System Architecture & Security

Applied Information Security

SSAS F2016
Søren Debois

About this course

Contents

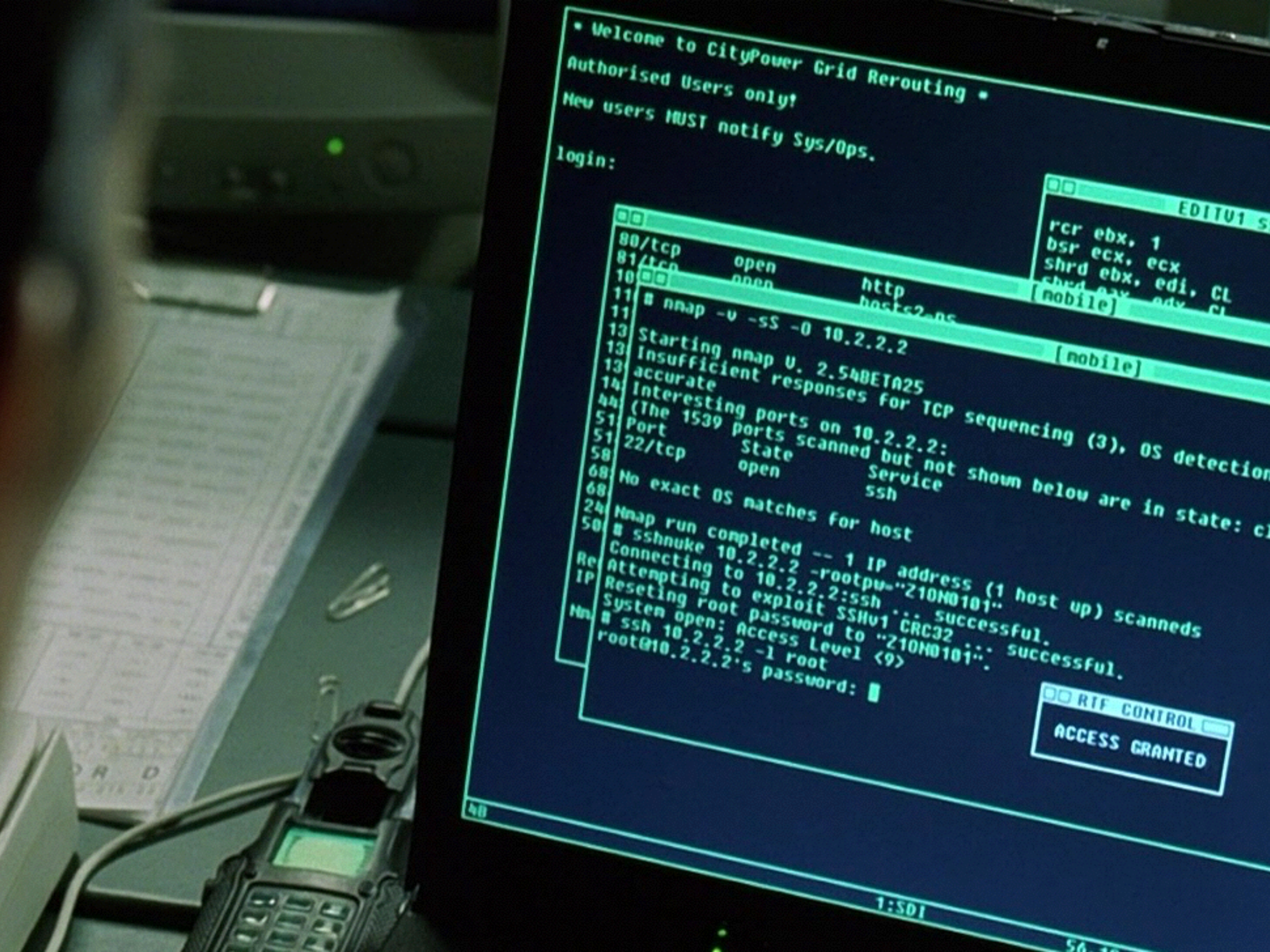
- operating system security (hardening, vulnerability scanning, access control, logging)

- 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.

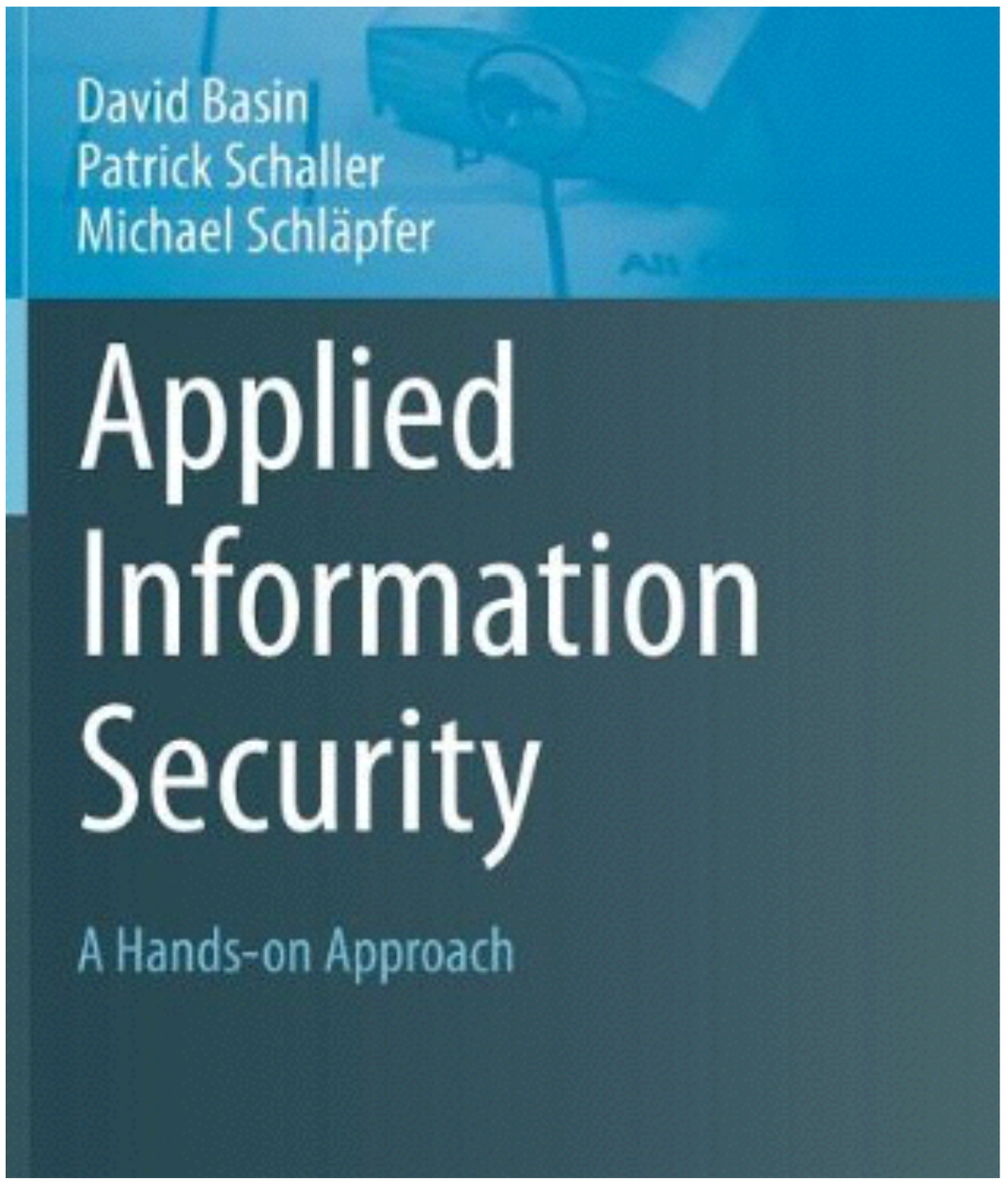

• Welcome to CityPower Grid Rerouting •
Authorised Users only!
New users MUST notify Sys/Ops.
login:
EDITV1
rcr ebx, 1
bsr ecx, ecx
shrd ebx, edi, CL
[mobile]
nmap -v -sS -O 10.2.2.2
Starting nmap V. 2.54BETA25
Insufficient responses for TCP sequencing (3), OS detection
accurate
Interesting ports on 10.2.2.2:
(The 1539 ports scanned but not shown below are in state: c
Port State Service
22/tcp open ssh
No exact OS matches for host
Nmap run completed -- 1 IP address (1 host up) scanneds
sshnuke 10.2.2.2 -rootpw="Z10N0101"
Connecting to 10.2.2.2:ssh ... successful.
Attempting to exploit SSHv1 CRC32 ... successful.
Reseting root password to "Z10N0101".
System open: Access Level <9>
ssh 10.2.2.2 -l root
root@10.2.2.2's password:
80/tcp open http
RTF CONTROL
ACCESS GRANTED
1:501

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 *here*.



“"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

Learning activities

- Lectures
- DIY Security on the command-line
- No exercises—office hours
  (schedule on learnit)
  NB! Not mandatory, but **do come and ask!**
- Mandatory quizzes
- Project (defense)
- Project swap (attack)

Mandatory Activities

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

Security Principles Quiz:	1ST: 12.02 2ND: 19.02
Networking Services Quiz:	1ST: 19.02 2ND: 26.02
Applied Cryptography Quiz:	1ST: 26.02 2ND: 04.03
Authentication & Logging Quiz:	1ST: 04.03 2ND: 11.03
Web Security (1) Quiz:	1ST: 11.03 2ND: 18.03
Web Security (2) Quiz:	1ST: 18.03 2ND: 25.03
Risk Management Quiz:	1ST: 29.03 2ND: 01.04
Computer Forensics Quiz:	1ST: 29.05 2ND: 06.05

System Description and Security Analysis	13.04
Fully functional implementation	15.04
Review Report	06.05

You must attend at least one session of the Project Workshop and the Review Workshops in weeks 16 and 19.

Examination

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

Staff

- Course manager, lecturer: Søren Debois (debois@itu.dk)
- TAs: Robin Bellini Olsson, Nina Holm-Jensen
- Guest lecturer: TBA

Communication

- Lectures (Søren Debois)
- Office hours (Nina, Robin)
- Forum (all)

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 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.

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.”

Confidentiality

- Attacks: *eavesdropping*

- Nets-skandalen (2008-2011)

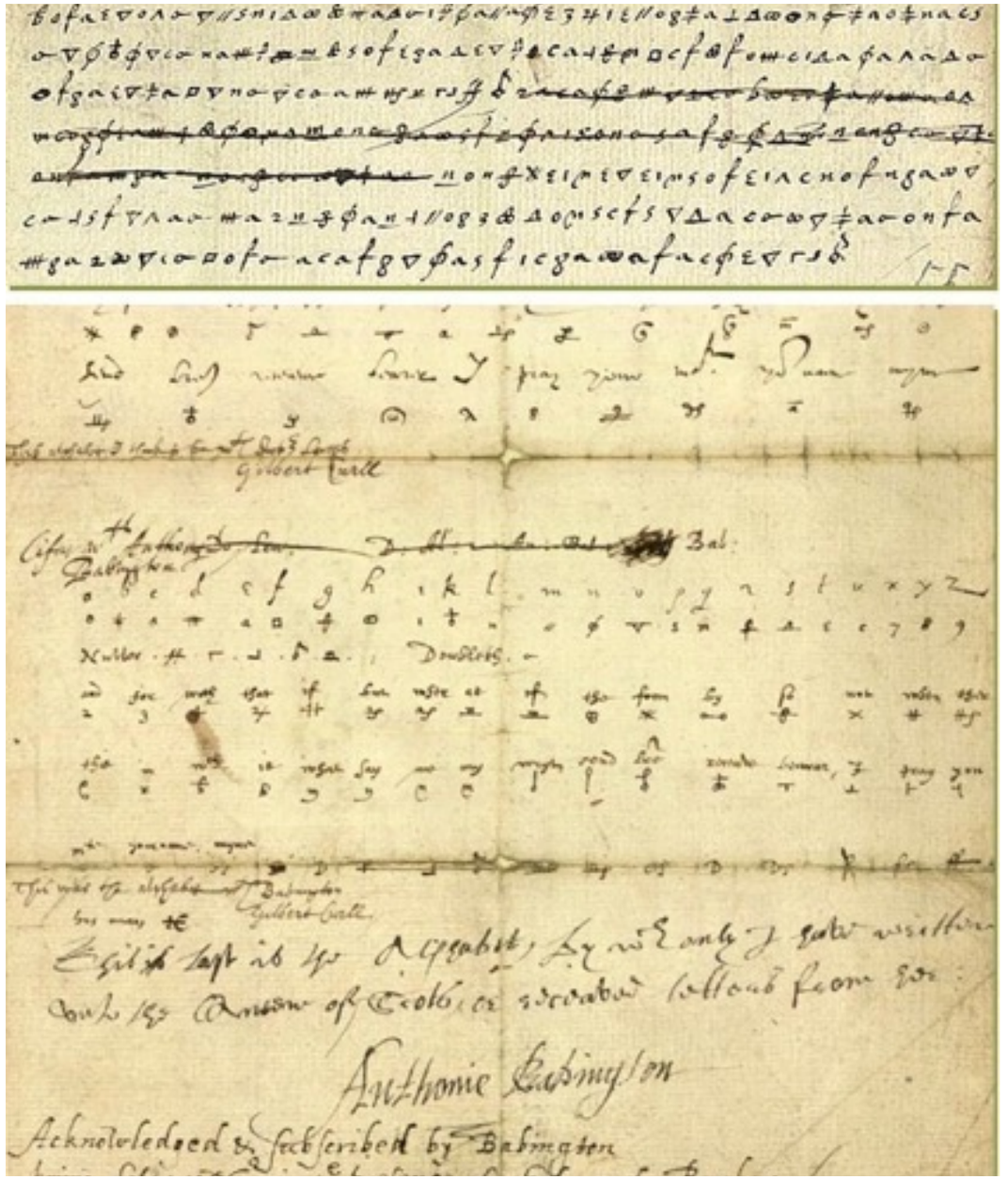
Integrity

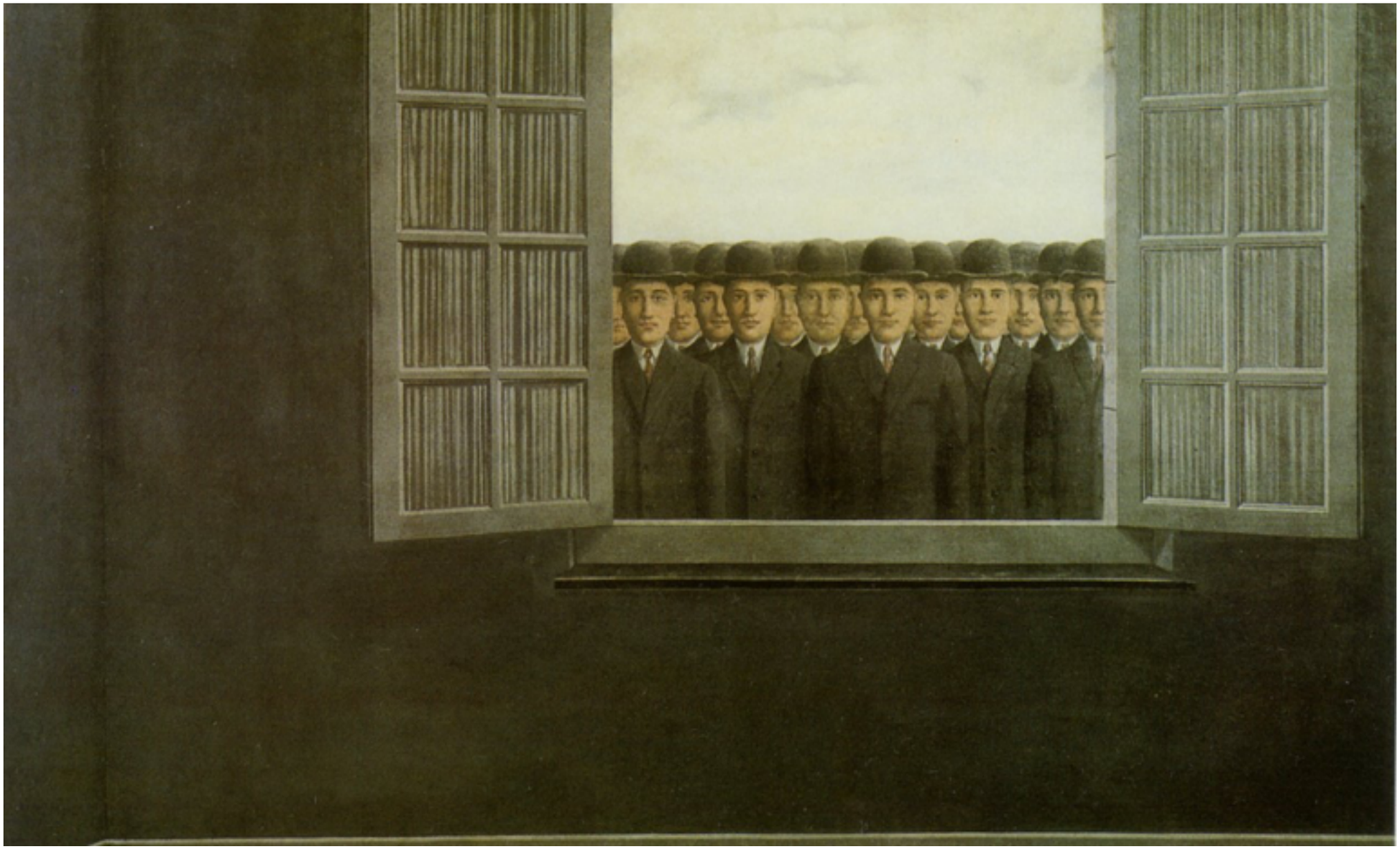
- Attacks: *Masquerading, message tampering, replaying*

- 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], …”

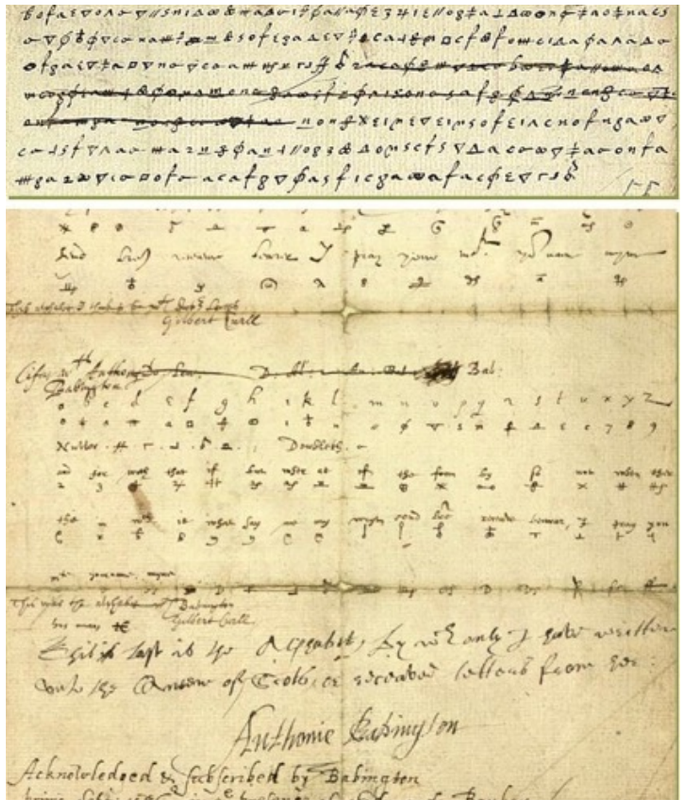


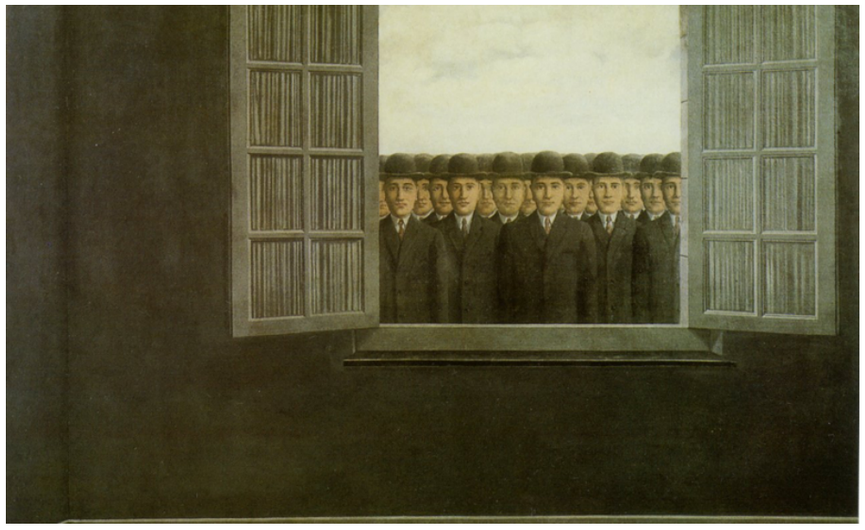


Availability

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.

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.

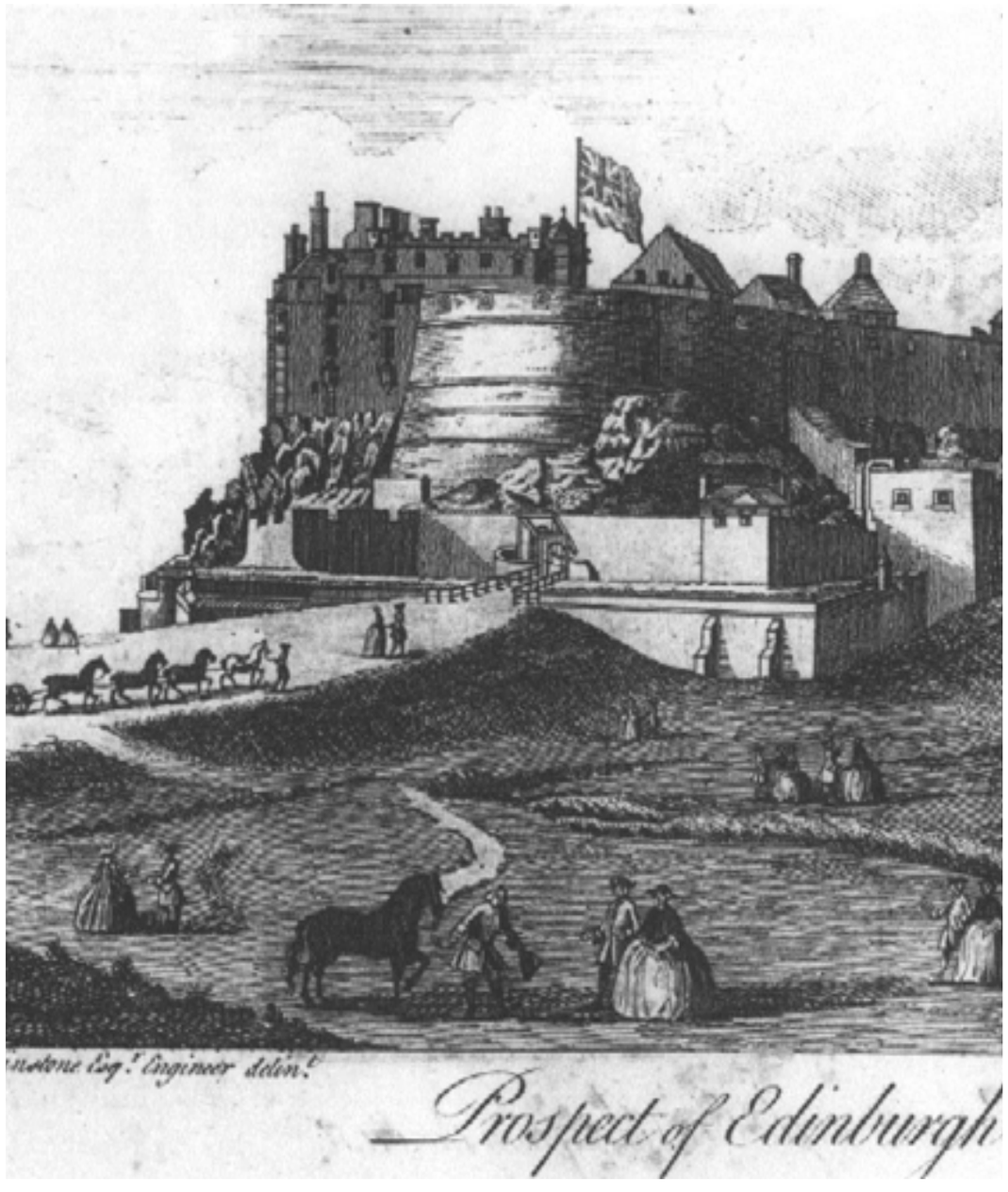
3. Compartmentalisation

- “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.

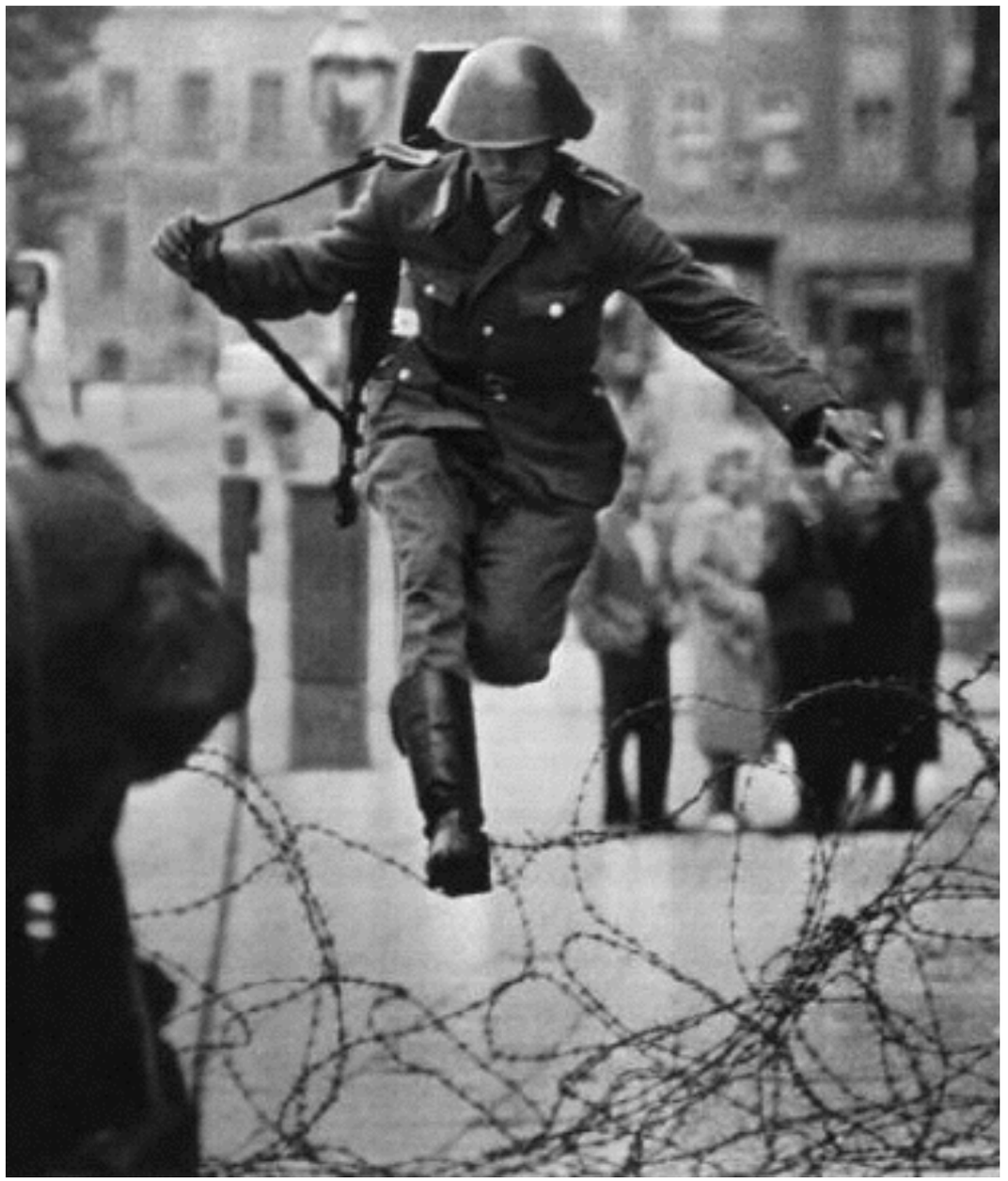


5. Least privilege

- “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.

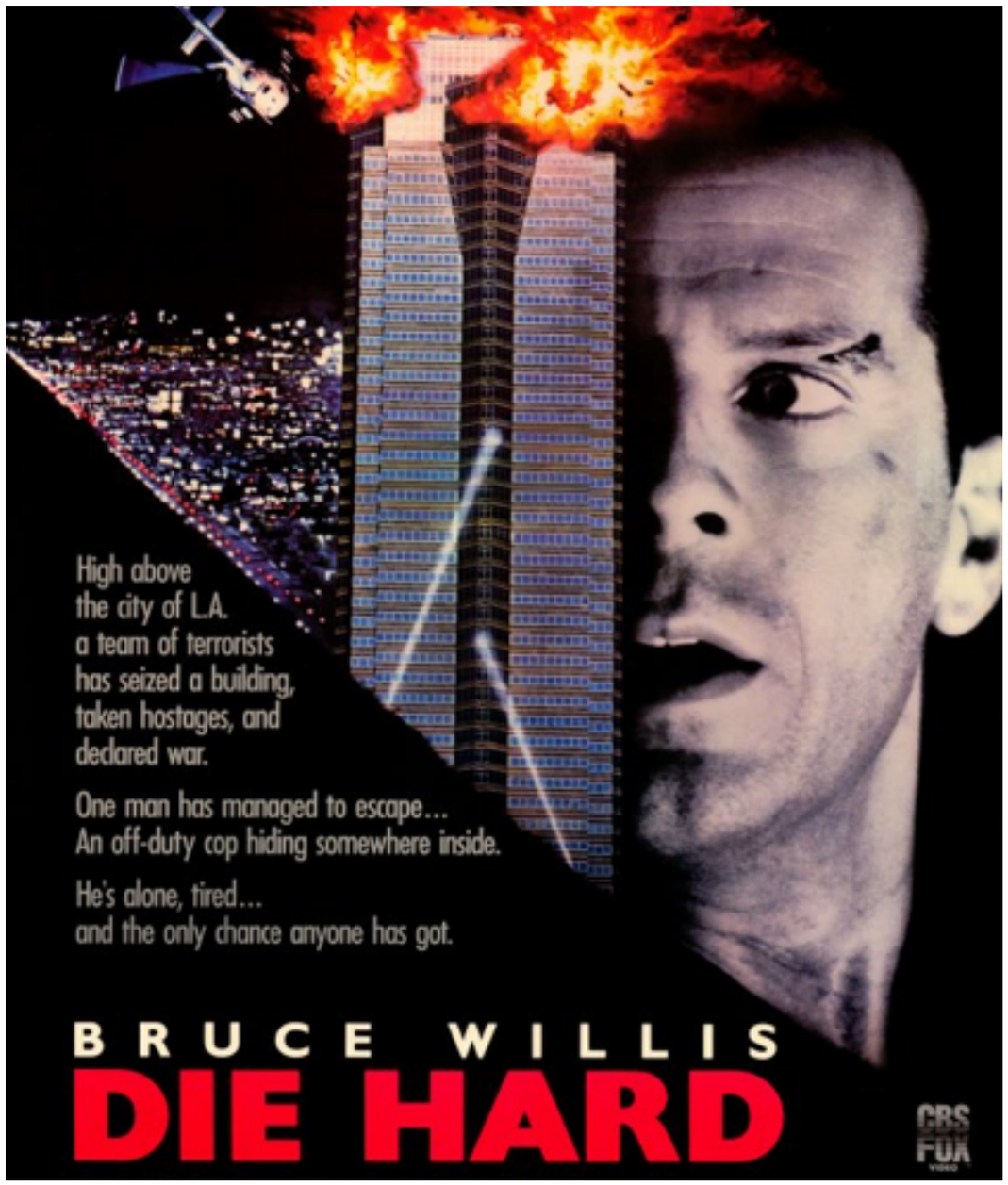


6. Minimum trust and maximum trustworthiness.

- “ 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”?

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.

Summary

Summary

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

Homework

Paper

- Read Chapter 1, 2, C and parts of Saltzer and Schroeder (see learnit.). Pay special attention to the examples accompanying each principle in Chapter 1. Google whatever terms you don't know.

- Answer questions 1.1–1.9, p. 15, in writing. Save your answers; you'll want them when you prepare for the exam.

- Take the quiz in learnit.
  It helps me understand how you're doing.
  It helps you since it (presumably) looks like the exam will.

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 4A14.**