Beveiliging van netwerken en computers

CHAPTER 1
INTRODUCTION

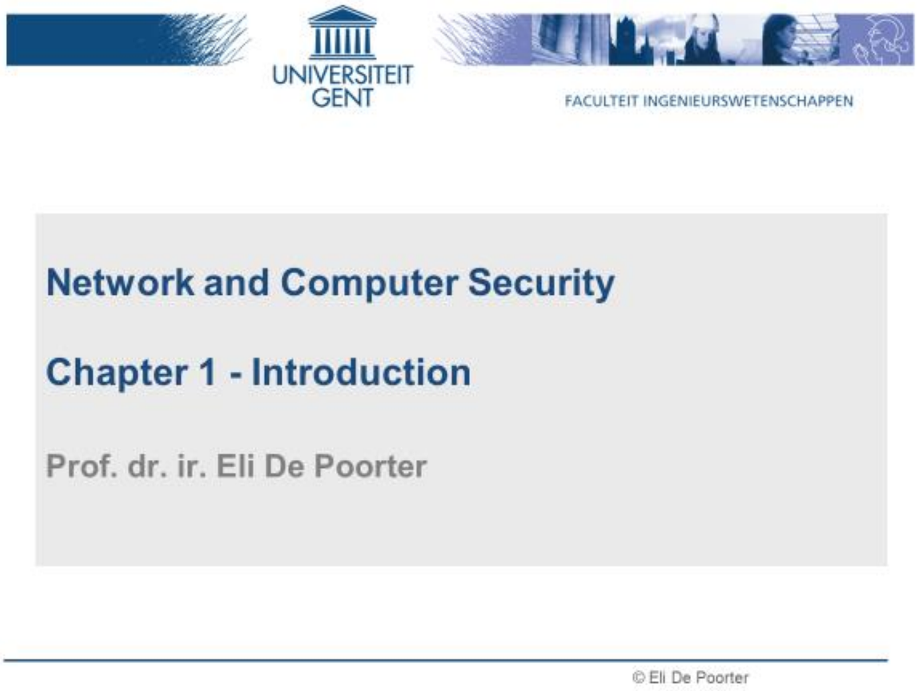
PROF. DR. IR. ELI DE POORTER

eli.depoorter@ugent.be

GHENT UNIVERSITY – IMEC

IDLAB

http://idlab.technology | *http://idlab.ugent.be*



UNIVERSITEIT GENT

FACULTEIT INGENIEURSWETENSCHAPPEN

Network and Computer Security

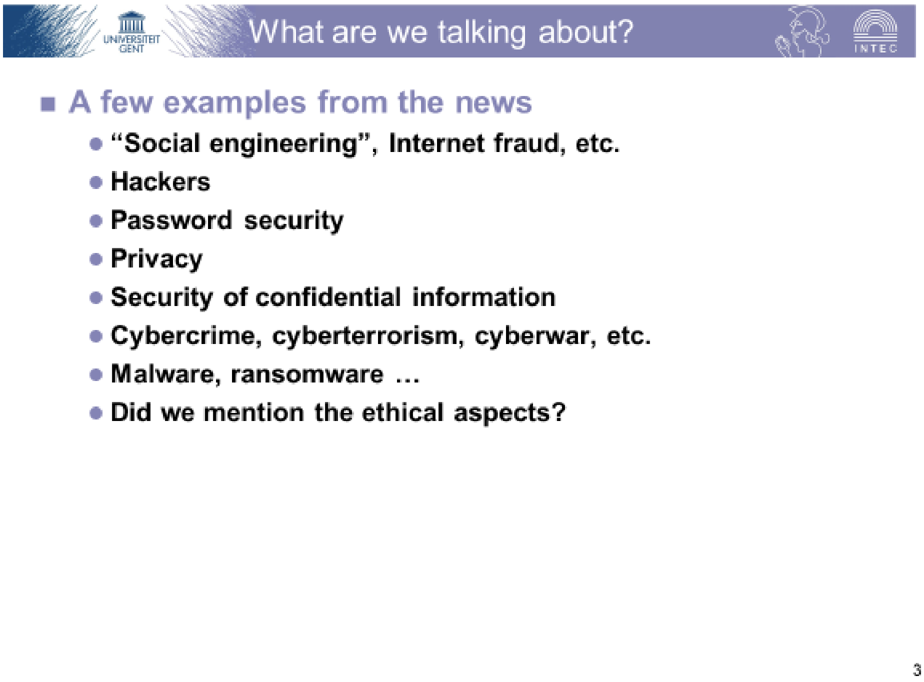
Chapter 1 - Introduction

Prof. dr. ir. Eli De Poorter

What are we talking about?

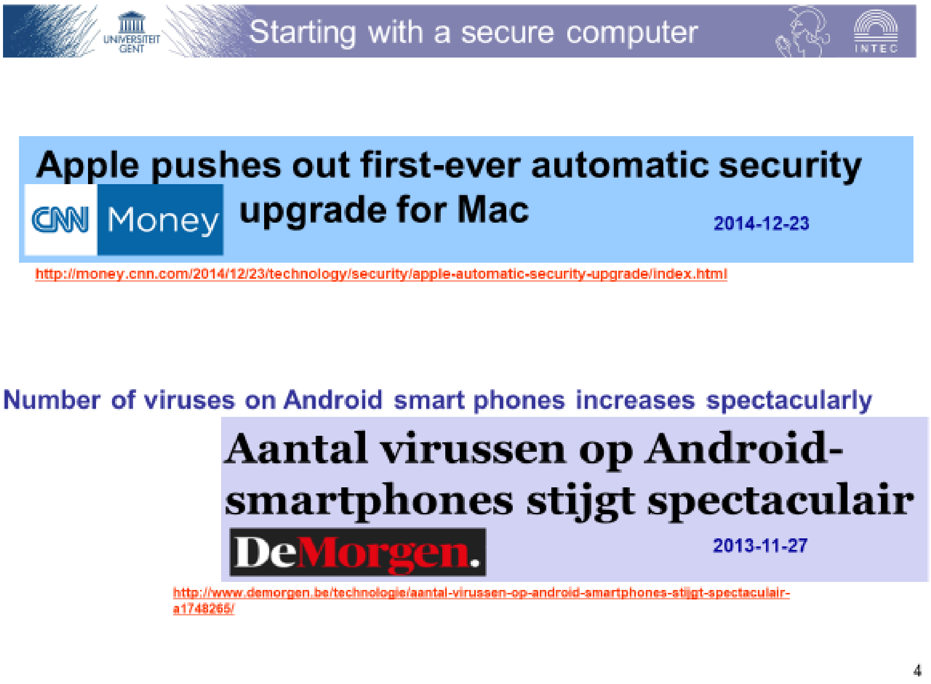
What comes to mind when you hear the term "Security"?

2



What are we talking about?

- A few examples from the news
  - “Social engineering”, Internet fraud, etc.
  - Hackers
  - Password security
  - Privacy
  - Security of confidential information
  - Cybercrime, cyberterrorism, cyberwar, etc.
  - Malware, ransomware …
  - Did we mention the ethical aspects?



Starting with a secure computer

Apple pushes out first-ever automatic security upgrade for Mac

CNN Money 2014-12-23

http://money.cnn.com/2014/12/23/technology/security/apple-automatic-security-upgrade/index.html

Number of viruses on Android smart phones increases spectacularly

Aantal virussen op Android-smartphones stijgt spectaculair

DeMorgen. 2013-11-27

http://www.demorgen.be/technologie/aantal-virussen-op-android-smartphones-stijgt-spectaculair-a1748265/

What about the user?

- Secure or user-friendly?

TO PROTECT THE SYSTEM, JPEG ATTACHMENT NOT ALLOWED TO BE DISPLAYED
TO PROTECT THE SYSTEM, MUSIC FILE NOT ALLOWED TO BE DOWNLOADED.
TO PROTECT THE SYSTEM, VIDEO ATTACHMENT NOT ALLOWED TO BE VIEWED.
YOU JUST ALLOW TEXT?
THINK OF IT AS NOSTALGIA... NET SURFING AS IF IT WERE 1993...
©2009 King Features Syndicate, Inc. World rights reserved
http://www.onthefastrack.com
E-mail: bholbrook1@gmail.com

2009-02-03 On the Fastrack

washingtonpost.com

5

What about the user?

- The user remains a security risk…
  - Due to lack of knowledge…

WHAT PART OF THE COMPUTER SEEMS TO BE CAUSING THE SECURITY PROBLEM?
THE NUT AT THE KEYBOARD!
HIS

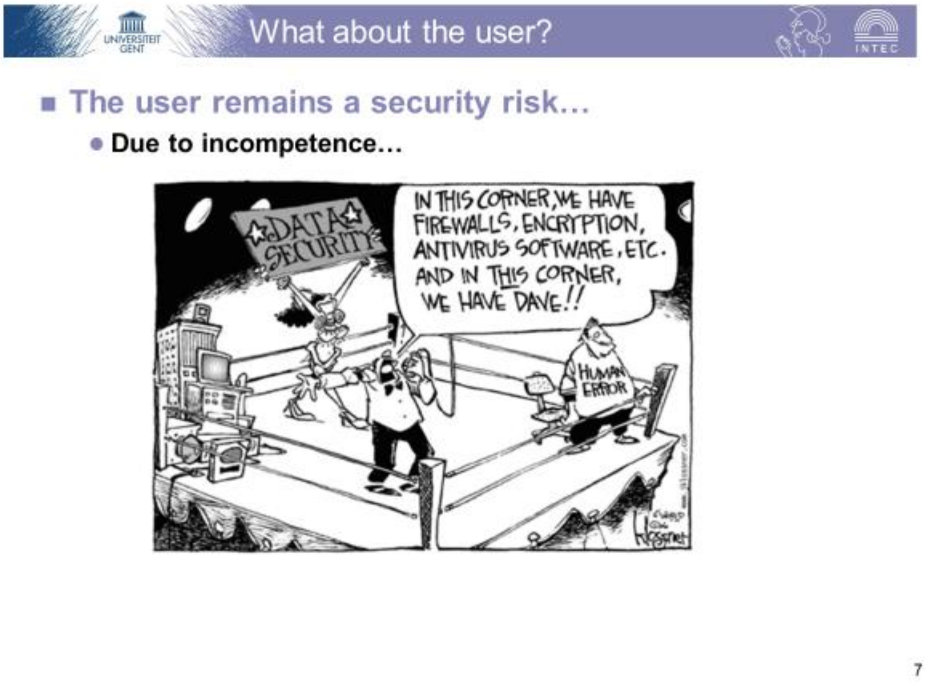
LA Times

1 in 10 in a survey think HTML is an STD

2014-03-04

http://www.latimes.com/business/technology/la-fi-tn-1-10-americans-html-std-study-finds-20140304-story.html

6

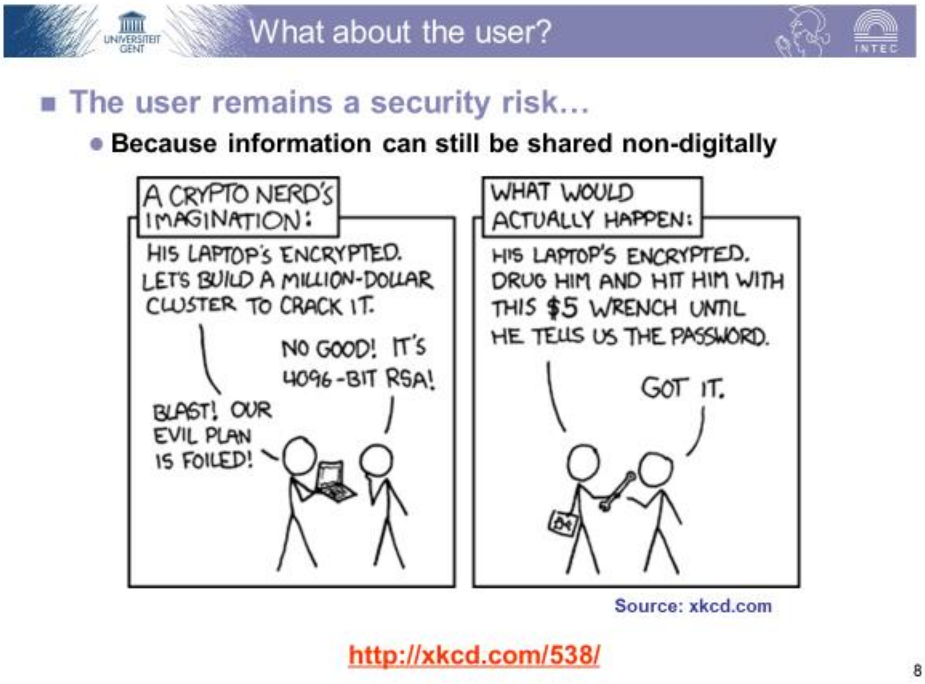


What about the user?

- The user remains a security risk…
  - Due to incompetence…

DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

7



What about the user?

- The user remains a security risk…
  - Because information can still be shared non-digitally

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Source: xkcd.com

http://xkcd.com/538/

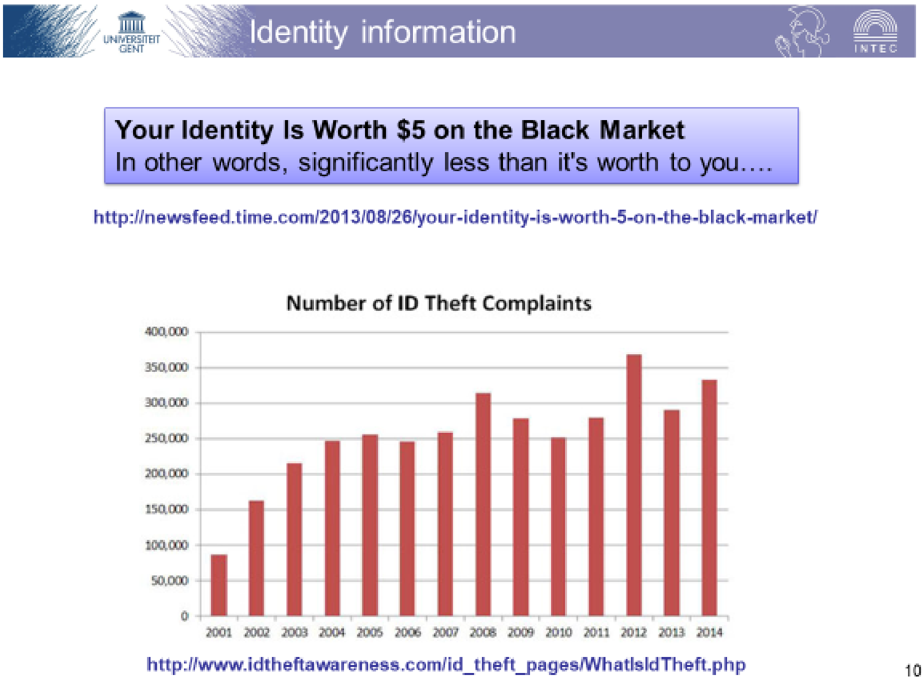
8

Social networks

© Randy Glasbergen
glasbergen.com

"I can't see your future, but I found your bank files, Social Security number and all of your company passwords."

9



Identity information

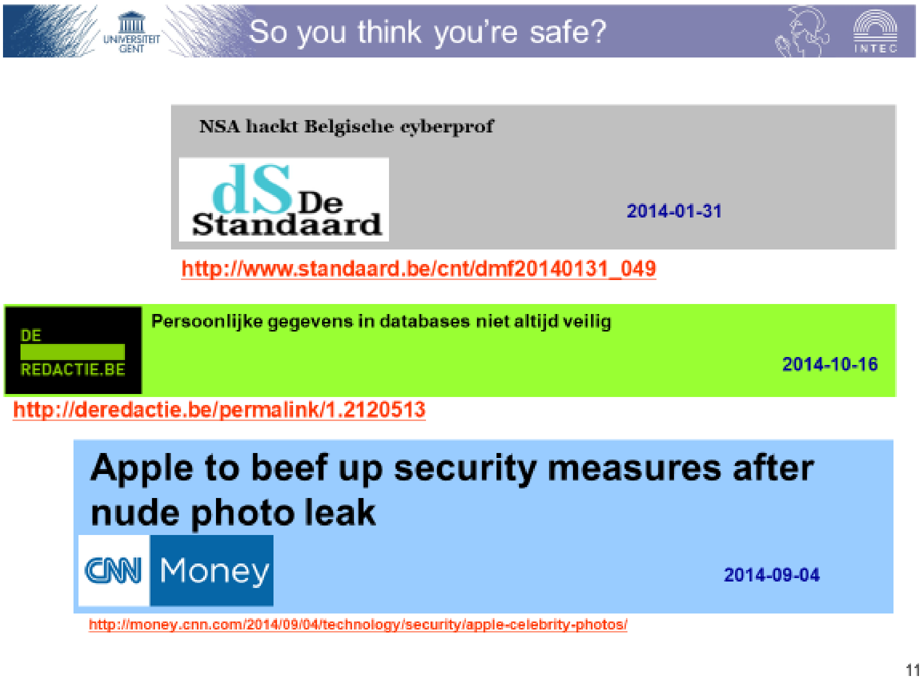
Your Identity Is Worth $5 on the Black Market
In other words, significantly less than it's worth to you….

http://newsfeed.time.com/2013/08/26/your-identity-is-worth-5-on-the-black-market/

Number of ID Theft Complaints

http://www.idtheftawareness.com/id_theft_pages/WhatIsIdTheft.php

10



So you think you're safe?

NSA hackt Belgische cyberprof

De Standaard

2014-01-31

http://www.standaard.be/cnt/dmf20140131_049

DE REDACTIE.BE

Persoonlijke gegevens in databases niet altijd veilig

2014-10-16

http://deredactie.be/permalink/1.2120513

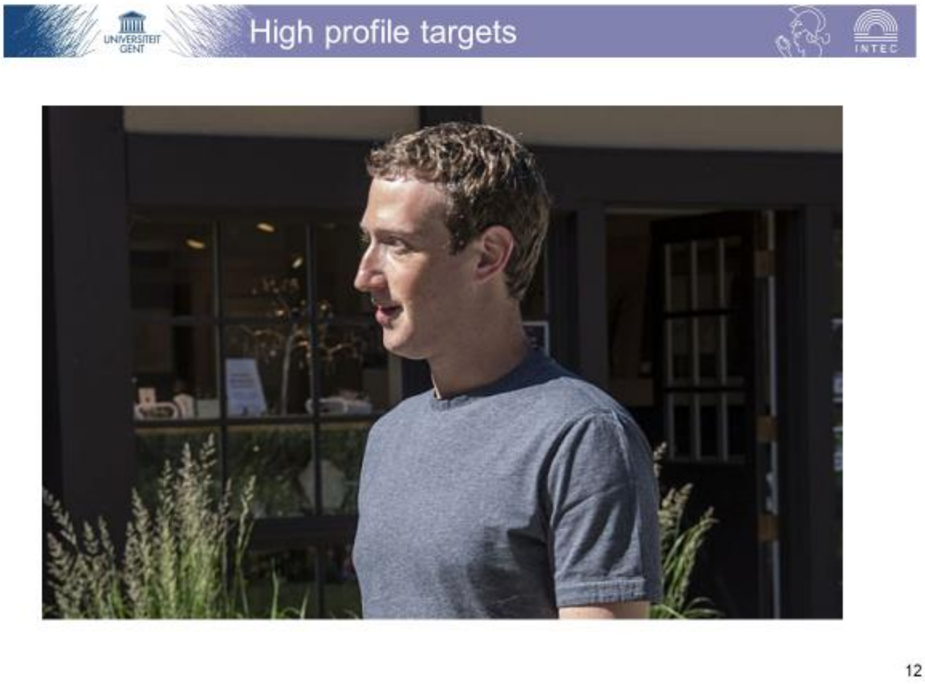
Apple to beef up security measures after nude photo leak

CNN Money

2014-09-04

http://money.cnn.com/2014/09/04/technology/security/apple-celebrity-photos/

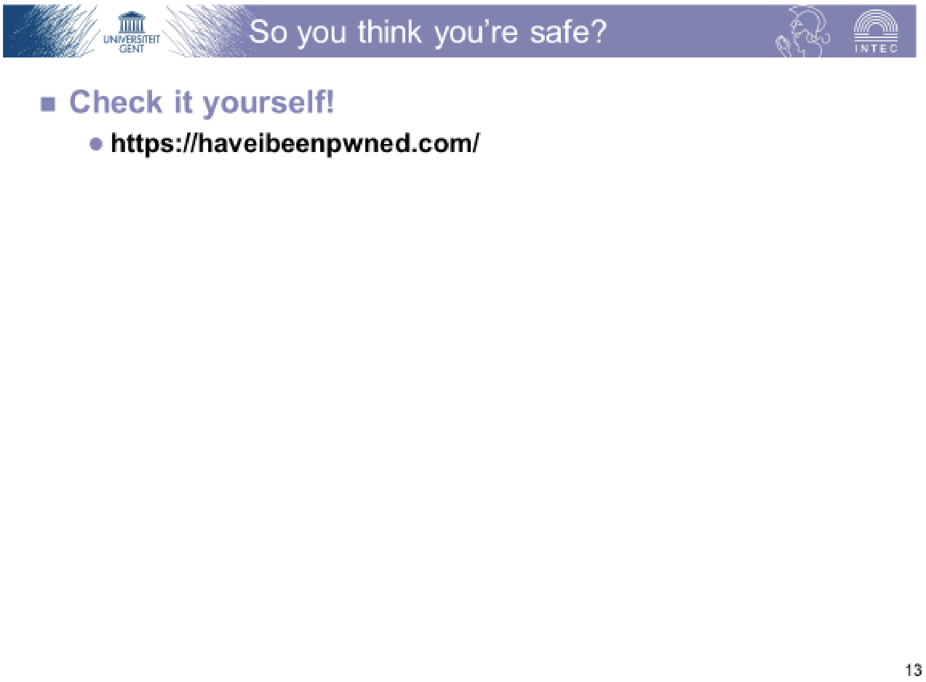
11



High profile targets

12

Facebook advises its users to never reuse a password on multiple accounts, The Wall Street Journal points out. Had its CEO and founder took this advice more seriously, he could have prevented his Twitter and Pinterest accounts from being hacked this past June. Zuckerberg's not-so-difficult-to-guess password “dadada” -- which was originally leaked in 2012 when 100 million LinkedIn passwords were stolen -- proved not so strong against hackers.



So you think you're safe?

- Check it yourself!
  - https://haveibeenpwned.com/

13

Privacy vs security

- "Defending Our Nation"?

PRIVAC
NSA
"SECURITY"
Data Mining
TOLES
EITHER ONE ?

2013-12-20 Tom Toles

washingtonpost.com

14

Privacy vs security

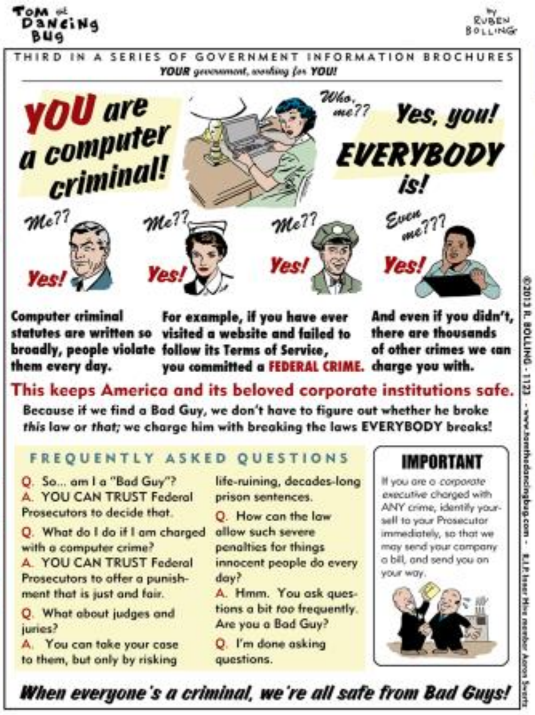
WAR IS PEACE
FREEDOM IS SLAVERY
IGNORANCE IS STRENGTH

George Orwell, "1984"

We are now 33 years later…

15

http://boingboing.net/2013/01/30/tom-the-dancing-bug-you-are.html


Tom the Dancing Bug
by Ruben Bolling
YOU are a computer criminal!
Who, me??
Yes, you! EVERYBODY is!
Me??
Yes!
Me??
Yes!
Me??
Yes!
Even me???
Yes!
©2013 R. BOLLING - 1123 - www.tomthedancingbug.com - R.I.P. Isser Mine member Aaron Swartz

THIRD IN A SERIES OF GOVERNMENT INFORMATION BROCHURES
YOUR government, working for YOU!

Computer criminal statutes are written so broadly, people violate them every day.

For example, if you have ever visited a website and failed to follow its Terms of Service, you committed a FEDERAL CRIME.

And even if you didn't, there are thousands of other crimes we can charge you with.

This keeps America and its beloved corporate institutions safe.

Because if we find a Bad Guy, we don't have to figure out whether he broke *this* law or *that;* we charge him with breaking the laws EVERYBODY breaks!

FREQUENTLY ASKED QUESTIONS

Q. So... am I a "Bad Guy"?
A. YOU CAN TRUST Federal Prosecutors to decide that.

Q. What do I do if I am charged with a computer crime?
A. YOU CAN TRUST Federal Prosecutors to offer a punishment that is just and fair.

Q. What about judges and juries?
A. You can take your case to them, but only by risking life-ruining, decades-long prison sentences.

Q. How can the law allow such severe penalties for things innocent people do every day?
A. Hmm. You ask questions a bit *too* frequently. Are you a Bad Guy?

Q. I'm done asking questions.

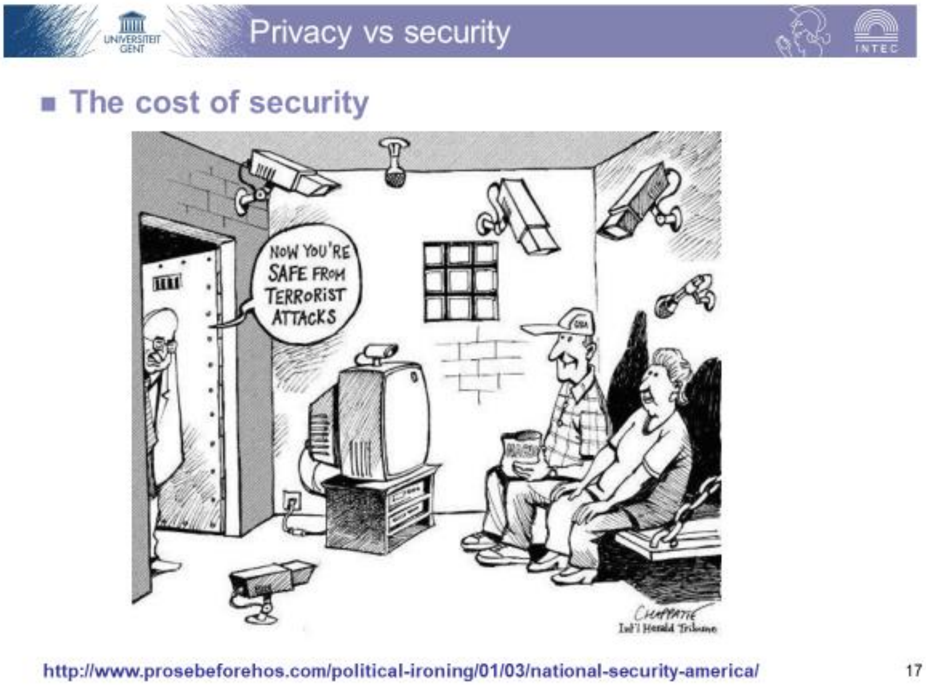
IMPORTANT

If you are a *corporate* executive charged with ANY crime, identify yourself to your Prosecutor immediately, so that we may send your company a bill, and send you on your way.

When everyone's a criminal, we're all safe from Bad Guys!

Source: dailykos.com

16


UNIVERSITEIT GENT
INTEC
NOW YOU'RE SAFE FROM TERRORIST ATTACKS
CHAPPATTE Int'l Herald Tribune

Privacy vs security

- The cost of security

http://www.prosebeforehos.com/political-ironing/01/03/national-security-america/

17

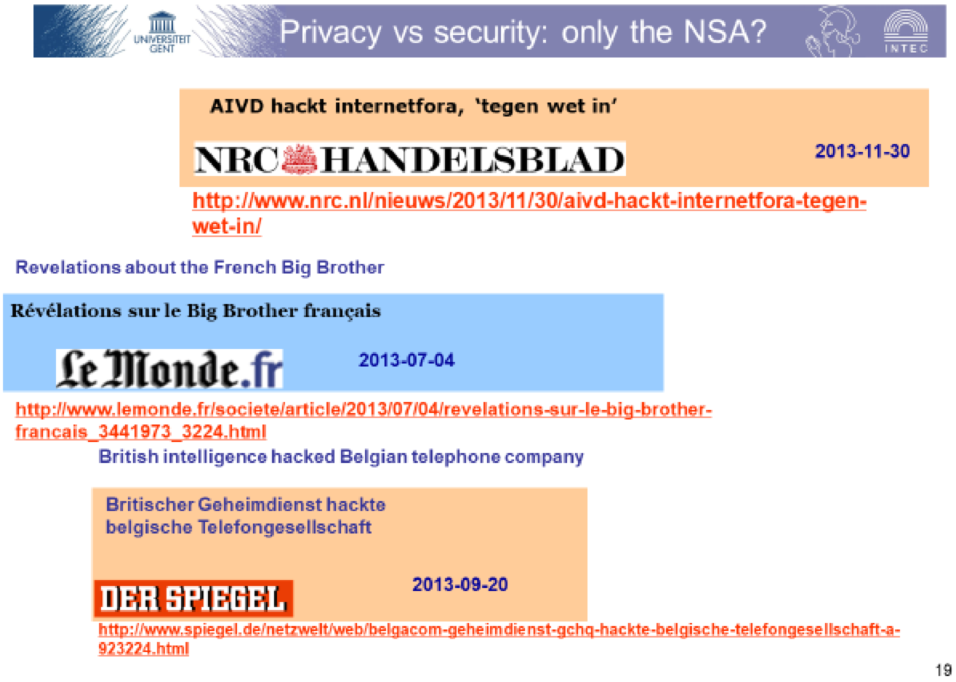
UNIVERSITEIT GENT
INTEC
HENRY, YOU DIDN'T JUST GOOGLE "BOMB" OR "JIHAD" OR SOMETHING, DID YOU?
BEN SARGENT

Privacy vs security

2013-10-31 Ben Sargent

washingtonpost.com

18



Privacy vs security: only the NSA?

AIVD hackt internetfora, 'tegen wet in'

NRC HANDELSBLAD 2013-11-30

http://www.nrc.nl/nieuws/2013/11/30/aivd-hackt-internetfora-tegen-wet-in/

Revelations about the French Big Brother

Révélations sur le Big Brother français

Le Monde.fr 2013-07-04

http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html

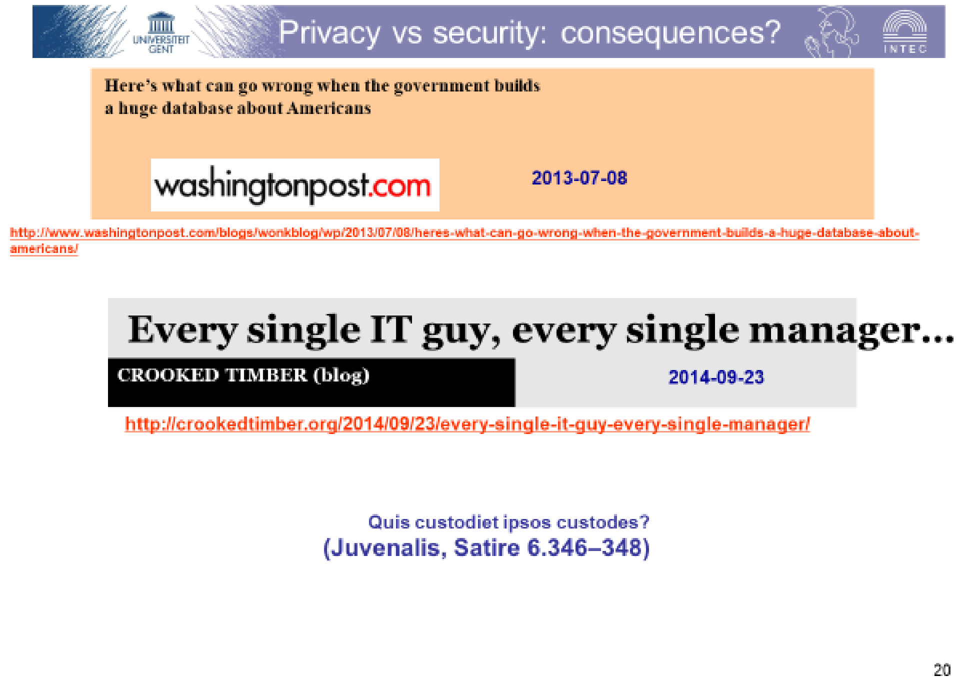
British intelligence hacked Belgian telephone company

Britischer Geheimdienst hackte belgische Telefongesellschaft

DER SPIEGEL 2013-09-20

http://www.spiegel.de/netzwelt/web/belgacom-geheimdienst-gchq-hackte-belgische-telefongesellschaft-a-923224.html

19



Privacy vs security: consequences?

Here's what can go wrong when the government builds a huge database about Americans

washingtonpost.com 2013-07-08

http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/08/heres-what-can-go-wrong-when-the-government-builds-a-huge-database-about-americans/

Every single IT guy, every single manager…

CROOKED TIMBER (blog) 2014-09-23

http://crookedtimber.org/2014/09/23/every-single-it-guy-every-single-manager/

Quis custodiet ipsos custodes?
(Juvenalis, Satire 6.346–348)

20

Privacy vs security: consequences?

- Hacking group that obtained several NSA hacking tools
  - First put them online for auction
  - Afterwards put online for free

21

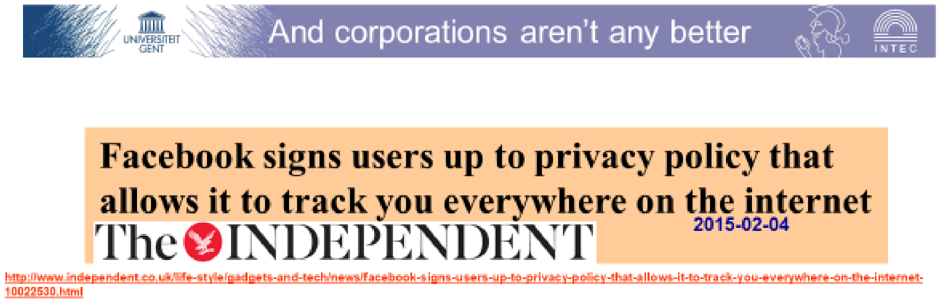
Privacy vs security: consequences?

NOW AND THEN, I ANNOUNCE "I KNOW YOU'RE LISTENING" TO EMPTY ROOMS.
IF I'M WRONG, NO ONE KNOWS.
AND IF I'M RIGHT, MAYBE I JUST FREAKED THE HELL OUT OF SOME SECRET ORGANIZATION.

http://xkcd.com/525/

Source: xkcd.com

22



And corporations aren't any better

Facebook signs users up to privacy policy that allows it to track you everywhere on the internet

The INDEPENDENT 2015-02-04

http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-signs-users-up-to-privacy-policy-that-allows-it-to-track-you-everywhere-on-the-internet-10022530.html

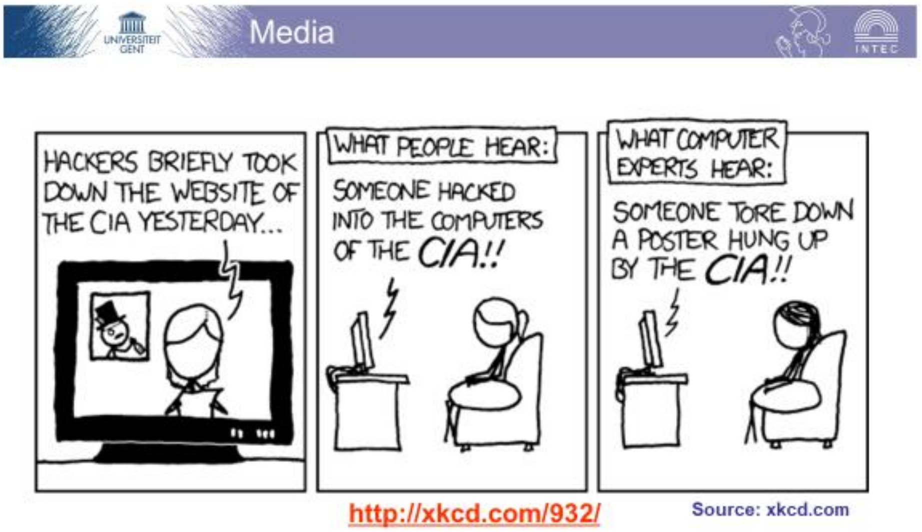
Does Uber Even Deserve Our Trust?

Forbes 2014-11-25

http://www.forbes.com/sites/chanellebessette/2014/11/25/does-uber-even-deserve-our-trust/

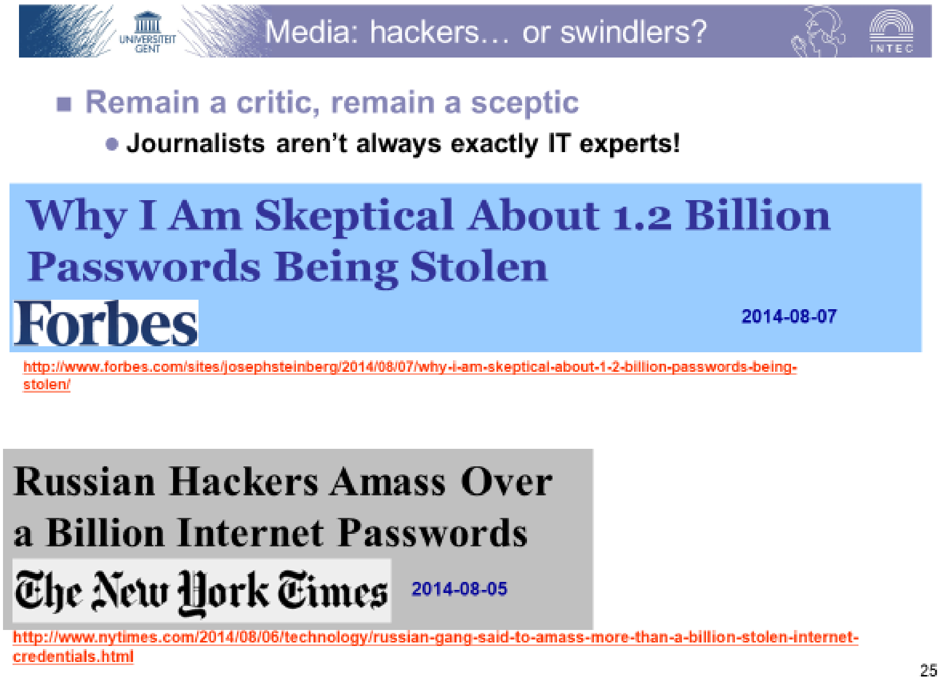
23

Media


HACKERS BRIEFLY TOOK DOWN THE WEBSITE OF THE CIA YESTERDAY...
WHAT PEOPLE HEAR:
SOMEONE HACKED INTO THE COMPUTERS OF THE CIA!!
WHAT COMPUTER EXPERTS HEAR:
SOMEONE TORE DOWN A POSTER HUNG UP BY THE CIA!!

http://xkcd.com/932/ Source: xkcd.com

24



Media: hackers… or swindlers?

- Remain a critic, remain a sceptic
  - Journalists aren't always exactly IT experts!

Why I Am Skeptical About 1.2 Billion Passwords Being Stolen

Forbes 2014-08-07

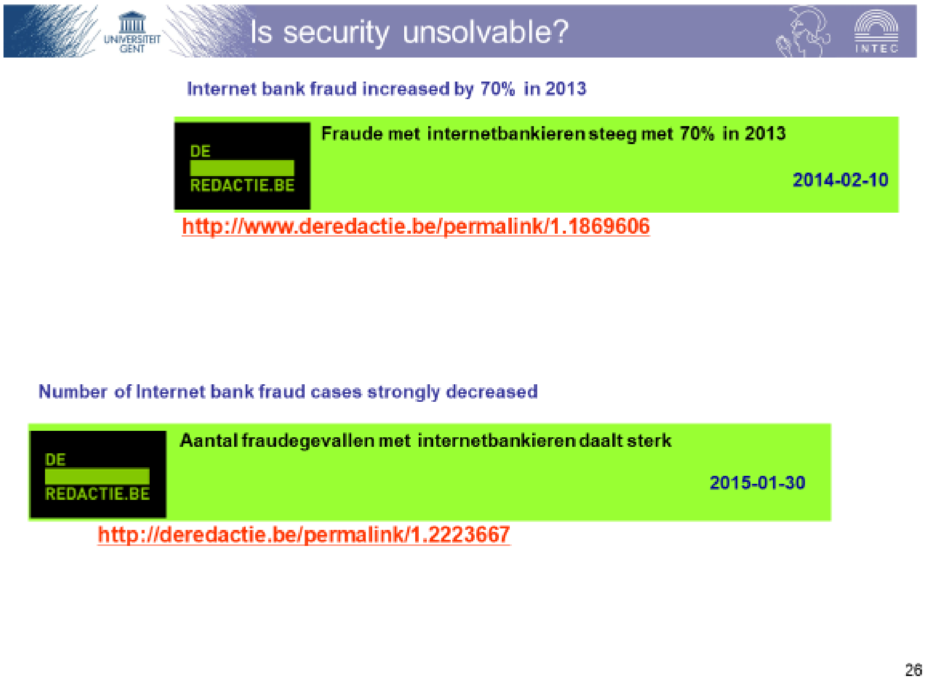
http://www.forbes.com/sites/josephsteinberg/2014/08/07/why-i-am-skeptical-about-1-2-billion-passwords-being-stolen/

Russian Hackers Amass Over a Billion Internet Passwords

The New York Times 2014-08-05

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

25



Is security unsolvable?

Internet bank fraud increased by 70% in 2013

DE REDACTIE.BE Fraude met internetbankieren steeg met 70% in 2013 2014-02-10

http://www.deredactie.be/permalink/1.1869606

Number of Internet bank fraud cases strongly decreased

DE REDACTIE.BE Aantal fraudegevallen met internetbankieren daalt sterk 2015-01-30

http://deredactie.be/permalink/1.2223667

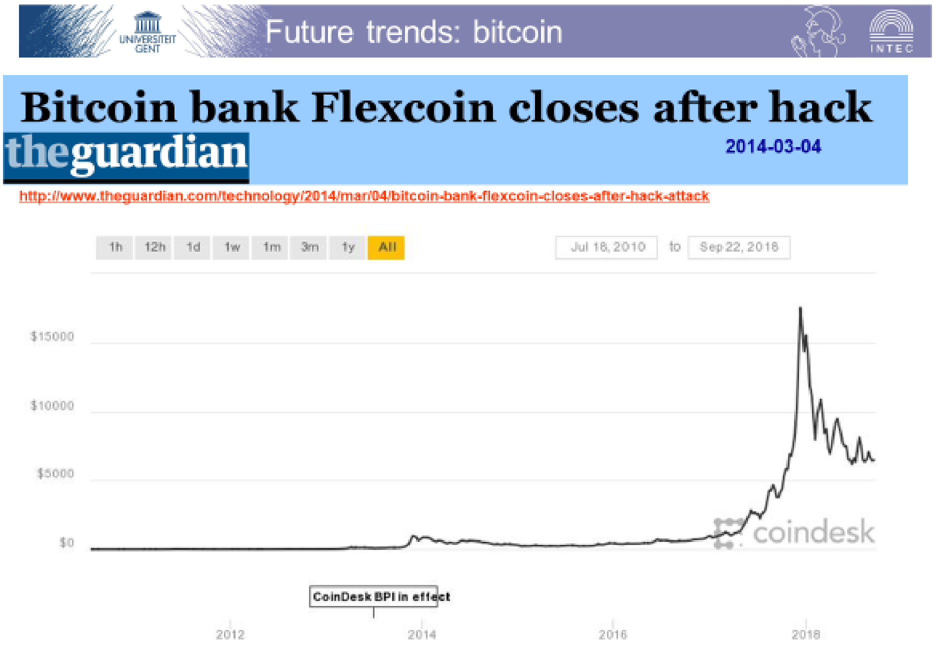
26

Future trends: bitcoin

- Hackers steel $65 million from BitFinex
  - The future for modern day bank robbers?

27

Recognized as the second largest Bitcoin hack in history, criminals managed to break into BitFinex -- a Hong Kong exchange -- and steal more than $65 million-worth of digital currency. As the incident is investigated, the nature of the break in remains unknown as well as the identity of the responsible party.



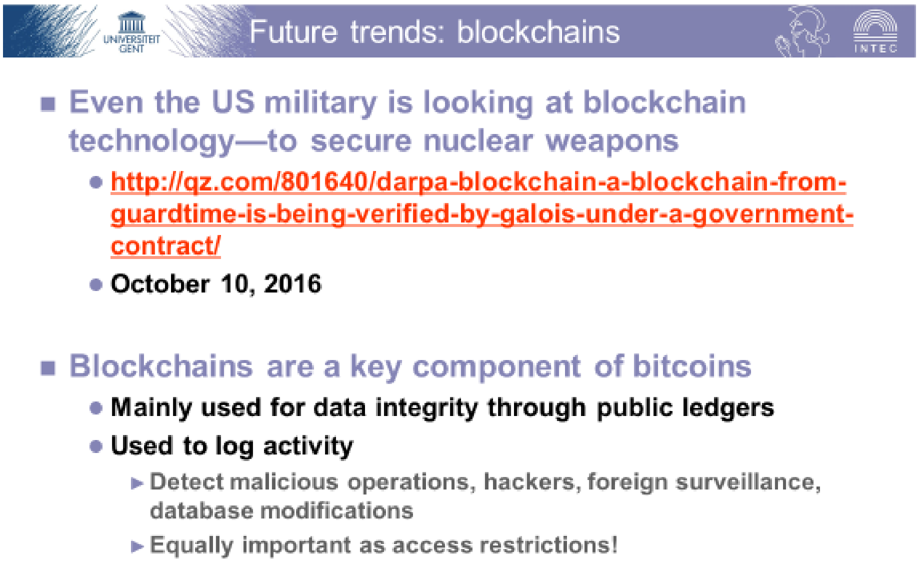
Future trends: bitcoin

Bitcoin bank Flexcoin closes after hack

theguardian 2014-03-04

http://www.theguardian.com/technology/2014/mar/04/bitcoin-bank-flexcoin-closes-after-hack-attack

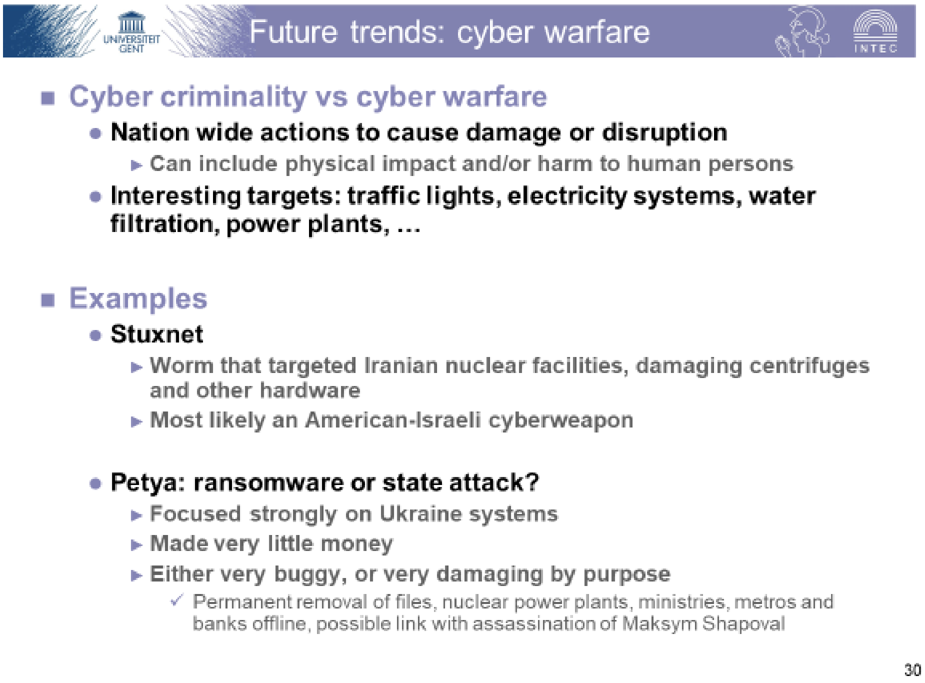
28



Future trends: blockchains

- Even the US military is looking at blockchain technology—to secure nuclear weapons
  - http://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/
  - October 10, 2016
- Blockchains are a key component of bitcoins
  - Mainly used for data integrity through public ledgers
  - Used to log activity
    - Detect malicious operations, hackers, foreign surveillance, database modifications
    - Equally important as access restrictions!

29



Future trends: cyber warfare

- Cyber criminality vs cyber warfare
  - Nation wide actions to cause damage or disruption
    - Can include physical impact and/or harm to human persons
  - Interesting targets: traffic lights, electricity systems, water filtration, power plants, …
- Examples
  - Stuxnet
    - Worm that targeted Iranian nuclear facilities, damaging centrifuges and other hardware
    - Most likely an American-Israeli cyberweapon
  - Petya: ransomware or state attack?
    - Focused strongly on Ukraine systems
    - Made very little money
    - Either very buggy, or very damaging by purpose
      - ✓ Permanent removal of files, nuclear power plants, ministries, metros and banks offline, possible link with assassination of Maksym Shapoval

30

The difference between cyber criminality and cyber warfare is often denoted as the real-world physical impact; whereby cyber criminality will often have a clear impact to the real world, cyber warfare adds the physical impact to such activities (cyber warfare results in people being physically harmed in the real world). The image of the hacker wearing a hoody at night in a basement is long gone; organized crime and even state actors have found their way to cyberspace. The threat of real-world physical damage was probably first widely demonstrated by Stuxnet, and the threat of cyber criminals (or warriors) taking over traffic lights, nuclear power plants and water filtration plants is more prominent than ever.

Further research and investigation into Petya ransomware -- which has affected computers in over 60 countries -- suggest three interesting things: 1. Ukraine was the epicentre of the attack. According to Kaspersky, 60 percent of all machines infected were located within Ukraine. 2. The attackers behind the attack have made little money -- around $10,000. Which leads to speculation that perhaps money wasn't a motive at all. 3. Petya was either "incredibly buggy, or irreversibly destructive on purpose." Because the virus has proven unusually destructive in Ukraine, a number of researchers have come to suspect more sinister motives at work. Peeling apart the program's decryption failure in a post today, Comae's Matthieu Suiche concluded a nation state attack was the only plausible explanation. "Pretending to be a ransomware while being in fact a nation state attack," Suiche wrote, "is in our opinion a very subtle way from the attacker to control the narrative of the attack." Another prominent infosec figure put it more bluntly: "There's no fucking way this was criminals." There's already mounting evidence that Petya's focus on Ukraine was deliberate. The Petya virus is very good at moving within networks, but initial attacks were limited to just a few specific infections, all of which seem to have been targeted at Ukraine. The highest-profile one was a Ukrainian accounting program called MeDoc, which sent out a suspicious software update Tuesday morning that many researchers blame for the initial Petya infections. Attackers also planted malware on the homepage of a prominent Ukraine-based news outlet, according to one researcher at Kaspersky.

Future trends: IoT

Well-Dressed couple, circa 2020
iSEE CONTACTS
iRINGS
iSPORTS BRA
iWATCH
iPHABLET WITH iPAY
iSKIRT
iHEEL SHOES
iGLASSES
iTEETH
iTACK
iWATCH
iBRIEFS
iPANTS
iSOLES
CARLSON

2014-09-15 Stuart Carlson

washingtonpost.com

31

Future trends: IoT

- How far is this future?

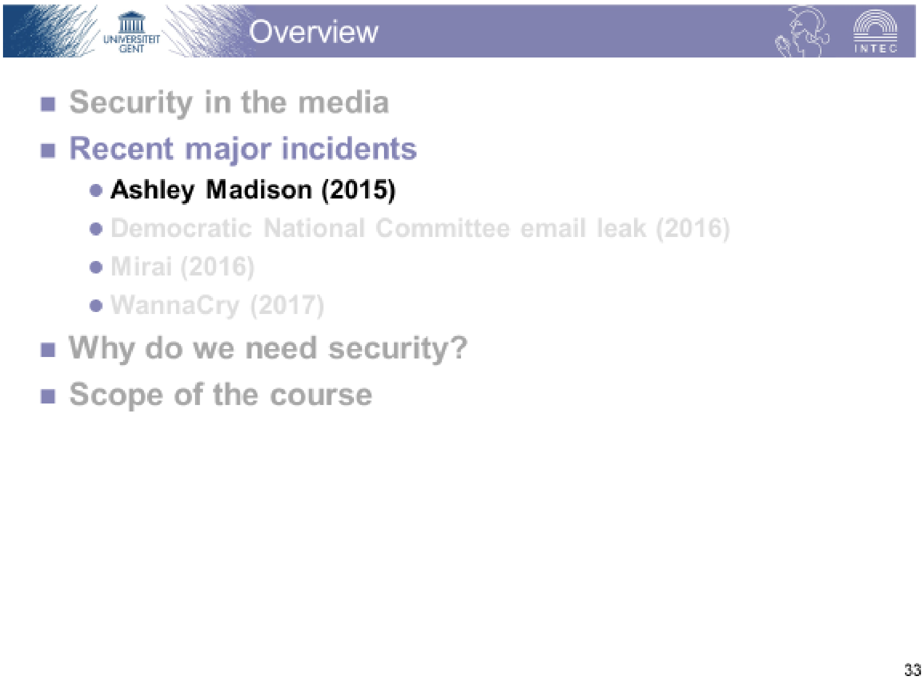
Cheney's defibrillator was modified to prevent hacking

CNN

2013-10-24

http://www.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/

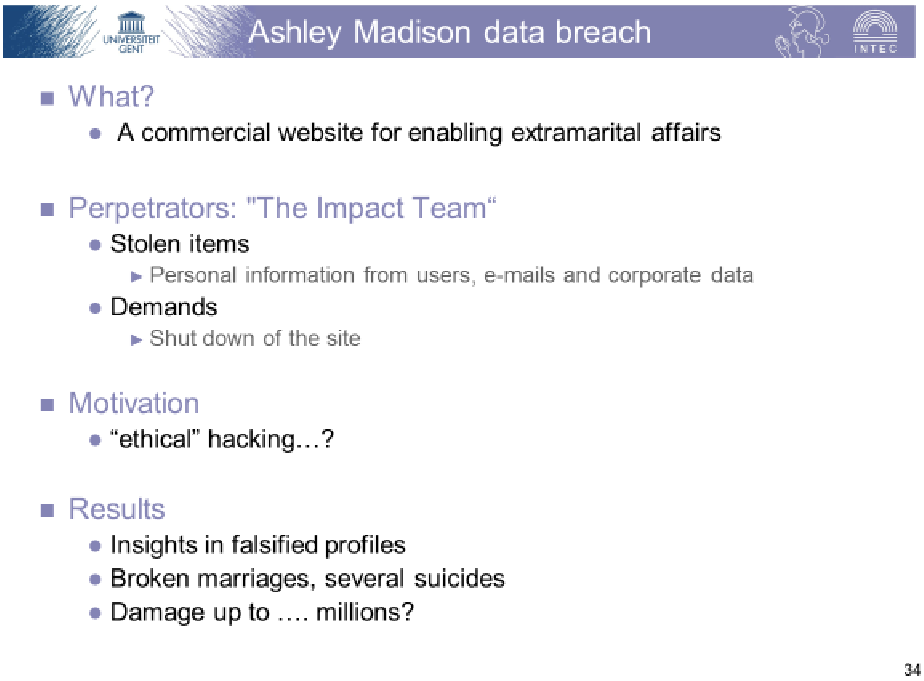
32



Overview

- Security in the media
- Recent major incidents
  - Ashley Madison (2015)
  - Democratic National Committee email leak (2016)
  - Mirai (2016)
  - WannaCry (2017)
- Why do we need security?
- Scope of the course

33

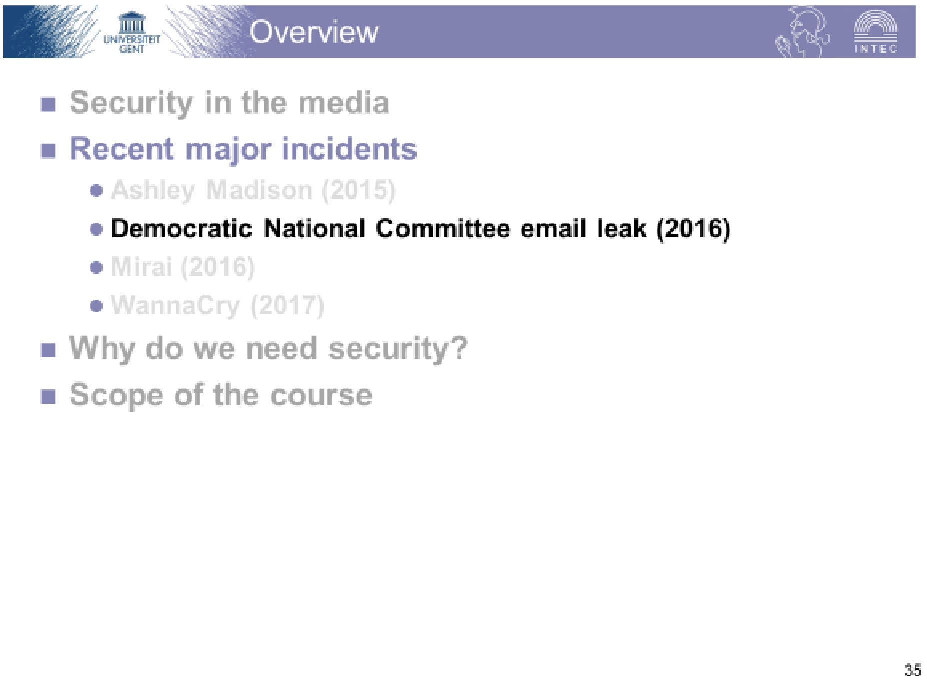


Ashley Madison data breach

- What?
  - A commercial website for enabling extramarital affairs
- Perpetrators: "The Impact Team“
  - Stolen items
    - Personal information from users, e-mails and corporate data
  - Demands
    - Shut down of the site
- Motivation
  - “ethical” hacking…?
- Results
  - Insights in falsified profiles
  - Broken marriages, several suicides
  - Damage up to …. millions?

34

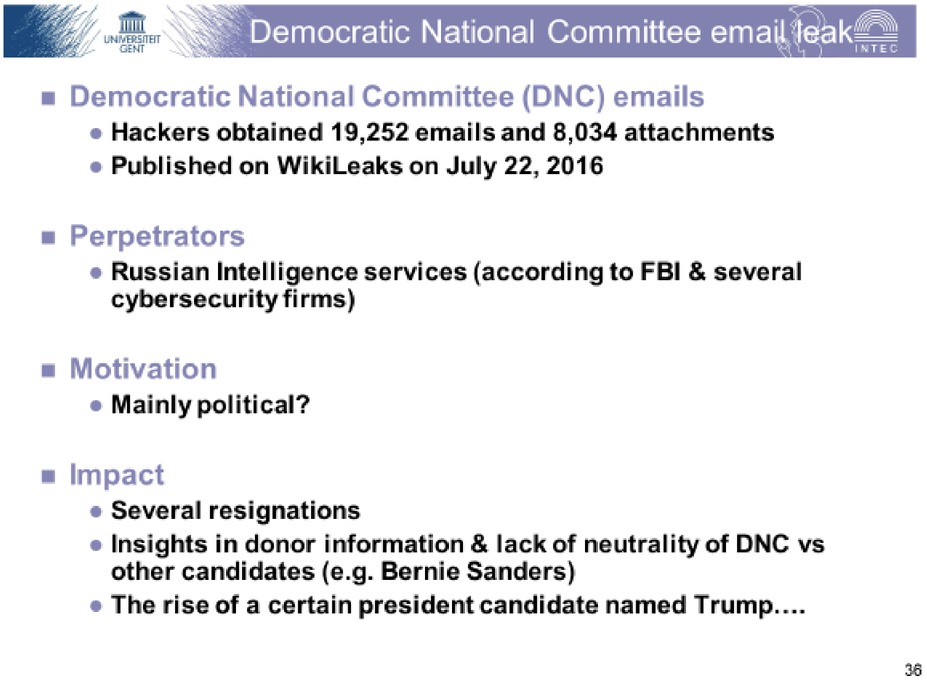
Passwords on the live site were hashed using the bcrypt algorithm. A security analyst using the Hashcat password recovery tool with a dictionary based on the RockYou passwords found that among the 4,000 passwords that were the easiest to crack, "123456" and "password" were the most commonly used passwords on the live website. An analysis of old passwords used on an archived version showed that "123456" and "password" were the most common. Due to a coding error where passwords were hashed with both bcrypt and md5. 11 million passwords were eventually cracked.



Overview

- Security in the media
- Recent major incidents
  - Ashley Madison (2015)
  - Democratic National Committee email leak (2016)
  - Mirai (2016)
  - WannaCry (2017)
- Why do we need security?
- Scope of the course

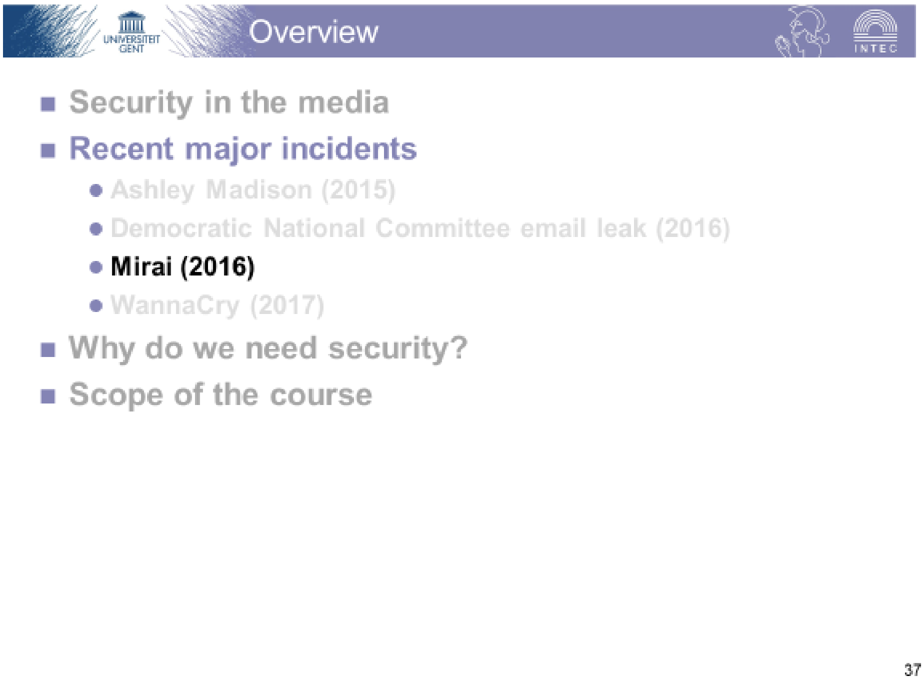
35



Democratic National Committee email leak

- Democratic National Committee (DNC) emails
  - Hackers obtained 19,252 emails and 8,034 attachments
  - Published on WikiLeaks on July 22, 2016
- Perpetrators
  - Russian Intelligence services (according to FBI & several cybersecurity firms)
- Motivation
  - Mainly political?
- Impact
  - Several resignations
  - Insights in donor information & lack of neutrality of DNC vs other candidates (e.g. Bernie Sanders)
  - The rise of a certain president candidate named Trump….

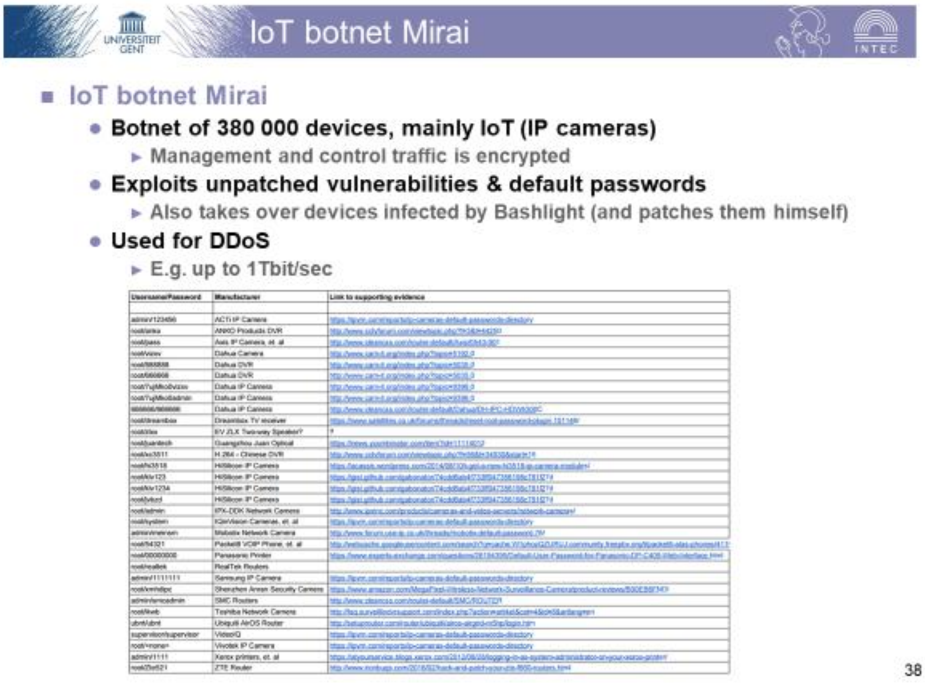
36



Overview

- Security in the media
- Recent major incidents
  - Ashley Madison (2015)
  - Democratic National Committee email leak (2016)
  - **Mirai (2016)**
  - WannaCry (2017)
- Why do we need security?
- Scope of the course

37



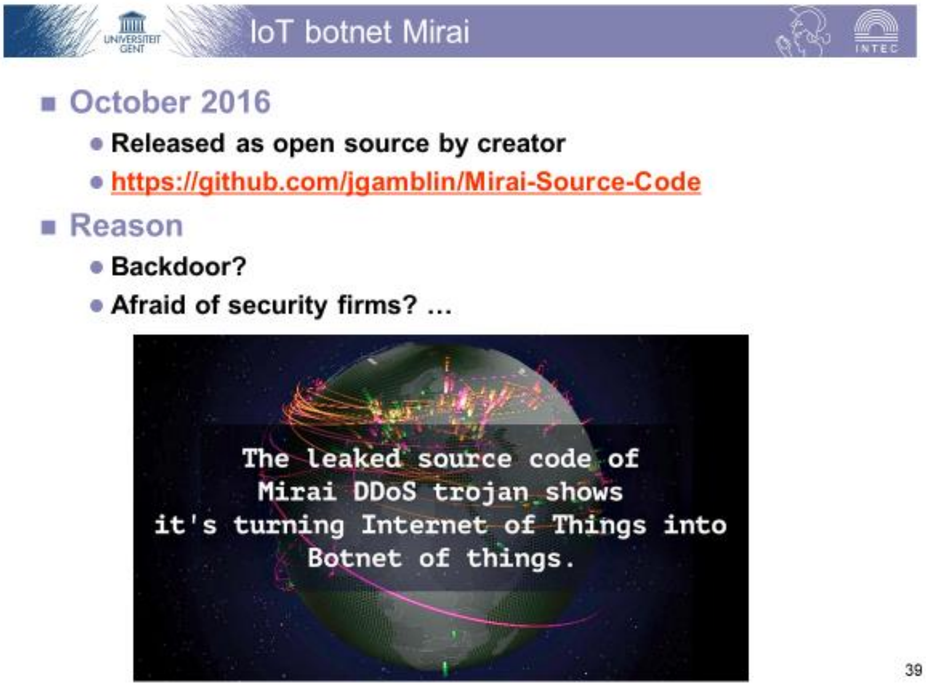
IoT botnet Mirai

- IoT botnet Mirai
  - **Botnet of 380 000 devices, mainly IoT (IP cameras)**
    - Management and control traffic is encrypted
  - **Exploits unpatched vulnerabilities & default passwords**
    - Also takes over devices infected by Bashlight (and patches them himself)
  - **Used for DDoS**
    - E.g. up to 1Tbit/sec

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

38

https://arstechnica.com/information-technology/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/



IoT botnet Mirai

- October 2016
  - Released as open source by creator
  - https://github.com/jgamblin/Mirai-Source-Code
- Reason
  - Backdoor?
  - Afraid of security firms? …

The leaked source code of Mirai DDoS trojan shows it's turning Internet of Things into Botnet of things.

39

https://arstechnica.com/information-technology/2016/10/double-dip-internet-of-things-botnet-attack-felt-across-the-internet/

https://tweakers.net/nieuws/116329/broncode-van-malware-achter-iot-botnet-mirai-verschijnt-online.html

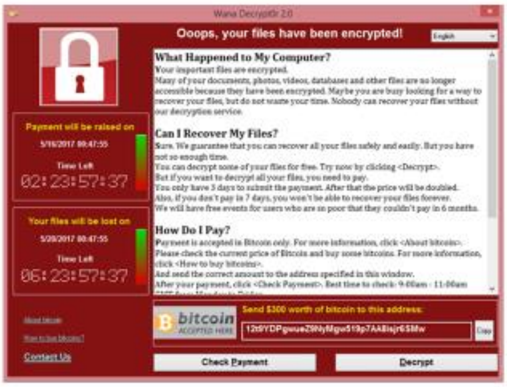
Overview

- Security in the media
- Recent major incidents
  - Ashley Madison (2015)
  - Democratic National Committee email leak (2016)
  - Mirai (2016)
  - WannaCry (2017)
- Why do we need security?
- Scope of the course

40

WannaCry

- Ransomware
  - Encryption of PC data
  - Utilized exploit of Windows SMB
    - Previously discovered and exploited by NSA, but never reported
  - 200,000 infected computers across 150 countries



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

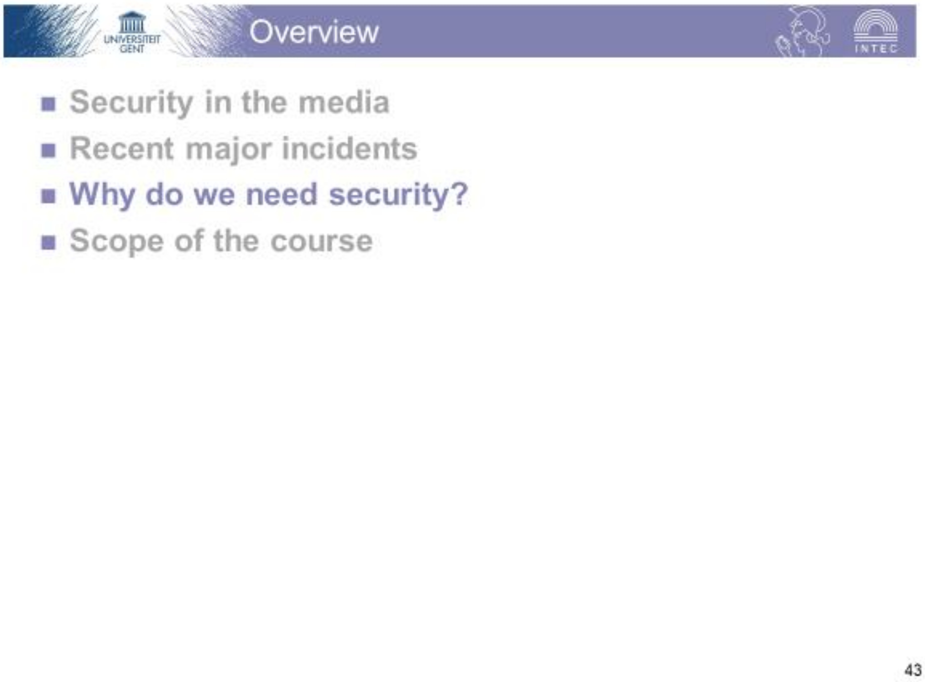
41

Facebook & Cambridge Analytica

42

Cambridge Analytica is a UK-based data analytics firm, whose parent company is Strategic Communication Laboratories. Cambridge Analytica helps political campaigns reach potential voters online. The firm combines data from multiple sources, including online information and polling, to build "profiles" of voters. It then uses computer programs to predict voter behavior, which could be influenced through specialized advertisements aimed at the voters. Cambridge Analytica reportedly acquired the data in a way that violated the social network's policies. It then reportedly tapped the information to build psychographic profiles of users and their friends, which were used for targeted political ads in the UK's Brexit referendum campaign, as well as by Trump's team during the 2016 US election.

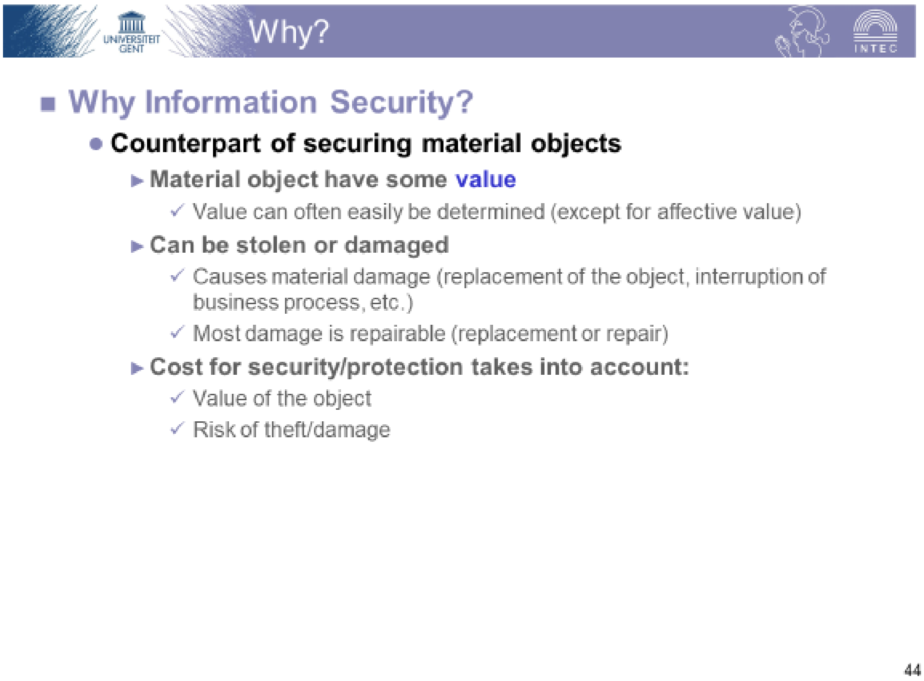
Facebook said in a statement on March 16 that Cambridge Analytica received user data from Aleksandr Kogan, a lecturer at the University of Cambridge. Kogan reportedly created an app called "thisisyourdigitallife" that ostensibly offered personality predictions to users while calling itself a research tool for psychologists. The app asked users to log in using their Facebook accounts. As part of the login process, it asked for access to users' Facebook profiles, locations, what they liked on the service, and importantly, their friends' data as well. The problem, Facebook says, is that Kogan then sent this user data to Cambridge Analytica without user permission, something that's against the social network's rules. The New York Times characterized the original problem as a data "breach" and said it's "one of the largest data leaks in the social network's history." That's in part because the roughly 270,000 users who gave Kogan access to their information allowed him to collect data on their friends as well. In total, more than 87 million Facebook users are said to have been affected. Facebook has been fined half a millions pound by the British privacy commission, the largest fine possible.



Overview

- Security in the media
- Recent major incidents
- Why do we need security?
- Scope of the course

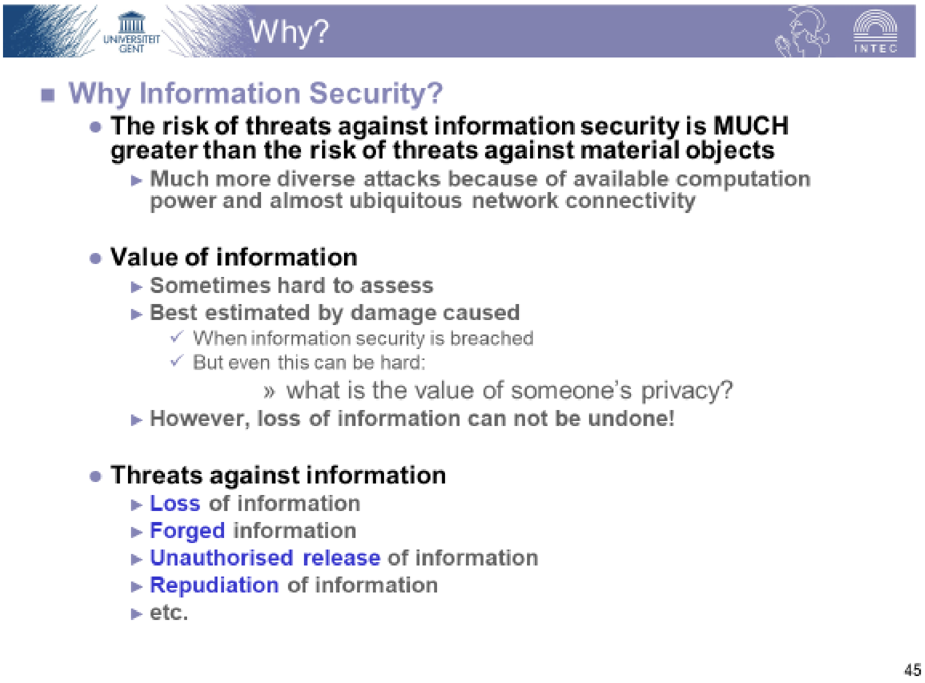
43



Why?

- Why Information Security?
  - Counterpart of securing material objects
    - Material object have some **value**
      - ✓ Value can often easily be determined (except for affective value)
    - Can be stolen or damaged
      - ✓ Causes material damage (replacement of the object, interruption of business process, etc.)
      - ✓ Most damage is repairable (replacement or repair)
    - Cost for security/protection takes into account:
      - ✓ Value of the object
      - ✓ Risk of theft/damage

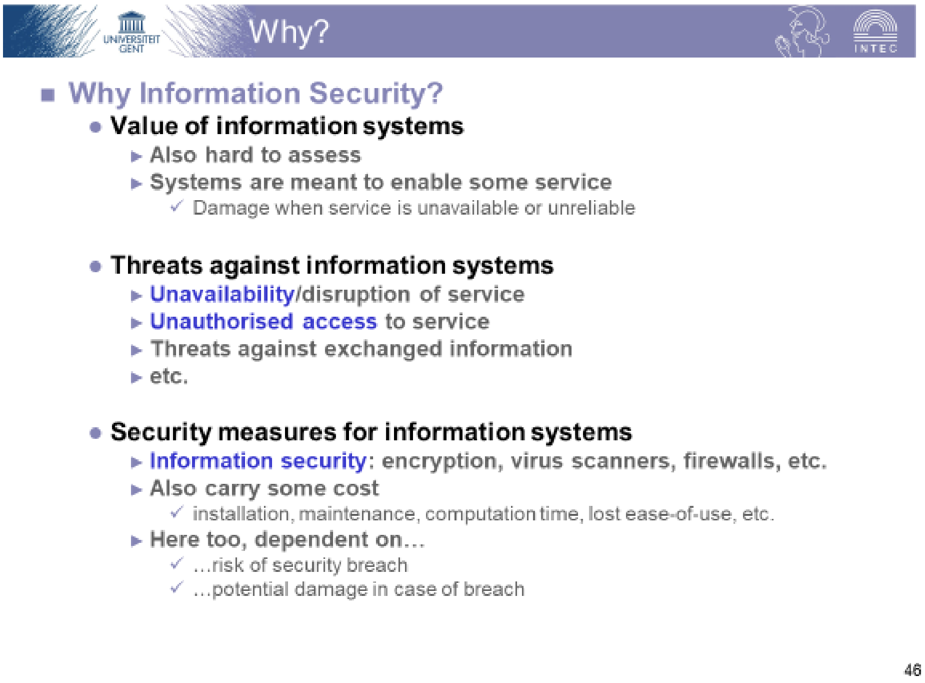
44



Why?

- Why Information Security?
  - **The risk of threats against information security is MUCH greater than the risk of threats against material objects**
    - Much more diverse attacks because of available computation power and almost ubiquitous network connectivity
  - **Value of information**
    - Sometimes hard to assess
    - Best estimated by damage caused
      - ✓ When information security is breached
      - ✓ But even this can be hard:
        - » what is the value of someone's privacy?
    - However, loss of information can not be undone!
  - **Threats against information**
    - Loss of information
    - Forged information
    - Unauthorised release of information
    - Repudiation of information
    - etc.

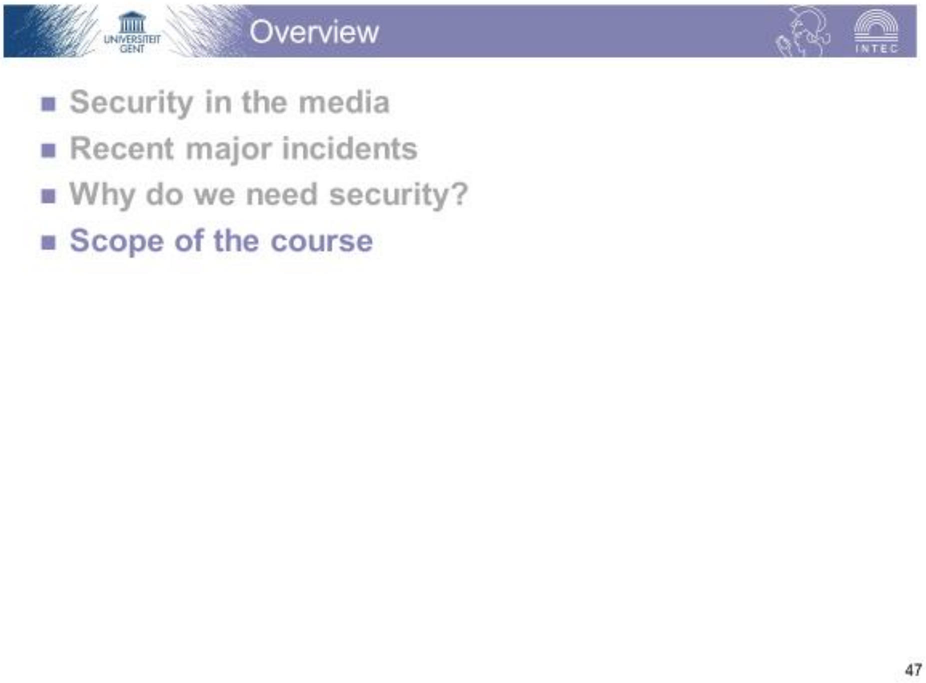
45



Why?

- Why Information Security?
  - **Value of information systems**
    - Also hard to assess
    - Systems are meant to enable some service
      - ✓ Damage when service is unavailable or unreliable
  - **Threats against information systems**
    - Unavailability/disruption of service
    - Unauthorised access to service
    - Threats against exchanged information
    - etc.
  - **Security measures for information systems**
    - Information security: encryption, virus scanners, firewalls, etc.
    - Also carry some cost
      - ✓ installation, maintenance, computation time, lost ease-of-use, etc.
    - Here too, dependent on…
      - ✓ …risk of security breach
      - ✓ …potential damage in case of breach

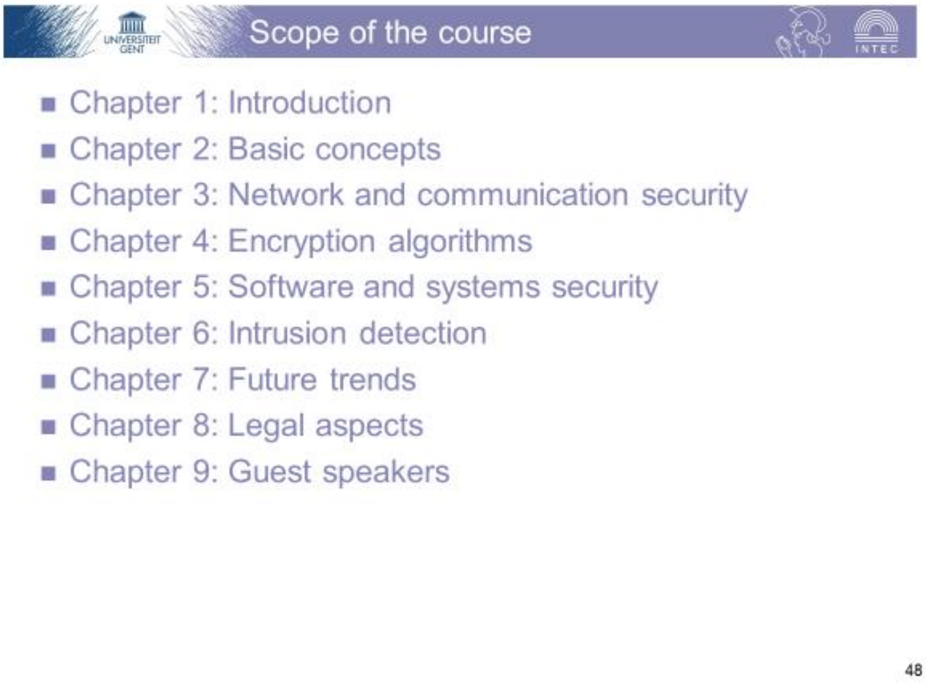
46



Overview

- Security in the media
- Recent major incidents
- Why do we need security?
- **Scope of the course**

47



Scope of the course

- Chapter 1: Introduction
- Chapter 2: Basic concepts
- Chapter 3: Network and communication security
- Chapter 4: Encryption algorithms
- Chapter 5: Software and systems security
- Chapter 6: Intrusion detection
- Chapter 7: Future trends
- Chapter 8: Legal aspects
- Chapter 9: Guest speakers

48