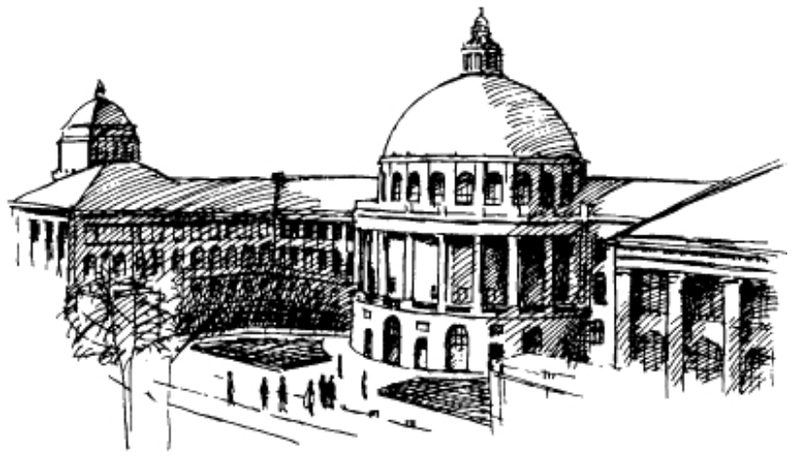
Applied Security Laboratory AS 2017

David Basin, Ralf Sasse, and Christoph Sprenger

Institute of Information Security

September 21, 2017



ETH zürich

Random Selection of Hacking News

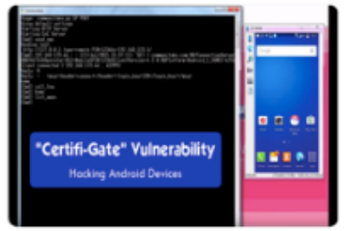
RollJam — $30 Device That Unlocks Almost Any Car And Garage Door

Saturday, August 08, 2015 Khyati Jain

We have talked a lot about car hacking. Recently researchers even demonstrated how hackers can remotely hijack Jeep Cherokee to control its steering, brakes and transmission. Now, researchers have discovered another type of car hack that can be used to unlock almost every car or garage door. You [...]

"Certifi-Gate" Android Vulnerability Lets Hackers Take Complete Control of Your Device

Friday, August 07, 2015 Swati Khandelwal



Android users are busy fighting with Stagefright vulnerability while the popular mobile operating system faces another critical security vulnerability, dubbed as "Certifi-Gate". Millions of Android devices could be hacked exploiting a plugin that comes pre-installed on your Android devices by [...]

Researchers to Share Details of Cyber-Terrorists Targeting Indian Government Officials

Saturday, August 08, 2015 Wang Wei

The Potential threat, range from very narrow to very broad, posed by Cyber-Terrorism has provoked considerable alarm. Terrorists involved in Cyber Espio critical infrastr sectors. The Fr

How Drones Can Find and Hack Internet-of-Things Devices From the Sky

Friday, August 07, 2015 Mohit Kumar

Security researchers have developed a Flying Drone with a custom-made tracking tool capable of sniffing out data from the devices he Internet – better known as the Internet-of-things. ernet of Things Map Project, a team of security he Texas-based firm [...]

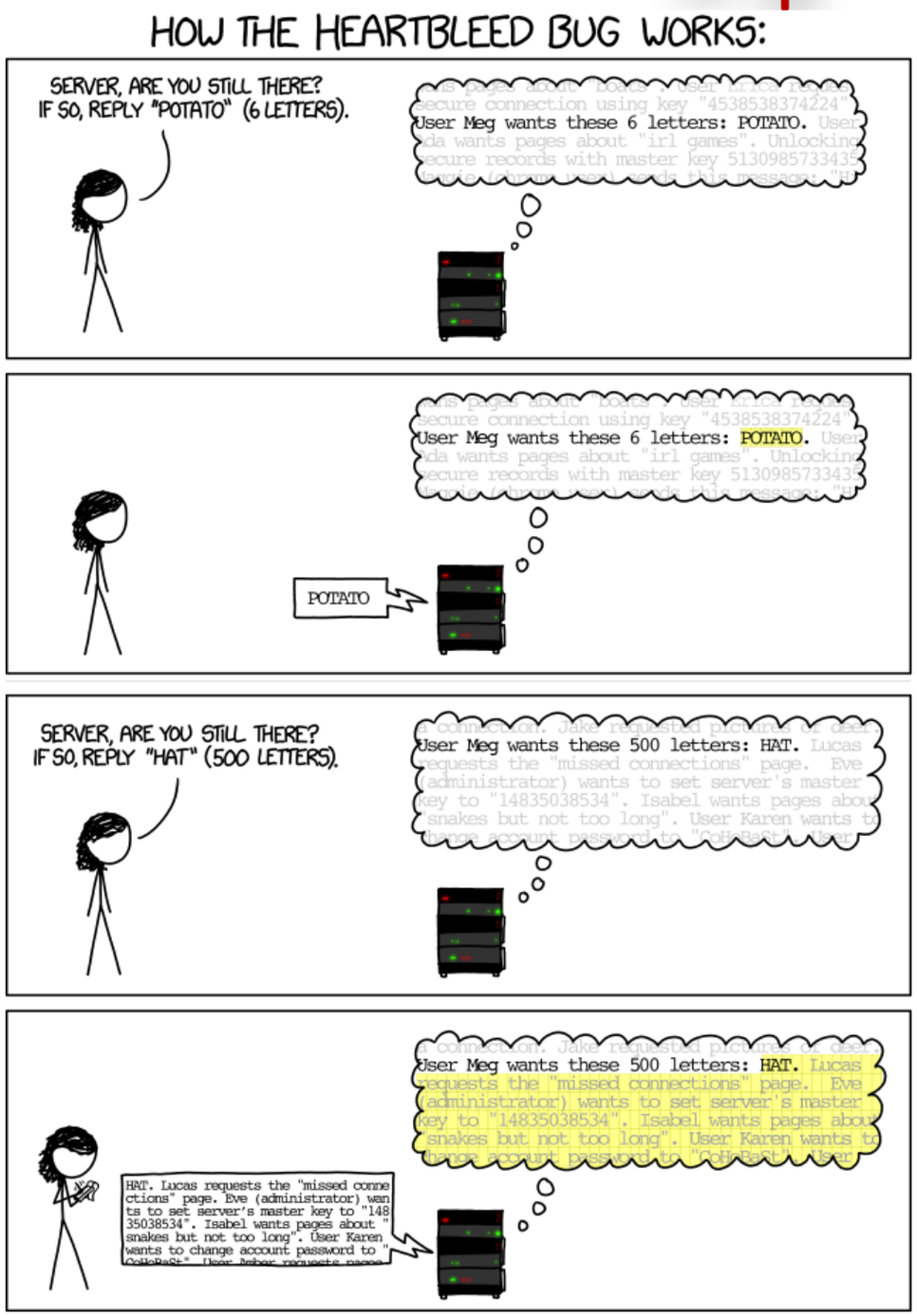
Windows Updates Can be Intercepted to Inject Malware into Corporate Networks

Friday, August 07, 2015 Khyati Jain

If you think that the patches delivered through Windows update can not be laced with malware, think again. Security researchers have shown that Hackers could intercept Windows Update to deliver and inject malware in organizations. Security researchers from UK-based security firm 'Context' [...]

Heartbleed Bug in OpenSSL (2014)

- simple programming error (buffer over-read) in TLS' heartbeat subprotocol
- leakage of passwords, session cookies, and private keys on servers and clients
- affected around half a million (17%) of secure web servers certified by trusted CAs
- fix/recovery requires:
  - installing patched version of OpenSSL,
  - generation of new asymmetric key pairs,
  - revocation and reissuing of certificates,
  - clearing cookie caches,
  - resetting passwords, ...



Ashley Madison Hacked (July 2015)

- Hacked by the “Impact Team”.
- Upset by “Full delete” service supposed to erase all user data for $19 not delivering its promise (generated $1.7m in revenue in 2014!!)
- Leaked data of 37 million users:
  - real names and addresses,
  - email addresses and phone #,
  - hashed passwords,
  - partial credit card data,
  - records of CC transactions.
- 11.2 million passwords cracked
- Consequences: blackmailing, divorce, job loss, suicide.

Espionage Attack on RUAG (May 2016)

Media release

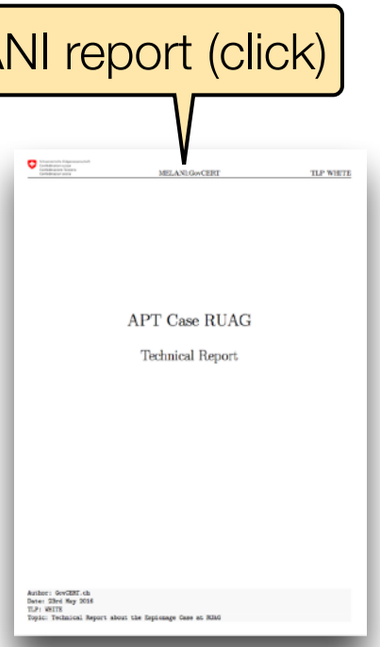
Cyber attack on RUAG: major damage averted

Berne, 12 May 2016. Cybercrime strikes Switzerland: RUAG has considerable IT expertise and many years of successful experience in the security field. Nevertheless, there is no such thing as 100% security. With the support of federal agencies, an attack on RUAG has been detected and halted. Further damage has thus been averted.

RUAG has expertise in detecting and eliminating IT attacks and securing systems against them. Based on information from the federal intelligence agency, RUAG was able to detect and successfully halt a highly professional hacker attack on its IT systems. Because of the small volume of data stolen, the attackers' strategy remained unrecognized for some time.

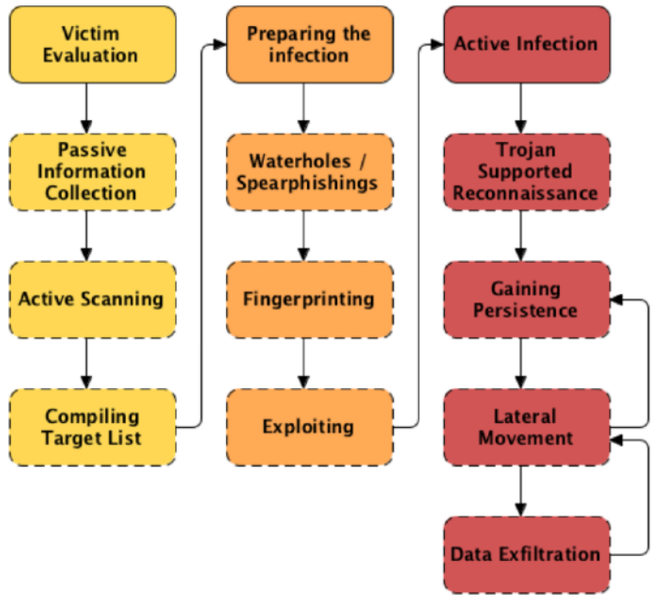
- RUAG strictly observes federal security regulations. No data classified as secret is stored on RUAG systems which are connected to the Internet.
- RUAG can therefore state that no secret data was affected by the attack on RUAG.
- Furthermore, any data classified as confidential stored on Internet-connected RUAG systems is encrypted.
- The data obtained account for less than 0.01% of the volume of data managed by RUAG.

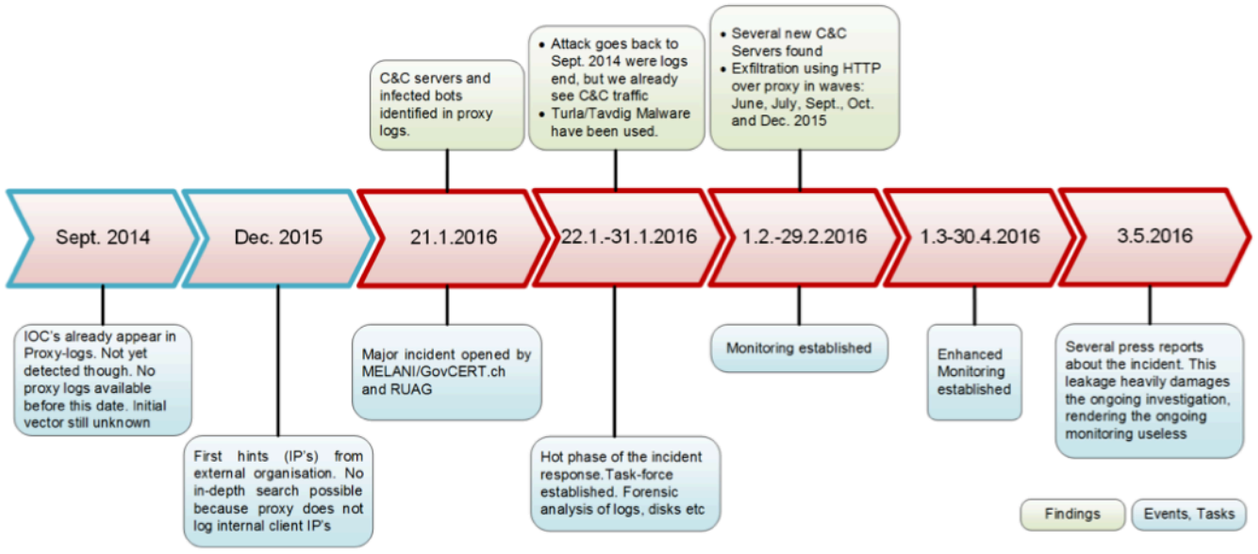
MELANI report (click)


MELANI/GovCERT TLP WHITE

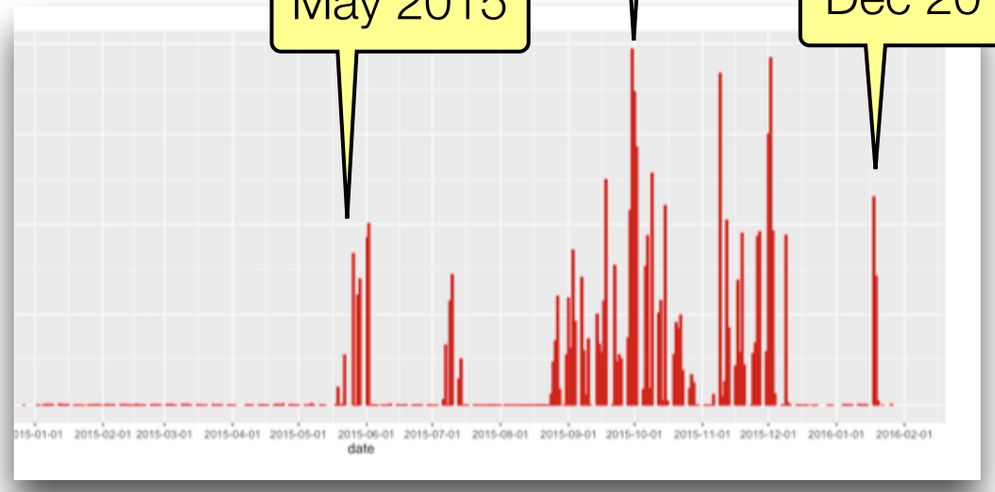
APT Case RUAG

Technical Report





1GB/day; **23 GB tot**



How to Defend Yourself

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

– Sun Tzu (The Art of War)

Motivation and Objectives

- More theoretical courses such as Security Engineering, System Security, and Network Security essential for understanding the basic concepts.
- But information security is ultimately about securing real computers in the real world.
- Hands-on experimental counterpart to the more theoretical courses.
- Improve understanding of theory by
  - putting it directly to use and
  - seeing first-hand the practical consequences and subtleties involved.
- Main focus: networks and operating systems, web applications, and risk management.

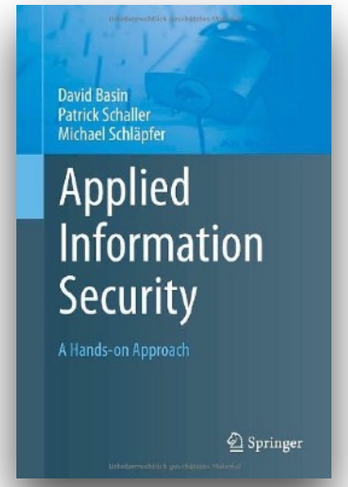
Course History

- Established 2003 by David Basin and Michael Näf.
- Minor updates and changes until 2010.
- Complete update in 2010:
  - Everything based on open-source software.
  - Updated operating systems and vulnerabilities.
  - New extended teaching material in English.
- Another update underway …

Course Components

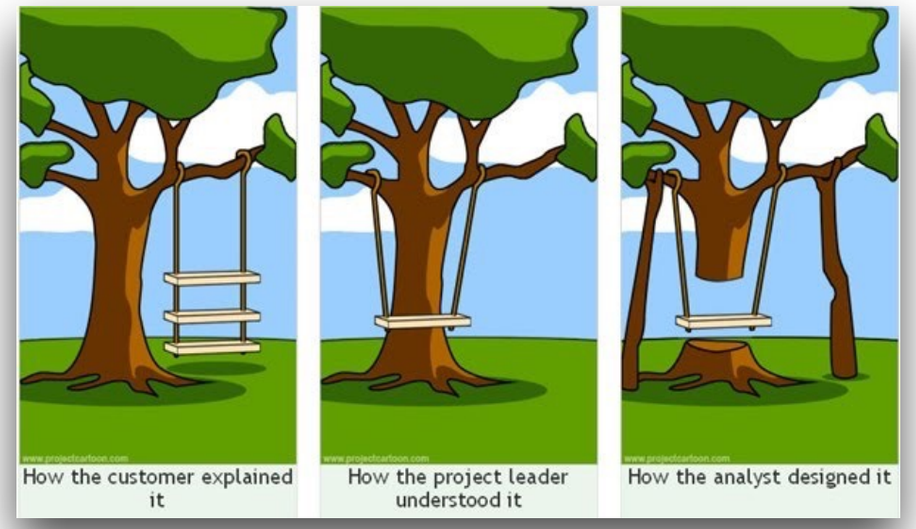
Lab / Book

- Self-learning (assistance provided).
- Background and principles.
- Computer-based, hands-on, practical exercises.



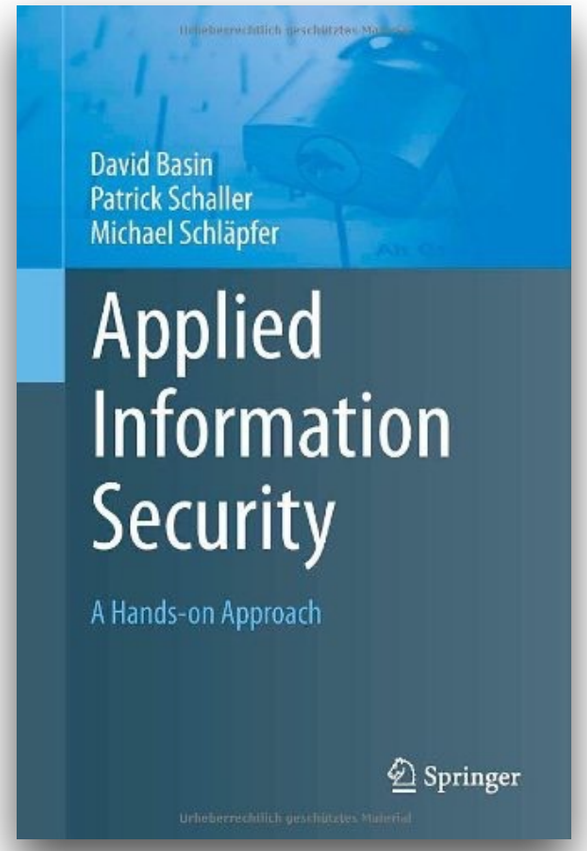
Project

- System development
- Risk analysis
- Peer review

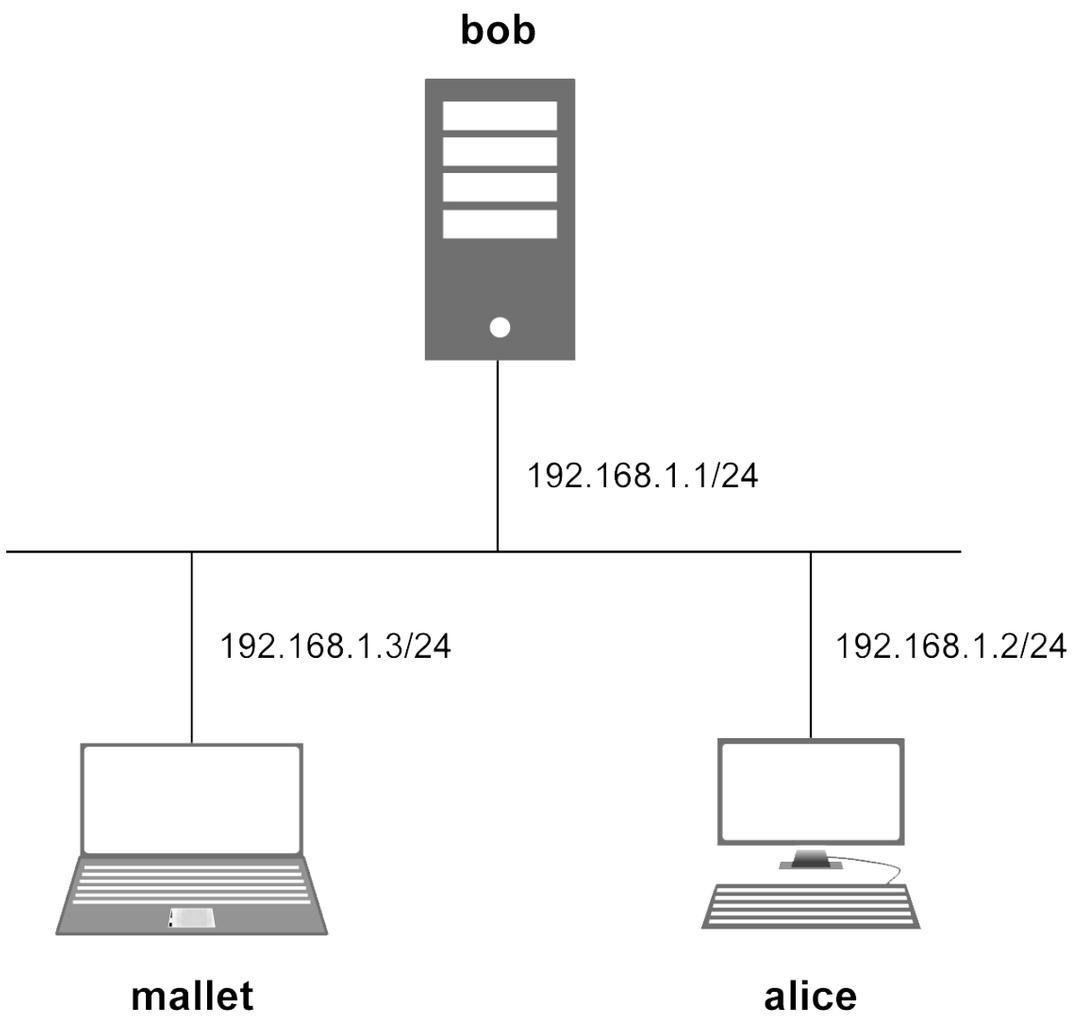


Book Contents

1. Security Principles
2. Lab Environment
3. Network Services
4. Authentication and Access Control
5. Logging and Log Analysis
6. Web Application Security
7. Certificates and Public-Key Cryptography
8. Risk Management
9. Computer Forensics
   (downloadable supplementary chapter)



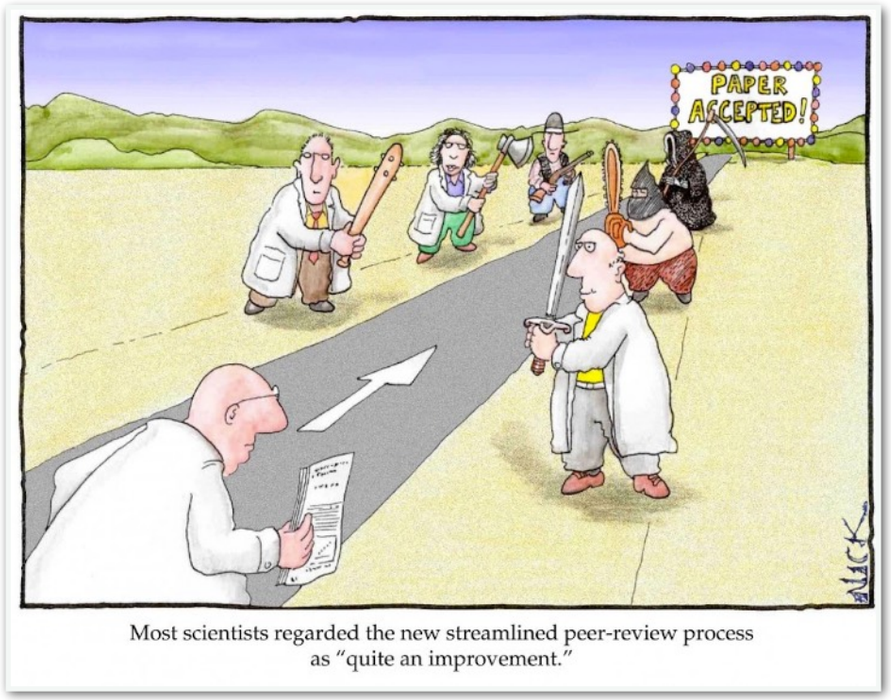
Lab Environment for Practical Work with Book



- Virtual machines (VirtualBox)
- Linux-based VMs
- Book
  - Practical, hands-on approach
  - Attack scenarios
  - Principles
  - Assignments
- Preparation for project and exam.
- Your responsibility!

Project: Certificate Authority for a Small Company

- Teamwork of three students.
- Phase I: System development
  - Design based on risk analysis
  - Linux-based virtual machines
- Phase II: Security review
  - Groups review each other's system.
- Deliverables
  - System Description and Risk Analysis
  - Reviewing Report
- Evaluation Criteria
  - System functionality and security.
  - Report quality.



Most scientists regarded the new streamlined peer-review process as "quite an improvement."

Real Or Virtual?

Use of VMs in the project:

- We work with VMs for just for the convenient simulation of the real world.
- But: Do consider your VMs as the real machines of our fictious company.
- Particularly relevant for risk analysis.
- Avoid reasoning like:

  “We do not need to physically secure our backups, since it is all virtual anyway.”

Important Dates

September 29	Register groups (by email)
October 23	Hand in initial draft of system design and risk analysis (by email)
October 27	Feedback to your draft (by email)
November 23	Hand in final system description and risk analysis, max 30 pages (by email). Hand-in and exchange VMs.
December 14	Hand in final reviews, max 18 pages (by email). 20 min presentation of main results (CAB E 87.1).
December 21	Semester end exam 90 minutes, written, closed-book (CAB H 52).

Performance Assessment

Exam

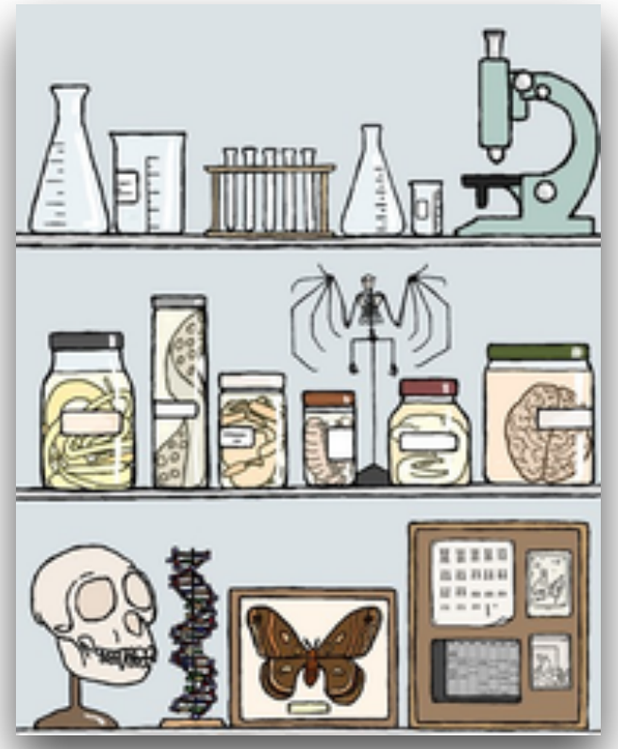
- Written semester end exam.
- No supporting material allowed.
- Covers topics from
  - book,
  - extension chapter, and
  - project.

Grading

- Exam: 60%
- Project: 40%

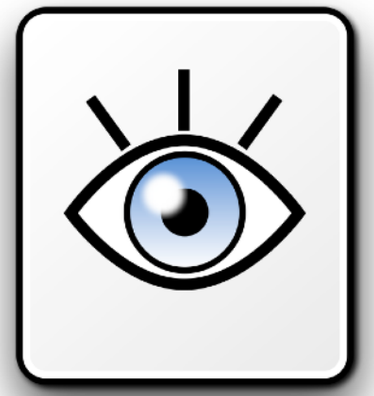
Laboratory

- Location: CAB E 87.1
- Capacity: ca. 16 students.
- 4 group tables.
- All software you need should run on your laptops.
- Access: from next week on with your legi.
- Network: WLAN.



Supervision

- David Basin, CNB F 106 (`basin@inf.ethz.ch`)
- Christoph Sprenger, CNB F 108 (`sprenger@inf.ethz.ch`).
- Ralf Sasse, CNB F 109.2 (`ralf.sasse@inf.ethz.ch`).
- Lukas Bischofberger (`lukasbi@student.ethz.ch`).



- Assisted lab hours: Thursdays 9-12, CAB E 87.1.

- In case of problems, you may also contact us by email, or pass by our offices.
- Flexible schedule: This is a lab course, not a lecture.
- Book is in English; German fine for labs and exam answers.

Ethical and Legal Matters

- The flip side of defense is attack, whether in martial arts, or Information Security.
- Someone who uses karate to attack others outside of practice will be evicted from the Dojo and may face criminal charges:
  - The same is true in this class.
  - Zero tolerance here!
- You are required to sign a Lab Usage Policy.
- Course is an opportunity to understand how to use technology to improve the security of IT systems.

"It doesn't *matter* that you never got caught!"

Lab Usage Policy (Main Points)

- All offensive techniques are taught exclusively for illustrative and educational purposes.
- No “hacking” outside VMs.
- No abuse or illegal use of learned techniques.
- No experiments with DoS attacks, malware, or other activities that deteriorate the availability, quality of service, or reliability of real systems.
- Do not rely on the availability of lab services; your responsibility to back up your information on the lab machines.

Final Remarks

- Course constantly under development.
  We welcome feedback of all kinds.

- This course is different: Interactive and hands-on.
  Self-learning is a large part of this.

- Limited class time.
  We are only scratching the surface of the subjects.

- Find all necessary material on the course webpage:
  `http://www.infsec.ethz.ch/education/as2017/seclab`

What's next? Questions?

- Please read, sign, and hand in the lab usage policy.
- Get the book and the extension chapter (`www.appliedinfsec.ch`).
- Install VirtualBox (`www.virtualbox.org`).
- Install the virtual lab environment (`www.appliedinfsec.ch`).
- Start with the book.

- Questions so far?