Imperial College
London

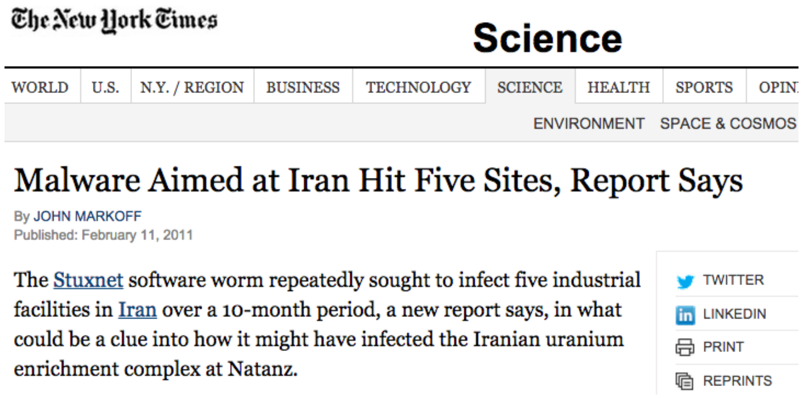
CO331 – Network and Web Security

1. Cybersecurity

Dr Sergio Maffeis
Department of Computing
Course web page: http://www.doc.ic.ac.uk/~maffeis/331

Stuxnet 2010

- Worm that spread on Windows machines aiming to reach specific Siemens controllers
- Would operate controller in a way to damage uranium-enriching centrifuges
- All hints pointed to secret USA +Israel joint effort
- First example of cyber weapon creating serious physical damage to critical infrastructure
- Now security of ICS is hot topic



The New York Times

Science

Malware Aimed at Iran Hit Five Sites, Report Says

By JOHN MARKOFF
Published: February 11, 2011

The Stuxnet software worm repeatedly sought to infect five industrial facilities in Iran over a 10-month period, a new report says, in what could be a clue into how it might have infected the Iranian uranium enrichment complex at Natanz.

Target 2013

- Hackers sent targeted email with malware to employee of HVAC (Target subcontractor)
- HVAC machines had access to Target internal network (for billing, etc.)
- Malware spread to Target machines
- Attackers stole data of 40 million customers
  - Unencrypted credit card information
  - Encrypted PINs
- Economic cost: + $200M

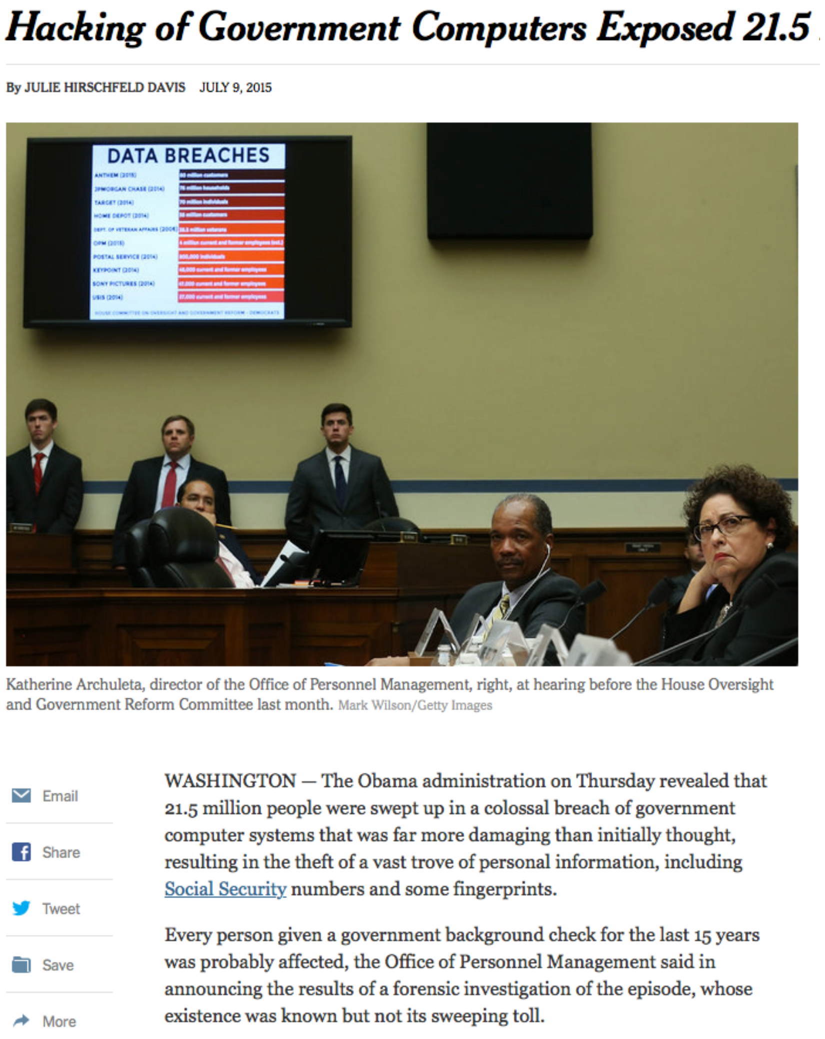
Sony 2014

- Responsibility claimed by “Guardians Of Peace” hacking group
  - Possibly motivated by planned release of satirical movie *The Interview*
  - NSA blamed North Korea
- Machines on corporate network infected
  - Probably users installed fake updates signed with a stolen Sony certificate
  - *Destover* malware: backdoor and rootkit (example of Advanced Persistent Threat)
- Leak of unreleased films and scripts, employee emails, salaries and passwords, other sensitive information (possibly terabytes of data)
- Collateral damage: leak of employees personal emails put some of them in trouble

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU
NEIGHBORS AND THIS IS THE END
전쟁은 시작될것이다
SETH ROGEN
JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE
INTERVIEW
인터뷰
인터뷰

U.S. Gov 2015

- Attacks "originated in China" according to US authorities
  - Location of cyberattack is not proof of intent
- Computer intrusions using compromised credentials of a contractor
  - On the Interior Department network
  - At the Office of Personal Management
- Two decades of warning from auditors about vulnerabilities
  - Two-factor authentication would have prevented hack
  - Lessons from Target hack ignored
- Attackers stole 21.5 million personal records
  - Data included Social Security numbers, fingerprints, addresses, health and financial history
  - Sensitive targets: every person given a government background check in the last 15 years



Hacking of Government Computers Exposed 21.5

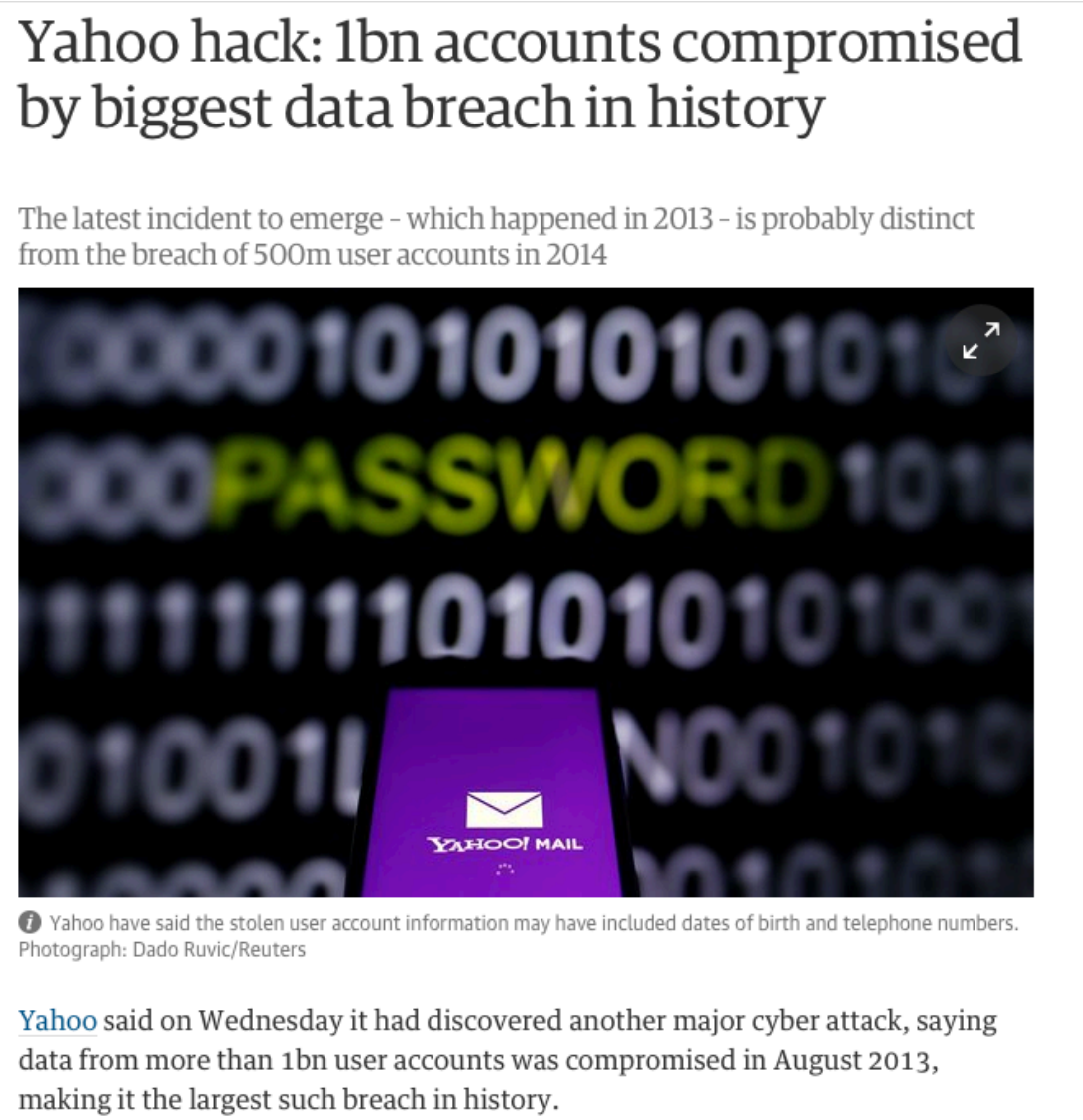
By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than initially thought, resulting in the theft of a vast trove of personal information, including Social Security numbers and some fingerprints.

Every person given a government background check for the last 15 years was probably affected, the Office of Personnel Management said in announcing the results of a forensic investigation of the episode, whose existence was known but not its sweeping toll.

And the winner is…



Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge - which happened in 2013 - is probably distinct from the breach of 500m user accounts in 2014

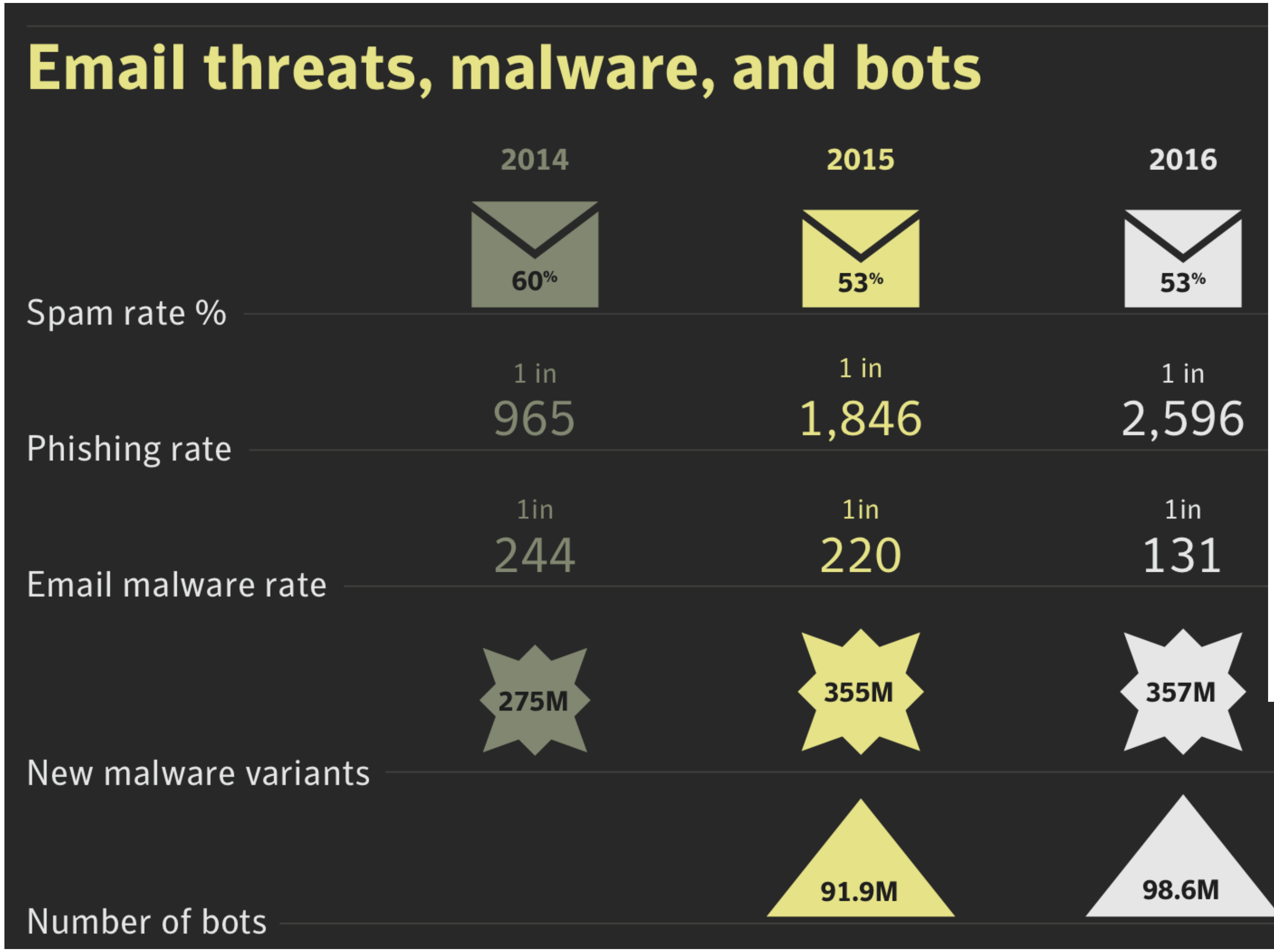
Yahoo have said the stolen user account information may have included dates of birth and telephone numbers. Photograph: Dado Ruvic/Reuters

Yahoo said on Wednesday it had discovered another major cyber attack, saying data from more than 1bn user accounts was compromised in August 2013, making it the largest such breach in history.

- Happened in 2013, discovered in 2016
- Theft of personal data
  - encrypted passwords
  - security questions & answers
- “not been able to identify the intrusion associated with this theft”
  - Perhaps attackers forged cookies to gain unauthenticated access (you will understand)
- The perfect heist.

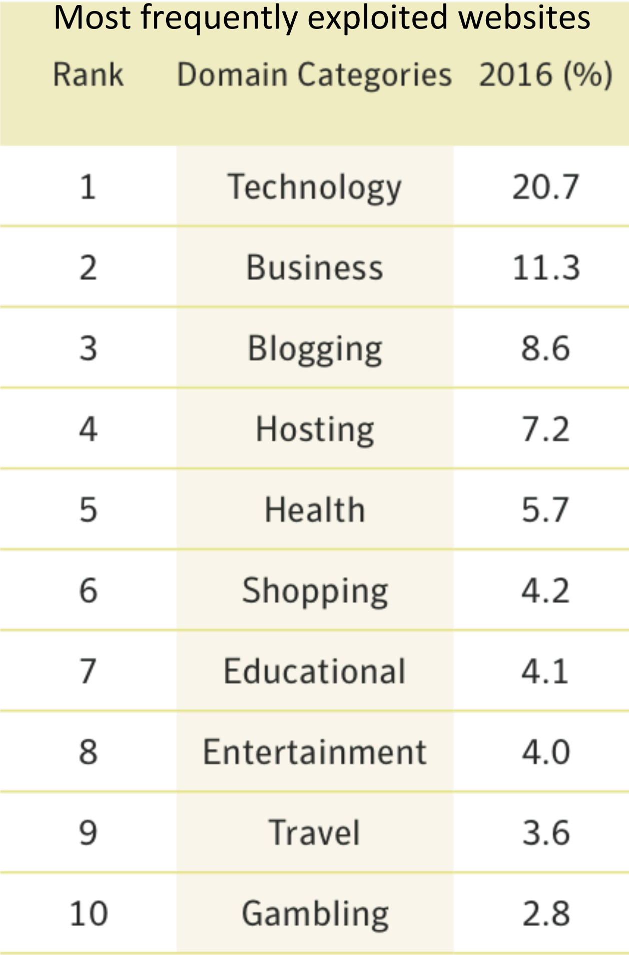
Statistics

- Lots of statistics about cybersecurity are available online
  - From security companies: consider possible bias
  - Sometimes contradicting each other: different customer base
  - Mostly instructive, help to get general overview



Email threats, malware, and bots

	2014	2015	2016
Spam rate %	60%	53%	53%
Phishing rate	1 in 965	1 in 1,846	1 in 2,596
Email malware rate	1in 244	1in 220	1in 131
New malware variants	275M	355M	357M
Number of bots		91.9M	98.6M



Most frequently exploited websites

Rank	Domain Categories	2016 (%)
1	Technology	20.7
2	Business	11.3
3	Blogging	8.6
4	Hosting	7.2
5	Health	5.7
6	Shopping	4.2
7	Educational	4.1
8	Entertainment	4.0
9	Travel	3.6
10	Gambling	2.8

Internet Security Threat Report, Symantec, 2017

Cybersecurity asymmetry

- Attacking is easy
  - Attackers include criminal organizations and nation-states
    - May have plenty of resources, and powerful capabilities
  - Attackers can ignore ethical concerns
  - **Attackers need to find ONE way in**
- Defending is hard
  - Defenses interfere with business goals
  - Hard to enforce laws across national barriers
    - Especially when attacks come from states unable or unwilling to cooperate
  - Targets are interconnected devices running vulnerable software
    - Hard/impossible to find all the bugs in a piece of code
      - Not just bugs, but also design and logical flaws
    - Software license agreements do not hold vendors accountable
  - Hard to identify who launched an attack, from where
    - NSA, GCHQ & friends have some network monitoring kit in place
      - NSA attribution of Sony hack to North Korea
    - There are big opportunities in digital forensics
  - **Defenders must protect on ALL fronts**

Human factors

- Humans introduce further weaknesses
  - Social engineering attacks
    - Sarah Palin's email, Jennifer Lawrence's pictures, …
    - Do not break defenses, but find a way around them
  - Weak passwords
    - We'll see more later on
  - Insider threats
    - Whistleblowers: Bradley Manning, Edward Snowden
    - Vengeful ex-employees, spies, thieves, etc.
    - Act from a position of privilege: have accounts, know systems and procedures
  - Coercion
    - Forced revelation of credentials
    - Lost or stolen devices
- Important to take human factors into account
  - This course focuses on technical aspects of network and web security