

Select language

```
> en_UK
fr_FR
tlh
```





2011 First APT detected (Stuxnet)

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...
- 11-12.2014 Apple "The Fappening", Sony, Microsoft, DPRK, Germany [1].

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...
- 11-12.2014 Apple "The Fappening", Sony, Microsoft, DPRK, Germany [1].
 - 01.2015 Finland, Switzerland, Germany, UK Banks and hedge funds

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...
- 11-12.2014 Apple "The Fappening", Sony, Microsoft, DPRK, Germany [1].
 - $01.2015\,$ Finland, Switzerland, Germany, UK Banks and hedge funds
 - 2015 UK, Aus, US, France, China, Russia unveil "Cyberwarfare" plans.

- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...
- 11-12.2014 Apple "The Fappening", Sony, Microsoft, DPRK, Germany [1].
 - 01.2015 Finland, Switzerland, Germany, UK Banks and hedge funds
 - 2015 UK, Aus, US, France, China, Russia unveil "Cyberwarfare" plans.
 - + countless intrusions and leaks...

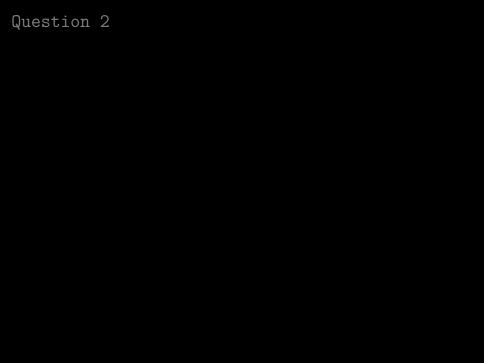
- 2011 First APT detected (Stuxnet)
- 2013 Russia: 50+ financial institutions attacked, est. \$17+ millions stolen in 6 months [0]
- 2013 Major US/UK/AUS operations to undermine information security worldwide revealed
- 2014 Critical vulnerabilities in widely used technologies: Inception, Heartbleed, goto fail, Shellshock, Dragonfly, Windigo, USB...
- 11-12.2014 Apple "The Fappening", Sony, Microsoft, DPRK, Germany [1].
 - 01.2015 Finland, Switzerland, Germany, UK Banks and hedge funds
 - 2015 UK, Aus, US, France, China, Russia unveil "Cyberwarfare" plans. + countless intrusions and leaks...
 - [0] Anunak, APT against financial institutions, Group-IB and Fox-IT, 2014.
 - [1] Die Lage der IT-Sicherheit in Deutschland 2014, Bundesamt für Sicherheit in der Informationstechnik, 2014.

Not that much in the news

- 08.15 Google Android Stagefright Exploit (still not fixed)
- 20.09.15 Google Chrome %%3030%30 bug (still not fixed)
- 21.09.15 Samsung S4 Kernel vuln (still not fixed)
- 21.09.15 Apple App Store compromised (still not fixed)
- 21.09.15 Skype down globally (now up)

New trends in 2015

- ► *Trending tools:* APTs, Skimmers, Spear-fishers, Surveillance, Darknets...
- ► Trending targets: Bitcoin stealing, Banks, Industrial sites, Cloud storages...
- ► Trending perpetrators: Government-backed expert teams...



Question 2

« Piracy » ?

Question 2

« Piracy » ?
« Virus » ?

Question 2

```
« Piracy » ?
« Virus » ?
« Cyberattack » ?
```

 $24 hrs \ starting \ 10 \ mins \ ago$

24hrs starting 10 mins ago

24hrs starting 10 mins ago

An overview of Information Security.

► Context: who, what, why, when ?

24hrs starting 10 mins ago

- Context: who, what, why, when ?
- ► *Technology:* how ?

24hrs starting 10 mins ago

- Context: who, what, why, when ?
- ► *Technology:* how ?
- Debates

24hrs starting 10 mins ago

An overview of Information Security.

- Context: who, what, why, when ?
- ► *Technology:* how ?
- Debates

+Slides

24hrs starting 10 mins ago

- Context: who, what, why, when ?
- ► *Technology:* how ?
- Debates
- +Slides +Textbook

24hrs starting 10 mins ago

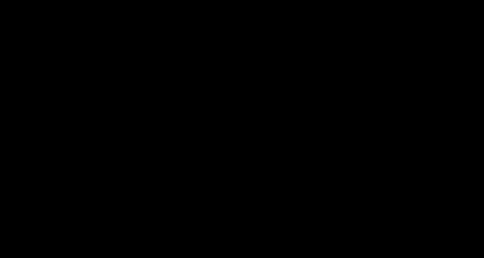
- Context: who, what, why, when ?
- ► Technology: how?
- Debates
- +Slides +Textbook +Demos/Labs

24hrs starting 10 mins ago

- Context: who, what, why, when ?
- ► *Technology:* how ?
- Debates
- +Slides +Textbook +Demos/Labs +Interviews

24hrs starting 10 mins ago

- Context: who, what, why, when ?
- ► *Technology:* how ?
- Debates
- +Slides +Textbook +Demos/Labs +Interviews +Exam



▶ What "information security" is all about, how to think about it and why it matters

- What "information security" is all about, how to think about it and why it matters
- A solid background to shine at the dinner table: Economics, Law, Geopolitics (not kidding)

- What "information security" is all about, how to think about it and why it matters
- ▶ A solid background to shine at the dinner table: Economics, Law, Geopolitics (not kidding)
- How it all really works, how attacks are planned, how vulnerabilities are exploited, and how to do all that

- What "information security" is all about, how to think about it and why it matters
- ▶ A solid background to shine at the dinner table: Economics, Law, Geopolitics (not kidding)
- How it all really works, how attacks are planned, how vulnerabilities are exploited, and how to do all that
- How to deal with information-related risks, mitigate vulnerabilities, thwart attacks and protect your business

- What "information security" is all about, how to think about it and why it matters
- A solid background to shine at the dinner table: Economics, Law, Geopolitics (not kidding)
- How it all really works, how attacks are planned, how vulnerabilities are exploited, and how to do all that
- How to deal with information-related risks, mitigate vulnerabilities, thwart attacks and protect your business
- Also, things not on this list.

infosec, law, econ, criminology, risk analysis, instrusion, detection, hacking, opsearch, politics, crypto, cyberdef, maths



▶ Laymen interested in the role of "information security" in today's world

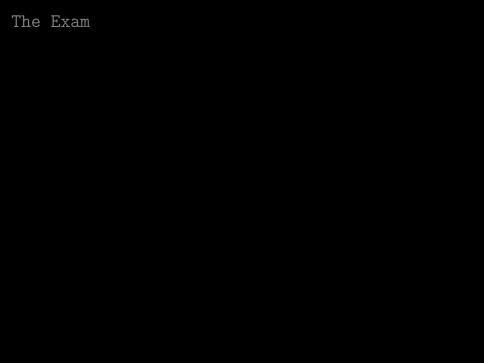
- ▶ Laymen interested in the role of "information security" in today's world
- Managers willing to deal in a responsible manner with information-related risks

- Laymen interested in the role of "information security" in today's world
- Managers willing to deal in a responsible manner with information-related risks
- Leaders understanding the importance of making informed decisions and leveraging ITsec

- Laymen interested in the role of "information security" in today's world
- Managers willing to deal in a responsible manner with information-related risks
- Leaders understanding the importance of making informed decisions and leveraging ITsec
- Researchers concerned with understanding the issues and pushing technology forward

- Laymen interested in the role of "information security" in today's world
- Managers willing to deal in a responsible manner with information-related risks
- Leaders understanding the importance of making informed decisions and leveraging ITsec
- Researchers concerned with understanding the issues and pushing technology forward
- Geeks that like to fiddle with things, break them, make them better and make them fly

- Laymen interested in the role of "information security" in today's world
- Managers willing to deal in a responsible manner with information-related risks
- Leaders understanding the importance of making informed decisions and leveraging ITsec
- Researchers concerned with understanding the issues and pushing technology forward
- Geeks that like to fiddle with things, break them, make them better and make them fly
- Hardcore hackers who come here to cheer, drink beer and see whether it's worth listening to.



You can choose what you find more exciting:

You can choose what you find more exciting:

./0 A short presentation about a topic (either you choose, or I provide) in small groups (1-3)

You can choose what you find more exciting:

- $_{\rm I}/_{\rm I}$ A short presentation about a topic (either you choose, or I provide) in small groups (1–3)
- ./1 A fight to the death between teams (4–6) on either side of the Force.

You can choose what you find more exciting:

- ./0 A short presentation about a topic (either you choose, or I provide) in small groups (1-3)
- ./1 A fight to the death between teams (4–6) on either side of the Force.
- ./2 A small project of your choosing.

You can choose what you find more exciting:

- ./0 A short presentation about a topic (either you choose, or I provide) in small groups (1–3)
- ./1 A fight to the death between teams (4–6) on either side of the Force.
- ./2 A small project of your choosing.

All documents, all computers and devices, WiFi enabled, interaction with other students strongly encouraged (except maybe 3).

Last year they chose ./0 by 1 vote.

You can choose what you find more exciting:

- ./0 A short presentation about a topic (either you choose, or I provide) in small groups (1–3)
- ./1 A fight to the death between teams (4–6) on either side of the Force.
- ./2 A small project of your choosing.

All documents, all computers and devices, WiFi enabled, interaction with other students strongly encouraged (except maybe 3).

Last year they chose ./0 by 1 vote.

Talk together, agree on something, let me know next week.

Good to have

- ► A Linux *virtual* machine (Debian *not* Ubuntu)
- ► Some knowledge of C and technology (there will be reminders)
- A critical and curious mind

The contract

NoBS: No bullshit, on either side.

ELI5: We're here to learn, ask questions.

80% : I advise you to attend most lectures. No repeats.

FUN: Serious stuff, but fun stuff.

Also I try to keep things fresh.

Programme Subject to change

- ▶ Lecture 0: Global Situation, Risk Analysis, Cybercriminality
- Lecture 1: Access Control: InfoSec and Crypto
- ▶ Lecture 2: Networks and Topology: Defence in Depth, NetSec
- ► **Lecture 3**: SoftSec and Injection + Lab: NetSec
- ▶ Lecture 4: Attack Planning + Lab: Soft Sec
- ► Lecture 5: Surveillance and Intrusion Detection
- ▶ **Lecture 6**: Web, API and Database Security
- Lecture 7 ?
- Exam



Any questions ? Please?