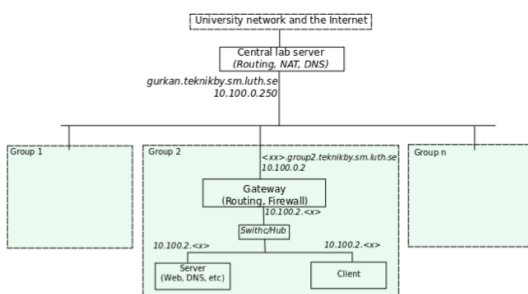


Figure 1: Labs setup overview

D0004E, 2011-12

Lab Assignments #2

- Form lab groups
- This is a course where your hands will get dirty
- You are expected to spend a lot of time in A1203, not only when we are there

D0004E, 2011-12

Lab Assignments #3

- The scheduled labs are there so you can ask questions
- You are expected to solve the extras without much guidance
- Access Code to A1203

D0004E, 2011-12

Policies

- All deadlines are firm
- Standard guidelines for academic integrity:
 - Discussion is good, copying files is not!
 - Items turned in should be your groups individual work
 - Violations will be reported to the disciplinary board

D0004E, 2011-12

Prerequisites

- Some programming experience
- A basic familiarity with the UNIX environment
- Basic knowledge of computer communication
- No previous experience of system administration nor security is required

D0004E, 2011-12

Small hints

- Always include some details of your method and/or an explanation:
 - To demonstrate your understanding of concepts
 - To show your problem solving skills in what you have learned
- Stating only the final answer may not result in full credit

D0004E, 2011-12

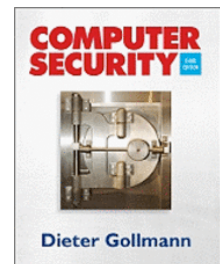
Failing

- New chance for lab assignments is next time the course is given.
- New chance for the exam is next time the exam is given.

D0004E, 2011-12

Course Literature

- Dieter Gollmann
Computer Security.
John Wiley And Sons
Ltd; 2nd revised ed.

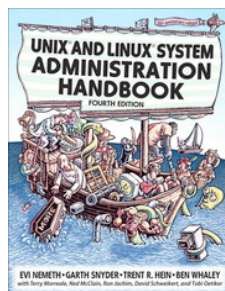


Additional literature

Evi Nemeth, Garth Snyder,
Trent R Hein, Ben Whaley

**Unix and Linux System
Administration Handbook.**

PRENTICE-HALL; 4th
edition.



Intro and Course Outline

Outline

- System administration
 - Unix
 - Networking
 - Storage/backup
- Security
 - Authorization and authentication
 - Keys
 - Web security
 - Cryptography
 - Software security

D0004E, 2011-12

What does System Administrator do?



D0004E, 2011-12

What does System Administrator do?

- no precise job description
- often learned by experience
- make things run
- might be referred to as Operator, Network Administrator, System Programmer, System Manager, Service Engineer, Site Reliability Engineer etc.

D0004E, 2011-12

Typical duties (after Wikipedia)

- Analyzing system logs and identifying potential issues with computer systems.
- Introducing and integrating new technologies into existing data center environments.
- Performing routine audits of systems and software.
- Performing backups.
- Applying operating system updates, patches, and configuration changes.
- Installing and configuring new hardware and software.
- Adding, removing, or updating user account information, resetting passwords, etc.
- Answering technical queries.
- Responsibility for security.
- Responsibility for documenting the configuration of the system.
- Troubleshooting any reported problems.
- System performance tuning.
- Ensuring that the network infrastructure is up and running.

D0004E, 2011-12

In short

- If everything works smoothly nobody notices existence of an SA. If something crashes then.... :)

D0004E, 2011-12

The powers

Possibilities

- Read any file
- Write any file
- Becoming any user
- Remove or edit logs

D0004E, 2011-12

With great power
comes great
responsibility

Expected behavior



D0004E, 2011-12

Expected behavior

- Do not read files without the users consent
- Mail is no exception!
- Abuse tracking might be an exception. Do not place the decision on the individual sysadmin.

D0004E, 2011-12

Free information

- Man pages, "man -k <keyword>" or "apropos keyword"
- Google.
- The Linux documentation project:
<http://www.tldp.org>
- Vendor documentation

D0004E, 2011-12

Security
- a bit of history

Introduction

- Security is a journey, not a destination.
- The challenges keep changing.
- So have the answers to familiar challenges.
- Security mechanisms must be seen in the context of the IT landscape they were developed for.

D0004E, 2011-12

Timeline

- 1930s: people as “computers”
- 1940s: first electronic computers
- 1950s: start of an industry
- 1960s: software comes into its own
- 1970s: age of the mainframe
- 1980s: age of the PC
- 1990s: age of the Internet
- 2000s: age of the Web

D0004E, 2011-12

1970s: Mainframes – Data Crunchers

- Technology: Winchester disk (IBM) 35–70 megabytes memory.
- Application: data crunching in large organizations and government departments.
- Protection of classified data in the defense sector dominates security research and development.
- Social security applications and the like.
- Security controls in the system core: operating systems, database management systems
- Computers and computer security **managed by professionals**.

D0004E, 2011-12

1970s: Security Issues

- Military applications:
 - Anderson report
 - Multi-level security (MLS)
 - Bell LaPadula model
- Status today: High assurance systems developed (e.g. Multics) but do not address today’s issues.
- Non-classified but sensitive applications
 - DES, public research on cryptography
 - Privacy legislation
 - Statistical database security
- Status today: cryptography is a mature field, statistical database security reappearing in data mining.

D0004E, 2011-12

1980s: PCs – Office Workers

- Technology: Personal Computer, GUI, mouse, ...
- Application: word processors, spreadsheets, i.e. office work.
- Liberation from control by the IT department.
- Single-user machines processing unclassified data: No need for multi-user security or for MLS.
- Risk analysis: no need for computer security.
- Security evaluation: Orange Book (TCSEC, 1983/85): Driven by the defense applications of the 1970s.

D0004E, 2011-12

1980s: Security Issues

- Research on MLS systems still going strong; Orange Book, MLS for relational databases.
- Clark-Wilson model: first appearance of “commercial security” in mainstream security research.
- Worms and viruses: research proposals, before appearing in the wild.
 - Also the worm comes from Xerox park (1982) ...
- Intel 80386 drops support for segmentation.

D0004E, 2011-12

1990s: Internet – Surfers Paradise?

- Technology: Internet, commercially used.
- Applications: World Wide Web (static content), email, entertainment (music, movies), ...
- Single-user machine that had lost its defenses in the previous decade is now exposed to the “hostile” Internet.
- No control on who can send what to a machine on the Internet.

D0004E, 2011-12

1990s: Security Issues

- Crypto wars: is wide-spread use of strong cryptography a good idea?
 - Internet security treated as a communications security problem.
- Buffer overrun attacks:
 - Aleph One: Smashing the Stack for Fun and Profit
 - Internet security is mainly an end systems issue!
- Java security model: the sandbox.
- Trusted Computing; DRM (digital rights management)
- Status today: mature security protocols (IPsec, SSL/TLS), better software security.

D0004E, 2011-12

2000s: Web – e-Commerce

- Technology: Web services, WLAN, PKI??
- Web 2.0: dynamic content
- B2C applications: Amazon, eBay, airlines, on-line shops, Google, ...
- Criminal activity replaces “hackers”.
- Legislation to encourage use of electronic signatures.
- PKIs have not taken off; e-commerce has essentially evolved without them.

D0004E, 2011-12

2000s: Security Issues

- SSL/TLS for secure sessions.
- Software security: the problems are shifting from the operating systems to the applications (SQL injection, cross-site scripting).
- Security controls moving to application layer: Web pages start to perform security checks.
- Access control for virtual organizations: e.g. federated identity management.
- Security of end systems managed by the user.

D0004E, 2011-12

Managing Security

Insider Fraud

- Programmer writing code for a bank made the program ignore overdrafts on his account.
- Discovered when the computer broke down and accounts were processed manually.
- Suspended sentence (money repaid).
- Fired, but re-hired as contractor.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

D0004E, 2011-12

Espionage – Identity Fraud

- Setting: competitors **A** and **B** with a common customer **C**; communication by phone to secret (unlisted) phone numbers.
- Employee of **A** finds out about the secret number **C** uses to call **B** (displayed over a terminal).
- Uses this number to ring **B** pretending to be **C**.
- Searches the filesystem, requests code to be sent to his terminal and punched cards to be sent.
- Discovered when **B** asks **C** about the cards and **C** knows nothing about it.
- Believed to be the first case where a warrant was used to search computer memory.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

D0004E, 2011-12

Password Sniffing

- Student wrote program for time-sharing system and left it on disk for curious users.
- On execution the program would “crash” and then ask for username and password.
- Username and password were collected and later used to delete the victims’ files.



From: A.R.D. Norman: Computer Insecurity, Chapman & Hall, 1983

D0004E, 2011-12

Security

- All cases of “security” problems.
- Security covers a wide range of issues; our list of attacks is by no means exhaustive.
- When thinking about security, start from the application, not from the technology.
- Attacks may exploit weak points of the “business model” rather than technical flaws.
- Security problems can rarely be eliminated, but they can be managed.

D0004E, 2011-12

Security

- Systems may fail for various reasons.
- **Reliability** deals with accidental failures.
- **Usability** addresses problems arising from operating mistakes made by users.
- **Security** deals with **intentional** failures: there is at some stage a decision by a person do something he is not supposed to do.
- Reasons: crime, malice, curiosity, stupidity, ...

D0004E, 2011-12

Security is a People Problem

- Technical solutions can only address a part of the problem.
- Technical measures have to be managed in a wider security culture.
- The legal system has to define the boundaries of acceptable behaviour.
- **Social engineering is a powerful attack method.**

D0004E, 2011-12

Security Awareness

- To be effective, security policies must be supported by top management: issue a **security charter**.
 - A crisp document explaining general rules.
- Don't treat users as the enemy: users have to understand that they protect their **own assets**.
- Security awareness programs should be part of the general security strategy.
- Not every member in an organisation has to become a security expert, but all members should know:
 - Why security is important for themselves and for the organisation.
 - What is expected of each member.
 - Which good practices they should follow.

D0004E, 2011-12

The Price of Security

- Price paid for security should not exceed the value of the assets you want to protect.
- To decide what to protect you should perform some kind of risk analysis.
- You have to know your **assets**.
- You have to understand how your assets might be damaged.
- Total cost of security measures goes beyond the cost of "security technology" (e.g. firewalls or intrusion detection systems).

D0004E, 2011-12

Assets

- Hardware: laptops, servers, routers, PDAs, mobile phones, smart cards, ...
- Software: applications, operating systems, database systems, source code, object code, ...
- Data & information: essential data for running and planning your business, design plans, digital content, data about customers, ...
- Services & revenue
- Reputation of enterprise, trust, brand name
- Employees' time

D0004E, 2011-12

Damage

- Disclosure of information, espionage
- Modification of data
- Being unable to do your job because required resources are not available
- Identity spoofing (identity "theft")
- Unauthorised access to services
- Lost revenue
- Damaged reputation
- Theft of equipment
- ...

D0004E, 2011-12

Security policies

- Question: Is this system secure?
- Answer: Wrong question; please be more specific about your protection requirements.
 - Protect PC from virus and worm attacks?
 - No unauthorized access to corporate LAN?
 - Keep sensitive documents secret?
 - Verify identity of partners in a business transaction?
- **Security policies** formulate security objectives.

D0004E, 2011-12

Types of Policies [Sterne]

- **Organisational security policy**: laws, rules, and practices that regulate how an organisation manages and protects resources to achieve its security policy objectives.
 - Organisations must comply with given regulations
- **Automated security policy**: restrictions and properties that specify how a computing system prevents violations of the organisational security policy.
 - A detailed technical specification

D0004E, 2011-12

ISO 27002

1. Risk assessment and treatment
2. Information security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

<http://www.iso27001security.com/html/27002.html>

D0004E, 2011-12

Access Control

- Access control can apply to data, services, and computers.
- Particular attention should be applied to remote access, e.g. through Internet or dial-in connections.
- **Automated security** policies define how access control is being enforced.

D0004E, 2011-12

Risk Analysis

Risk Analysis

- To organize the process of risk analysis, we will look at **assets, vulnerabilities, and threats**.
- Risk is a function of **assets, vulnerabilities, and threats**:
- **Risk = Assets × Threats × Vulnerabilities**
- During risk analysis values are assigned to assets, vulnerabilities, and threats.

D0004E, 2011-12

Vulnerabilities

- Weaknesses of a system that could be accidentally or intentionally exploited to damage assets.
- Typical vulnerabilities in an IT system are:
 - Accounts with system privileges where the default password, such as "MANAGER", has not been changed.
 - Programs with unnecessary privileges or known flaws.
 - Weak access control settings on resources, e.g. having kernel memory world writable.
 - Weak firewall configurations that allow access to vulnerable services.
- Sources for vulnerability updates: CERTs (Computer Emergency Response Teams), SANS, BugTraq, ...

D0004E, 2011-12

Rating Vulnerabilities

- Rate vulnerabilities according to their impact (level of criticality):
 - A vulnerability that allows an attacker to take over a systems account is more critical than a vulnerability that gives access to an unprivileged user account.
 - A vulnerability that allows an attacker to completely impersonate a user is more critical than a vulnerability where the user can only be impersonated in a single specific service.
- **Vulnerability scanners** provide a systematic and automated way of identifying vulnerabilities.
- Some vulnerability scanners also give a rating for the vulnerabilities they detect.

D0004E, 2011-12

Microsoft Severity Rating System

- **Critical:** Exploitation could allow propagation of an Internet worm without user action.
- **Important:** Exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources.
- **Moderate:** Exploitability mitigated to a significant degree, e.g. by default configuration or by auditing.
- **Low:** Exploitation extremely difficult, or impact is minimal.

D0004E, 2011-12

Threats

- **Threats:** actions by adversaries who try to exploit vulnerabilities to damage assets.
- Various ways for identifying threats:
 - Categorize threats by the damage done to assets.
 - Identify source of attacks. Would the adversary be a member of your organisation or an outsider, a contractor or a former member? Has the adversary direct access to your systems or is the attack launched remotely?

D0004E, 2011-12

Attacks

- “materialized threats”
- An attack against an IT system is a sequence of actions, exploiting weak points in the system until the attacker’s goals have been achieved.
- To assess the risk posed by an attack we have to evaluate the amount of damage being done and the likelihood for the attack to occur.
- This likelihood will depend on the attacker’s motivation and on how easy it is to mount the attack.
- In turn, this will further depend on the security configuration of the system under attack.

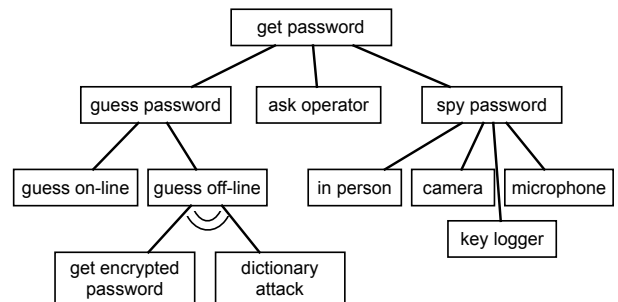
D0004E, 2011-12

Attack Trees

- We can analyze how an attack is executed in detail.
- An attack may start with innocuous steps, gathering information needed to move on to gain privileges on one machine, from there jump to another machine, until the final target is reached.
- To get a fuller picture of potential threats, **attack trees** can be constructed.

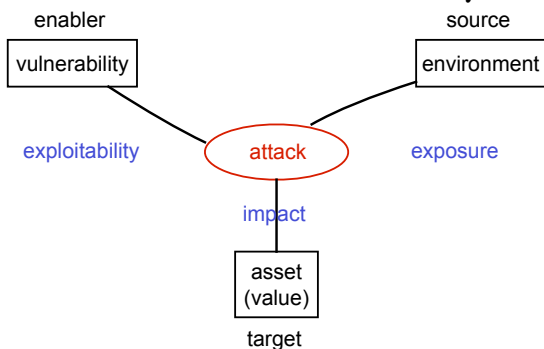
D0004E, 2011-12

Attack Tree - example



D0004E, 2011-12

Factors in Risk Analysis



D0004E, 2011-12

Risk Mitigation

- Risk analysis produces a prioritized list of threats, with recommended countermeasures to mitigate risk.
- Analysis tools usually have a knowledge base of countermeasures for the threats they can identify.
- General risk mitigation strategies:
 - **Accept risk** (and live with it); there may be good reasons to do so.
 - **Avoid risk:** eliminate a vulnerability that causes the risk; drop product feature that has a vulnerability.
 - **Limit risk:** use controls to make a threat less likely.
 - **Transfer risk:** buy insurance.

D0004E, 2011-12