Introduction to IT-Security
ITS2017

Today's agenda

- Course overview

- Threat modeling and the security mindset

Administrative information

- Outline
  - Lectures and exercises, week 47-51 and 1-2
  - Christmas vacation, week 52
  - No activities in week 3
  - Exam in week 4 (Thursday, January 25)
- Lectures: Tue/Thu 10-12 in Lille UP1
- Exercises: Thu 13-16 in 4-0-10 (Biocenteret)

Topics at a glance

- Intro and attacker modus
- Software and web app security
- System security
- Cryptography
- Network security
- Reactive security
- Outro

Reading material

- Online resources (see lecture plan)
- Lectures are not 1:1 with reading material
- Lectures focus on the big picture

Exercises

- 6 exercise sets
- Pass 4 or more (resubmission only first set)
- Solve in groups or by yourself
- Hand in individually

- (All exercises part of syllabus)

Exercise elements

- True or False
- Multiple-choice
- Short Answer Questions
- Hands-on

Exam

- 4-hour written exam, January 25, 2018
- Syllabus is exercises and reading material
- All aids allowed except Internet

- (Oral re-exam in week 16, 2018)

What you need for this course

- CompSys, i.e. ARK, OSM, Datanet
- Some programming experience
- Willingness to learn a new exciting field

Goals

- Broad introduction to field of IT-security
- Theory and practice
- How to think about security

What this course it not

- *Not* the inside on the latest and greatest hacks
- *Not* every aspect of IT-security
- *Not* how to hack stuff

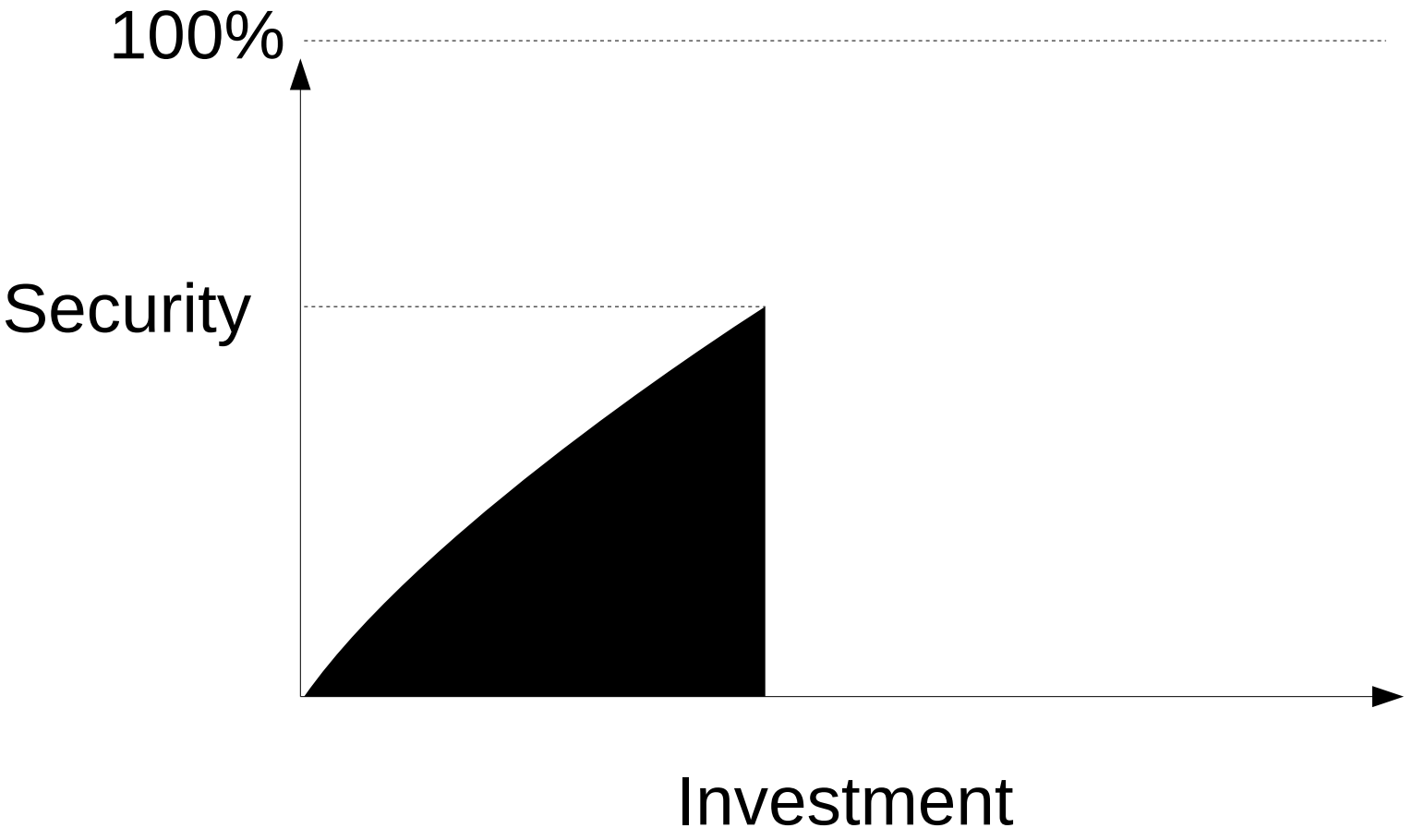
Ethics and legal disclaimer

So what is IT-security?

It’s many things, and more

- Firewalls
- Reverse engineering
- Software flaws
- Code review
- Security management
- Incident handling
- Cryptopgraphy
- Access controls
- Passwords
- Risk analysis
- Threat models
- Intrusion detection
- Steganography
- Patching

100% security is an illusion



Even big budget-firms get breached

BBC | BBC iD | Menu | Search

NEWS | Sections

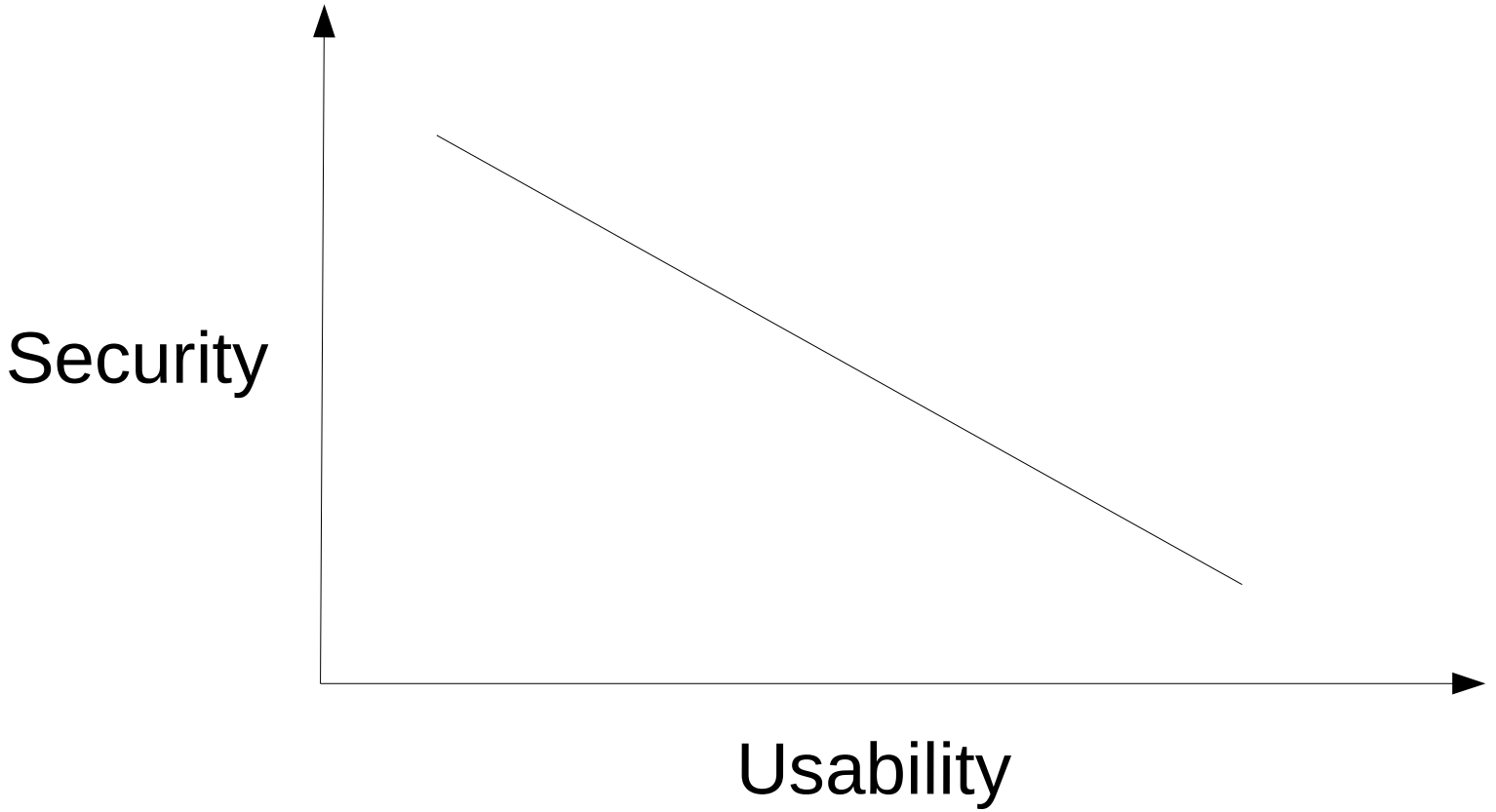
Technology

Coca-Cola 'targeted' by China in hack ahead of acquisition attempt

5 November 2012 | Technology

What about usability?

- The duality of security?



People don't like security that much

Some times people work against it

November 20, 2015

69% of users would avoid security controls to make big business deals

Share this content:

Some 69 percent of users would bypass security controls so they could win business.

People will bypass security

What does IT-security mean to you?

Is this security?

PSN, Blizzard, and Riot hit with massive DDoS attack

By Imad Khan

Aug 24, 2014, 1:44pm CT | Last updated Aug 25, 2014, 11:16am CT

A massive cyberattack is currently crippling some of the most prominent gaming services in existence.

A group known as Lizard Squad has claimed responsibility for attacks on the PlayStation Network (PSN), Blizzard's Battle.net, Riot's *League of Legends*, and Grinding Gear Games' Path of Exile, according to a report by Shack News. President of Sony Online Entertainment John Smedley confirmed the news on Twitter.

> We are under attack by a large scale ddos. Being dealt with but it will impact games until its handled.
>
> — John Smedley (@j_smedley) August 24, 2014

Is this security?

GitHub hit by Massive DDoS Attack From China

Friday, March 27, 2015 Mohit Kumar

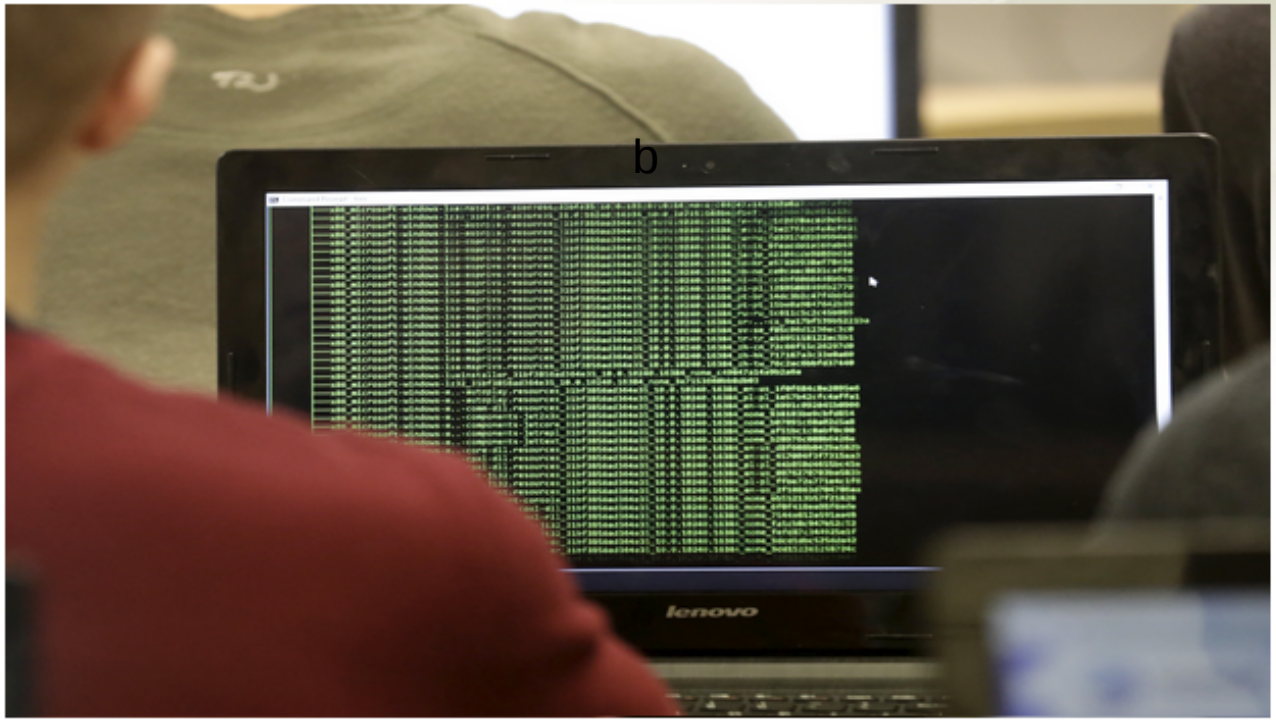
Github – a popular coding website used by programmers to collaborate on software development – was hit by a large-scale *distributed denial of service (DDoS) attack* for more than 24 hours late Thursday night.

Is this security?

15. DEC. 2015 KL. 14.41

Folketinget lagt ned af utrolig lille cyberangreb

Et såkaldt distributet denial of service-angreb har over flere omgange tvunget folketingets hjemmeside i knæ. Nu viser det sig, at angrebet var lillebitte.



Et lillebitte angreb lagde folketinget.dk ned. (Foto: Ints Kalnins © Scanpix)

Is this security?

DANMARK 28. SEP. 2012 KL. 15.37

Hovedstadens sygehuse er ramt af stort it- og telefonnedbrud

Patienter på Rigshospitalet må belave sig på aflysninger og længere ventetid.

NEDBRUD. Rigshospitalet beklager de gener, som systemnedbruddet påfører patienterne og deres pårørende. - Foto: MARTIN SLOTTEMO LYNGSTAD

Is this security?

DOWNTIME, NEW YORK

Massive Flooding Damages Several NYC Data Centers

BY RICH MILLER ON OCTOBER 30, 2012 26 COMMENTS

Is this security?

10 December 2012 Last updated at 12:13 GMT

Apple Maps 'is life-threatening' to motorists lost in Australia heat

Inaccuracies in Apple Maps could be "life-threatening" to motorists in Australia's searing heat, police have warned.

Officers in Mildura, Victoria, say they have had to assist drivers stranded after following the software's directions.

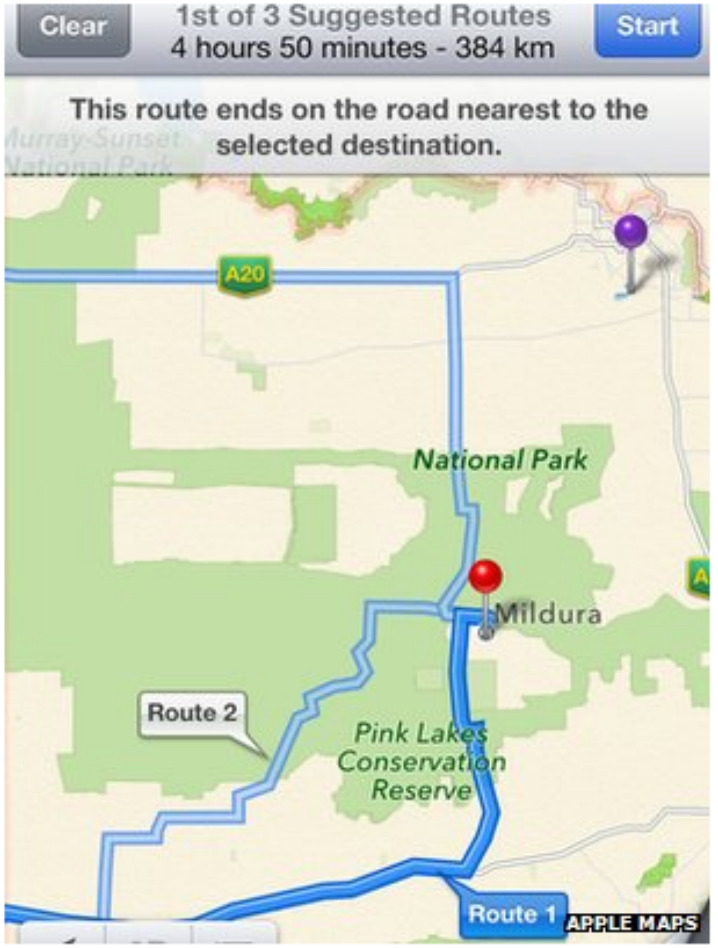
Some of the drivers had been without food or water for 24 hours.

Apple's software was heavily criticised by users when it was released in September.

Last week, chief executive Tim Cook admitted Apple had "screwed up" and was working to improve the program.

'No water supply'

In a press release, Victoria police's acting senior sergeant Sharon Darcy made her force's concerns clear.



Is this security?

Texas students hijack superyacht with GPS-spoofing luggage

Don't panic, yet

29 Jul 2013 at 18:04, Iain Thomson

Students from the University of Texas successfully piloted an $80m superyacht sailing 30 miles offshore in the Mediterranean Sea by overriding the ship's GPS signals without any alarms being raised.

Is this security?

Af uransalige grunde blev et anbefalet brev til Danmarks Statistik med følsomme oplysninger og 5 mio. cpr-numre afleveret til den kinesiske visummyndighed.

Is this security?

Sony Breach Exposed Employee Healthcare Data, Salaries

MACK GELBER
Dec 2nd 2014 1:48PM

You know that massive data breach at Sony Pictures Entertainment you've been hearing about--the one that leaked films like "Annie" and the still-in-theaters "Fury" to file-sharing sites? Well, it turns out that a lot more than were leaked. As security news site Krebs on Security reports, hackers also stole documents containing sensitive employee data, including Social Security numbers, salary, and healthcare information.

Security defined

- Computer systems fail for many reasons

- **Reliability** = accidental failures
- **Usability** = failures caused by mistakes made by users
- **Security** = intentional failures made by malicious parties

Security is about
computing in the presence of an adversary

The flat tire analogy

Keys questions in security

- **Who** are my adversaries?
- What is their **motivation**?
- What are their **capabilities**?
- **What** are they after?

Threat actor skill and focus

What are they after

- Conversely, what are the typical security goals

- Confidentiality
- Availability
- Integrity

- Authenticity
- Authorisation
- Non-repudiation

Security is a huge issue

Security is a huge issue

Hackerangreb koster Mærsk milliardbeløb

Mærsk anslår, at hackerangrebet fra juni og juli vil koste selskabet 1,3 til 1,9 milliarder kroner.

Security is a huge issue

Kreditbureau mistede følsomme oplysninger om 143 millioner mennesker – og tabte en milliard dollars på få minutter

Hackere har fået adgang til 143 millioner menneskers personlige oplysninger efter indbrud hos et amerikansk kreditbureau. Cpr-numre, kørekort, adresser og kreditkortnumre er lækket.

12. september 2017 kl. 08.00

Hacking must be easy

Sure it’s an uneven playing field

- The attacker needs only one way in
- While the defender has to defend all

- But defenders are capable of doing much more

- (More on this next time)

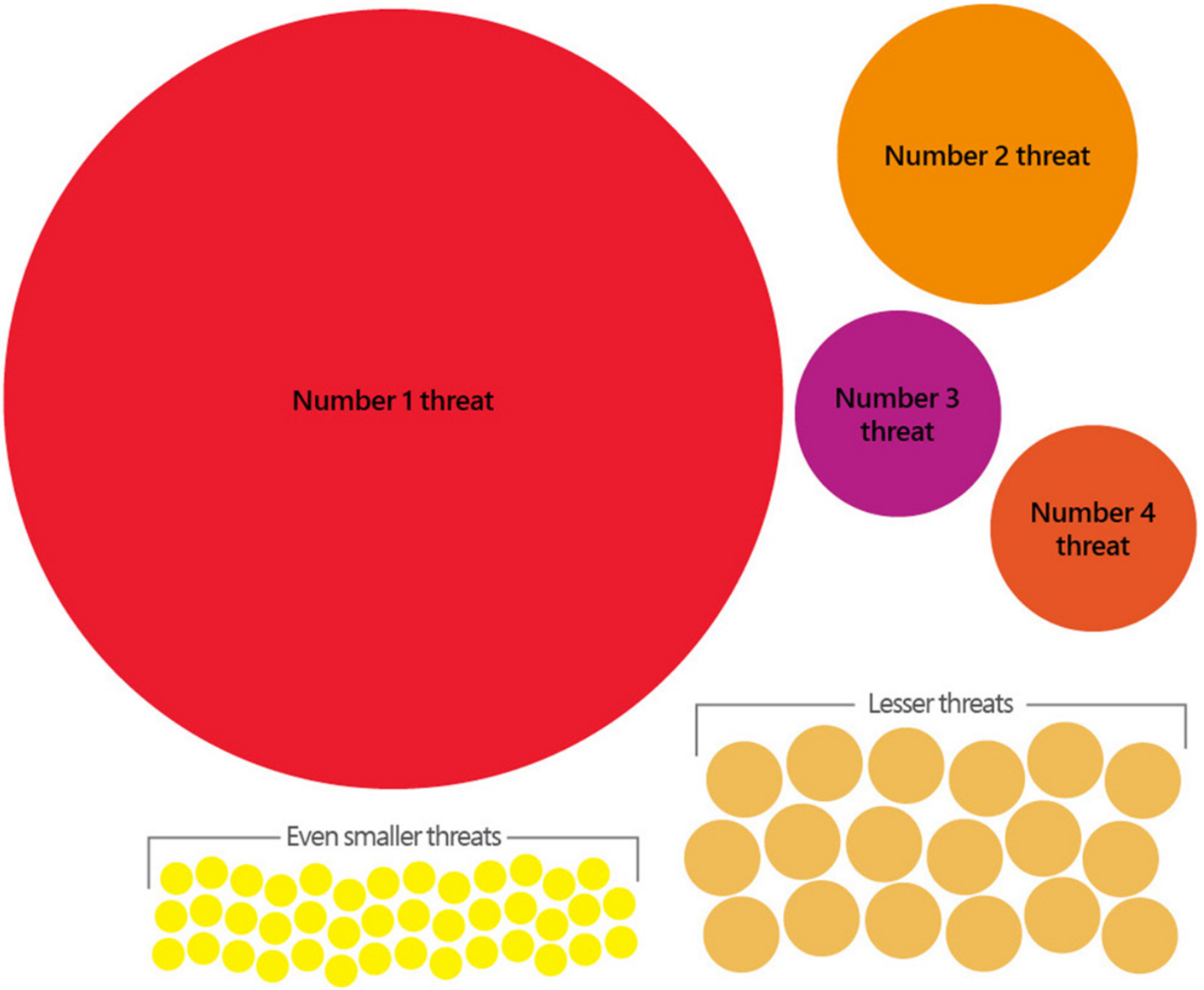
What to do?

- Study, adjust, repeat

Best practice standards

- ISO2700x
- CIS Critical Security Controls
- NIST Standards
- ISF Standard of Good Practice
- Australian Signals Directorate
- ICS-CERT

Not all threats are equal



The key is understanding

- The business
- The threats
- The risk

- Then apply best practices

For the exercises

- Install VirtualBox on your Host
  - https://www.virtualbox.org/wiki/Downloads
- Create an Ubuntu 16.04 VM in VirtualBox
  - https://www.wikihow.com/Install-Ubuntu-on-VirtualBox