


Computer Security

in the news...

Aggelos Kiayias

In the news...

A walk through history...


DDoS

- February 7, 2000, time 10:30 am.
  - Yahoo.com goes down.
  - Incoming traffic on the order of 1GBit/s.
  - CNN, Ebay, Buy.com, Etrade, Amazon follow.
  - Total loss of revenue for Yahoo alone over $500,000
  - Claims for $1.7 billion overall.
  - In November 7, 2000, 'Mafiaboy' Canadian 15 year old pleads guilty.
    - Janet Reno: *We must punish MafiaBoy*. http://www.wired.com/politics/law/news/2000/04/35765
    - Mafiaboy sentenced to 8 months Youth Detention Center (+$160 fine)

Phishing

- A typical case of phishing:

Bavier, Anne <Anne.Bavier@uconn.edu>
To: Undisclosed recipients:;
ADMIN FINAL WARNING *** YOUR MAILBOX HAS REACHED IS LIMITED STORAGE LIMIT ***

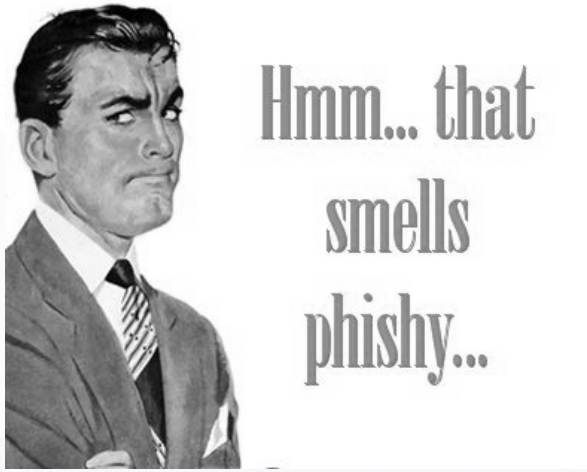
ATTENTION.

Your mailbox has reached is limited storage, 10GB as
exceeded set by your administrator, you are
currently 10.9GB, you may not be able To send or
receive new e-mail.To re-validate your mailbox.

To re-check your mailbox, please click the following link:
http://www.survivorgold.com/picksform/use/contract/form1.html

If the above link does not work, please copy
and paste the link below to your browser window
http://www.survivorgold.com/picksform/use/contract/form1.html

Thanks
System Administrator




Identity Theft

- A serious concern:
  - in a Federal Trade Commission 2006 ID Theft Report:
    - 8.3 million victims.
    - $15 billion total damage
  - Children identities stolen - check your 5 year old brothers credit report!
    - https://www.allclearid.com/assets/docs/ChildIDTheftReport2012.pdf

http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf


Hacked in minutes...

- In a honeypot experiment USAToday and Avantgarde monitored a number of PCs for 2 weeks (Sept. 2004).
- They counted 305,922 break-in attempts.
- The first breach occurred 4 minutes after the test started!
  (against the most vulnerable machine)

http://www.usatoday.com/money/industries/technology/2004-11-29-honeypot_x.htm


Private Data Exposure

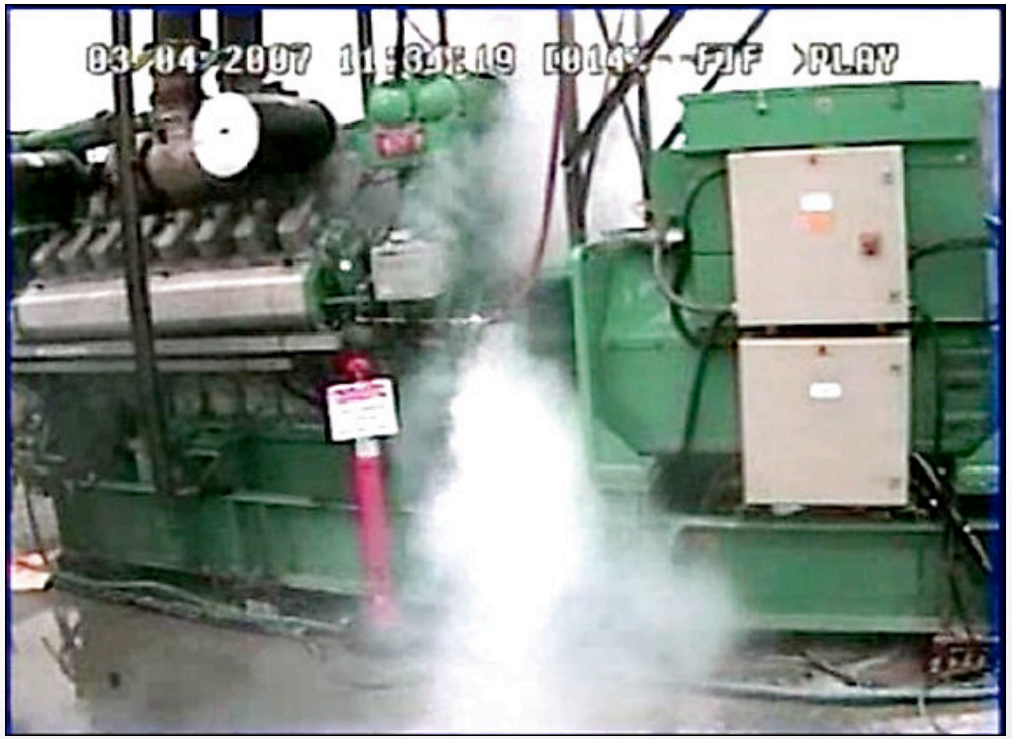
- (*an example*) In June 2005 Cardsystems Solutions, a credit-card processing company in AZ was hacked with targeted malicious intent. 40 million debit and credit-card accounts were exposed.
  - Amusingly, their network had been certified in '04 by VISA according to Payment Card Industry Data Security Standard.
  - After the breach it was determined they were not compliant.

http://www.wired.com/news/technology/0,1282,67980,00.html

Infrastructure Attacks

The "aurora generator test"

- In simulation: Remote hacker destroys a $1M diesel-electric generator part of US utility infrastructure



Generator room at the Idaho National Laboratory was remote accessed by a hacker and a $1 Million diesel-electric generator destroyed. (U.S. Homeland Security photo)


2005...

- in 2005, the treasury department was reporting: Cybercrime has outgrown illegal drug sales!

http://money.cnn.com/2005/12/29/technology/computer_security/index.htm?cnn=yes


2006...

- Year of spam
  - in oct. more than 90% of all e-mail was junk mail.
- 3-4 million "bots" active at any time in the Internet.
- Attacks have moved from weekends to 9-5 weekdays:
  - online crime is evolving into a full-time profession!

http://www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122200367.html


2007...

- A year of multiple data privacy breaches..
- Millions of private records are revealed to hackers.
- Average annual losses $350,000

http://www.computerworlduk.com/management/security/data-control/in-depth/index.cfm?articleid=1065
http://www.darkreading.com/document.asp?doc_id=133658


2008-9

- KeeLoq Attacks (vehicle lock system)
- Big botnet years :
  - Top botnets: Bobax, Storm, Kraken, Conficker...
  - Conficker 10 million PCs to 2009.
    --- In 12 hours a single bot sent 42,298 spam e-mails.
- Botnets become hard to penetrate, self-protecting, self-healing.


Twitter hacks

January 6, 2009

An 18-year-old hacker with a history of celebrity pranks has admitted to Monday's hijacking of multiple high-profile Twitter accounts, including President-Elect Barack Obama's, and the official feed for Fox News.

The hacker, who goes by the handle GMZ, told Threat Level on Tuesday he gained entry to Twitter's administrative control panel by pointing an automated password-guesser at a popular user's account. The user turned out to be a member of Twitter's support staff, who'd chosen the weak password "happiness."

Cracking the site was easy, because **Twitter allowed an unlimited number of rapid-fire log-in attempts**.

... A fake message sent to followers of the Fox News Twitter feed announced that Fox host Bill O'Reilly "is gay,"

http://blog.wired.com/27bstroke6/2009/01/professed-twitt.html


Passwords?

from a myspace phishing attack

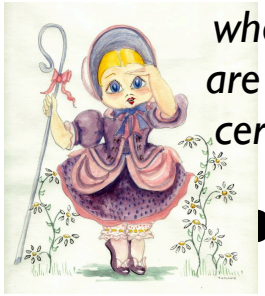
1-4	0.82 percent
5	1.1 percent
6	15 percent
7	23 percent
8	25 percent
9	17 percent
10	13 percent
11	2.7 percent
12	0.93 percent
13-32	0.93 percent

- The top 20 passwords are (in order): password1, abc123, myspace1, password, blink182, qwerty1, fuckyou, 123abc, baseball1, football1, 123456, soccer, monkey1, liverpool1, princess1, jordan23, slipknot1, superman1, iloveyou1 and monkey

http://www.schneier.com/blog/archives/2006/12/realworld_passw.html


2010

- Increasing privacy concerns for social networking sites such as facebook - (firesheep session hijacking).
- Cryptographic techniques used for "insurance" + cyberwarfare. The wikileaks case - Julian Assange.
- Stuxnet worm : first worm to infiltrate successfully nuclear power plant (in Iran). The worm affects the way attached motors rotate aiming to damage them.



2011

- Fraudulent digital certificates are created by hackers - Comodo (EU) and DigiNotar (certification authorities - CAs) were breached.
  CAs are the trusted parties of all Internet transactions.

40M tokens revoked

- Spear Phishing against RSA: An Excel spreadsheet opened, which completely blank except for an "X" that appeared in the first box of the spreadsheet. The "X" was the only visible sign that there was an embedded Flash exploit in the spreadsheet. When the spreadsheet opened, Excel triggered the Flash exploit to activate, which then dropped the backdoor -- in this case a backdoor known as Poison Ivy -- onto the system.
- Sony Playstation network hacked - around 100 million users' private data exposed.
  http://www.schneier.com/blog/archives/2011/08/details_of_the.html
- DUQU worm (stuxnet relative)


2011

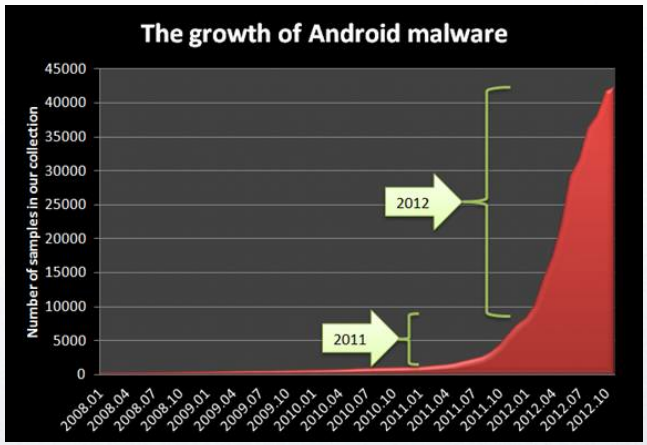
- Hacking cars with an MP3 CD
- (... also google driverless car approved in Nevada)
- Hacktivism - Anonymous, LULZSEC, ANTISEC



http://www.schneier.com/blog/archives/2011/03/hacking_cars_wi.html


2012

- SOPA/PIPA demonstrations :
  - wikipedia, google, and others: blackout in protest Jan 18, 2012.
- FLAME and GAUSS
  - nation state cyber warfare
- Flashback / Flashfake
  - first major Mac OSX virus - 700K Mac's infected
- Mobile (Exploits) - Android Threats
- APT - Advanced Persistent Threats
- Shamoon malware against Aramco (Oil conglomerate)




2013

- The Snowden revelations regarding the extended surveillance programs run by the NSA.
- Point of Sale Hacks: Massive breach in Target stores. Covert channel setup leaked > 100 million credit cards.


2013

- The Silk-Road take-down. (an online black market. started in 2011 - relaunched 2013). trade volume > $1M per month.
- E-mail interception and key-logging software installed on computers in Internet cafe's during G8 meeting (was in 2009).


2014

- Security vulnerabilities!

shellshock

https://shellshocker.net

heartbleed

http://heartbleed.com

poodle

(Padding Oracle On Downgraded Legacy Encryption)

2014

- Increased attacks against industrial control systems (ICS)

a decoy set up by Kaspersky on an ICS typically used to control national infrastructure saw 1,300 attempts to gain unauthorised access in a single month.... 400 were successful.

http://www.computerweekly.com/news/2240223685/Industrial-control-systems-increasingly-under-attack-says-Kaspersky

- Banks under report cyber fraud...

the amount of money being taken from people's accounts through cyber crime is twice as much as what is reported.

http://www.computerweekly.com/news/2240234371/Banks-play-down-cyber-attack-levels


End of Computer Security in the news..

- Have a good semester! (and get your updates)

