0x103 – What is Computer Security?

ECED4406 – Computer Security

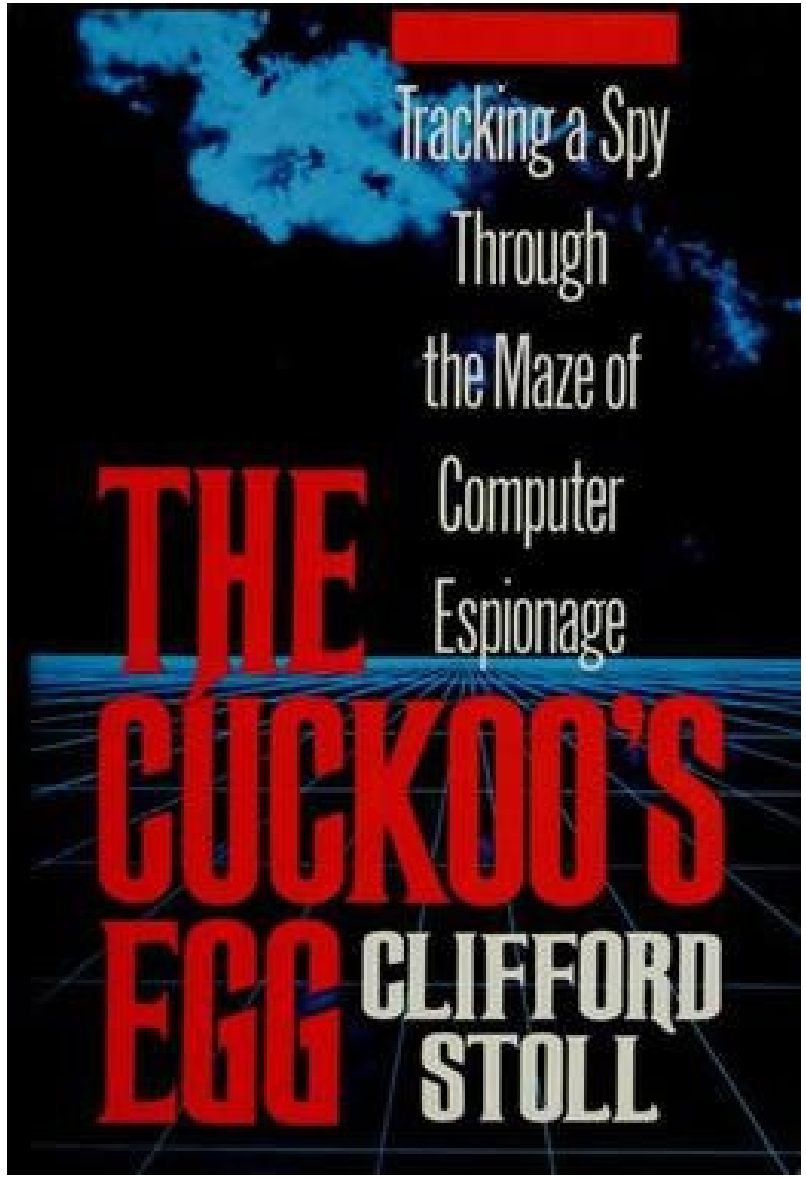
Dr. Colin O'Flynn
Dalhousie University.

Let’s Look at Failures

#1 Early Hackers (Late 1980's)

- The year… is 1986. Clifford Stole discovers a $0.75 error in the computer accounts…

https://www.youtube.com/watch?v=hTx9h3Sm29I



#1 What did this result in?

- Long project to catch the hackers (also – convince FBI this is an issue!).
- Hacker used fact that many people had default or not passwords (this will come up again, forever).
- A ‘honeypot’ was setup with some files the hacker would be interested in, resulted in additional information about the hacker.
- Hacker was stealing information to sell to KGB.

#2 United States v. Elcom Ltd. (2001)

- Wrote “Advanced E-Book Processor”
- Capable of removing some security mechanisms from books.
  - From previous slides – the “Rotate by 13” Cipher.
- Arrested in U.S. under law known as DMCA (we’ll come back to this).
- Charges eventually dropped.

#3 Target Data Breach (2013)

- Hackers found (public) information on Target suppliers, such as HVAC (heating/cooling) contractor.
- Hackers attacked these vendors, on assumption they will have poor security controls.

#3

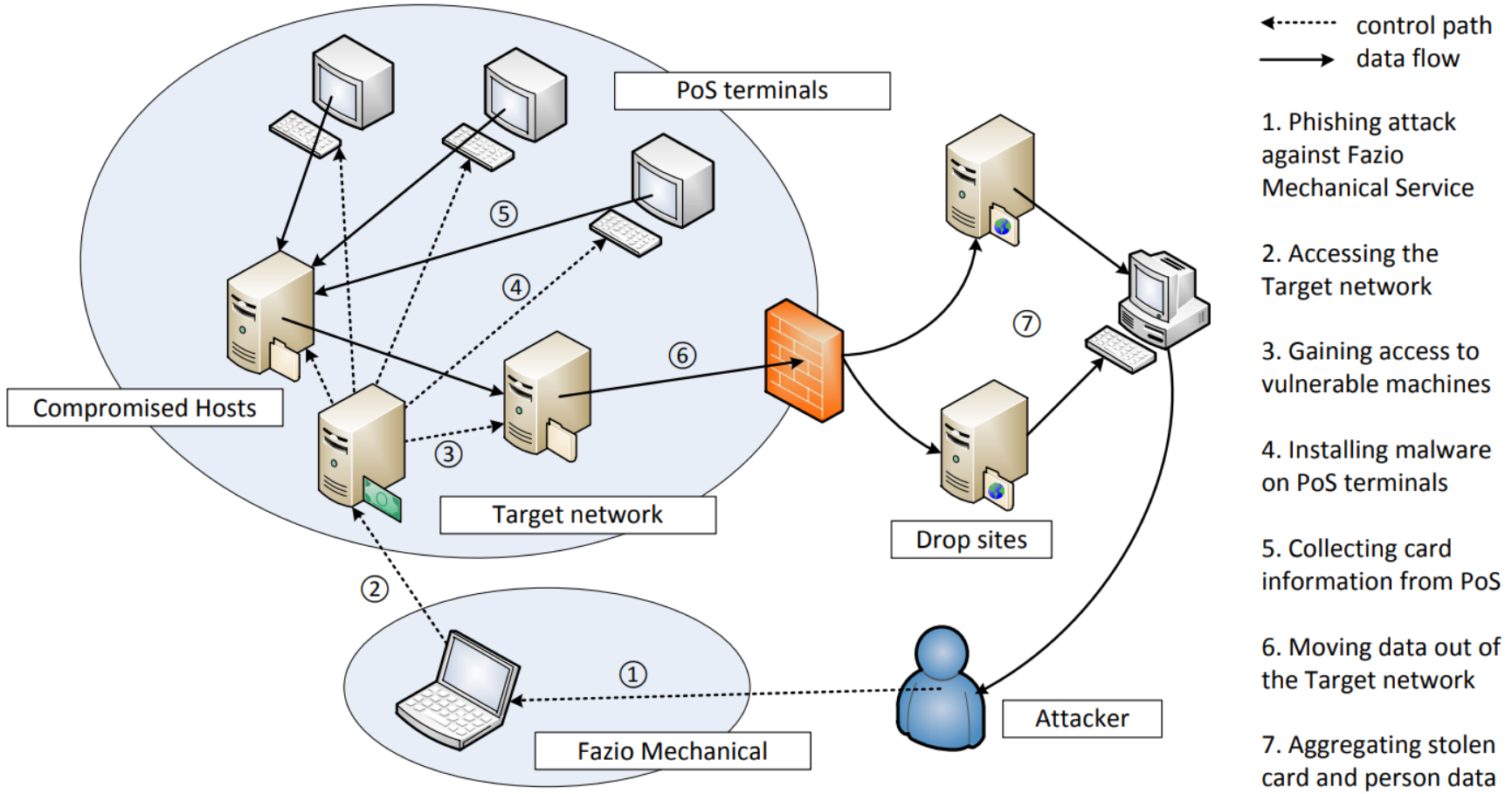


Fig. 2. Attack steps of the Target breach.

Xiaokui Shu, Ke Tian, Andrew Ciambrone and Danfeng (Daphne) Yao.
"Breaking the Target: An Analysis of Target Data Breach and Lessons Learned".
https://arxiv.org/pdf/1701.04940.pdf

#3 What did this result in?

- Objective was stealing customer information (including credit card) for fraud.
- Total of 40 million customers affected.
- Target claims total cost of break ~$200 million dollars.
- Fined $18.5 million to settle claims in 2017.
- Some charged or suspected of helping (linked):
  - Ruslan Bondars, 14 years
  - Taylor Huddleston
  - Andrey Hodirevski

Some starting points for more info on the topic, see:

- https://malicious.life/episode/episode-29/
- https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/
- https://www.washingtonpost.com/local/public-safety/hacker-linked-to-target-data-breach-gets-14-years-in-prison/2018/09/21/839fd6b0-bd17-11e8-b7d2-0773aa1e33da_story.html

#4 – Many Other Data Breaches

- Target was not first or biggest! Using https://en.wikipedia.org/wiki/List_of_data_breaches (at least 30K records leaked):

Entity	Year	Records	Organization type	Method	Sources
Clearview AI	2020	3,000,000,000 (Number of photos obtained)	information technology	hacked	[81]
Yahoo	2013	3,000,000,000	web	hacked	[354][355]
First American Corporation	2019	885,000,000	financial service company	poor security	[141]
Facebook	2019	540,000,000	social network	poor security	[136]
Marriott International	2018	500,000,000	hotel	hacked	[209][210]
Yahoo	2014	500,000,000	web	hacked	[356][357][358][359][360]
Friend Finder Networks	2016	412,214,295	web	poor security / hacked	[142][143]

passwords, was posted on the web for sale.

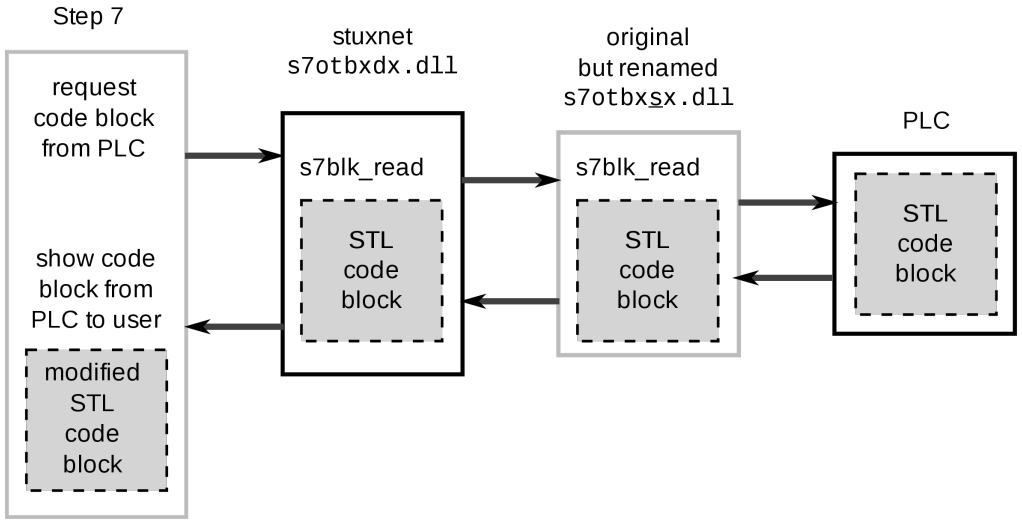
Entity	Year	Records	Organization type	Method	Sources
AOL	2004	92,000,000	web	inside job, hacked	[26][27]
CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express)	2005	40,000,000	financial	hacked	[67][68]
Citigroup	2005	3,900,000	financial	lost / stolen media	[77]
DSW Inc.	2005	1,400,000	retail	hacked	[104]
Bank of America	2005	1,200,000	financial	lost / stolen media	[42]

#5 Stuxnet (2010)

- One of the largest (at the time) nationally-sponsored cyber-physical attack.
- Objective: **set back Iranian atomic program**.

#5 – How it Worked

- Computer work with very specific programming & objective:
  - Searched for an exact configuration of computer and PLC, as used in centrifuge control.
  - Malware attacked the PLC & control computer to run a complicated program.
- Malware would occasionally over-speed the centrifuge, but report back to the users that everything was normal.
- Malware would then return to normal operation.



- For (a LOT!) more, see:
  - https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/
  - https://www.amazon.ca/Countdown-Zero-Day-Stuxnet-Digital-ebook/dp/B00KEPLC08
  - https://en.wikipedia.org/wiki/Stuxnet

Important Computer Security Terms

Zero-Day

These are previously unknown “exploits”. A vulnerability in some software that *has not been seen before, thus there is no protection against it*.

Normally a vendor is aware of the vulnerability, and has some time to patch it. Exploits happen because of a failure of users to patch.

Computer Security Failures

- What is objective of attacker?
  - Fame?
  - Money?
  - Fraud?
  - Military?
  - Revenge?
- What are resources available to attacker?
  - Technical resources?
  - Funding?
  - Network of others to work with?

Computer Security – Relevance to Us

- We are interested in embedded systems – what does that mean?