SC3010
Computer Security

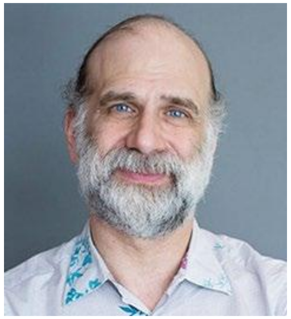
Lecture 1: Introduction

What is Computer Security

Guarantee the correct usage of computer systems and desired properties in the presence of malicious entities

Rose Anderson
Professor, Univ. of Cambridge

> *"Security engineering is about building systems to remain dependable in the face of malice, error, or mischance."*



Bruce Schneier
Adj Lecturer, Harvard Kennedy School

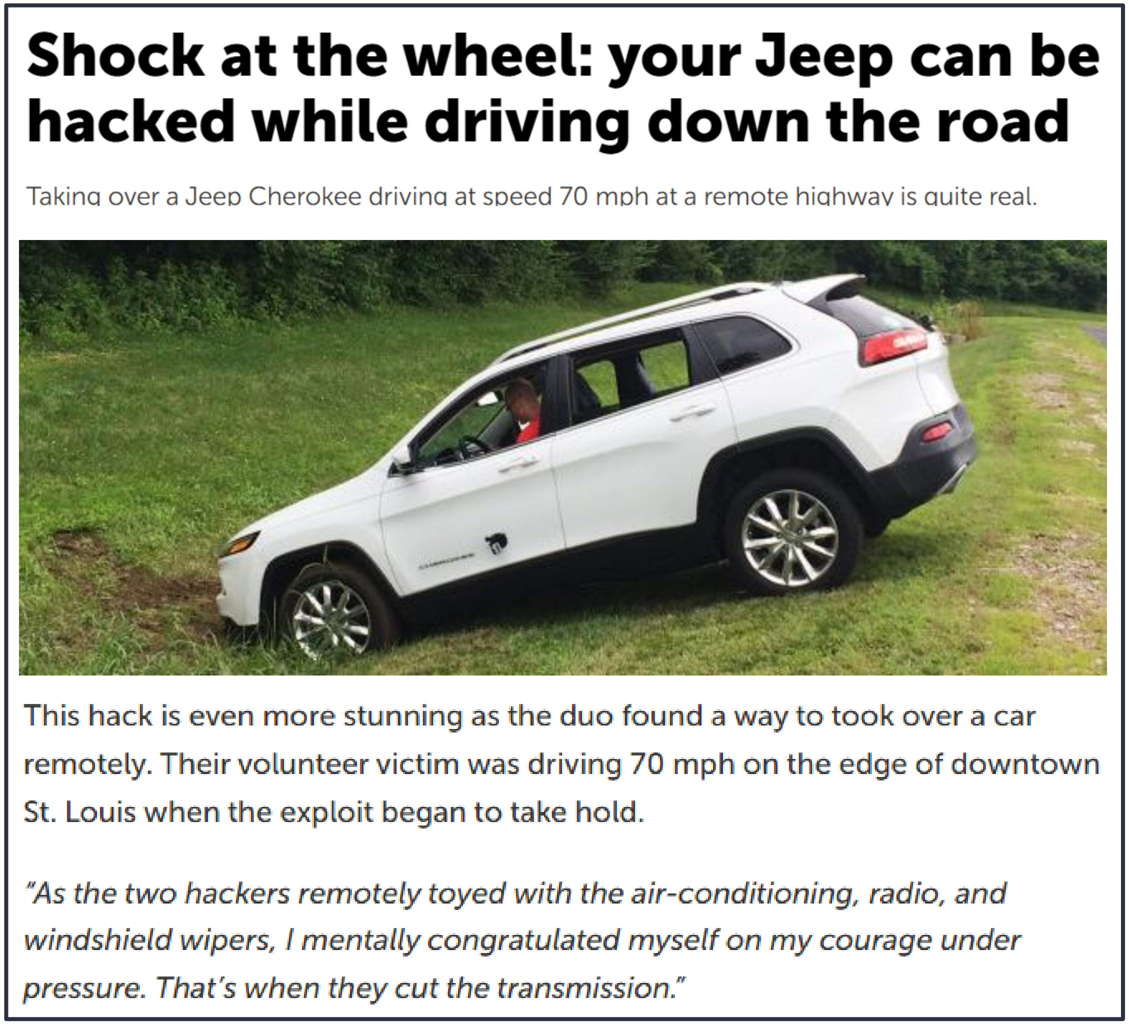
> *"Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time … again and again. It is truly programming Satan's computer."*

Significance of Computer Security

Critical to physical safety

- Power grid and water systems: blackouts, water contamination or disruption of supply
- Transportation networks and connected vehicles: traffic jam, car collisions or crashes
- Aviation: interfere with navigation and communication, leading to accident
- Factory automation: sabotage industrial processes, leading to equipment failure or explosions
- Medical devices: pose life-threatening risks to patients (e.g., pacemakers)
- Start home systems: compromise devices like thermostats or locks can lead to unsafe temperature levels or unauthorized access to homes
- Electric Vehicle charging stations: overload circuits and cause fire hazards

Case Study: Jeep Hack



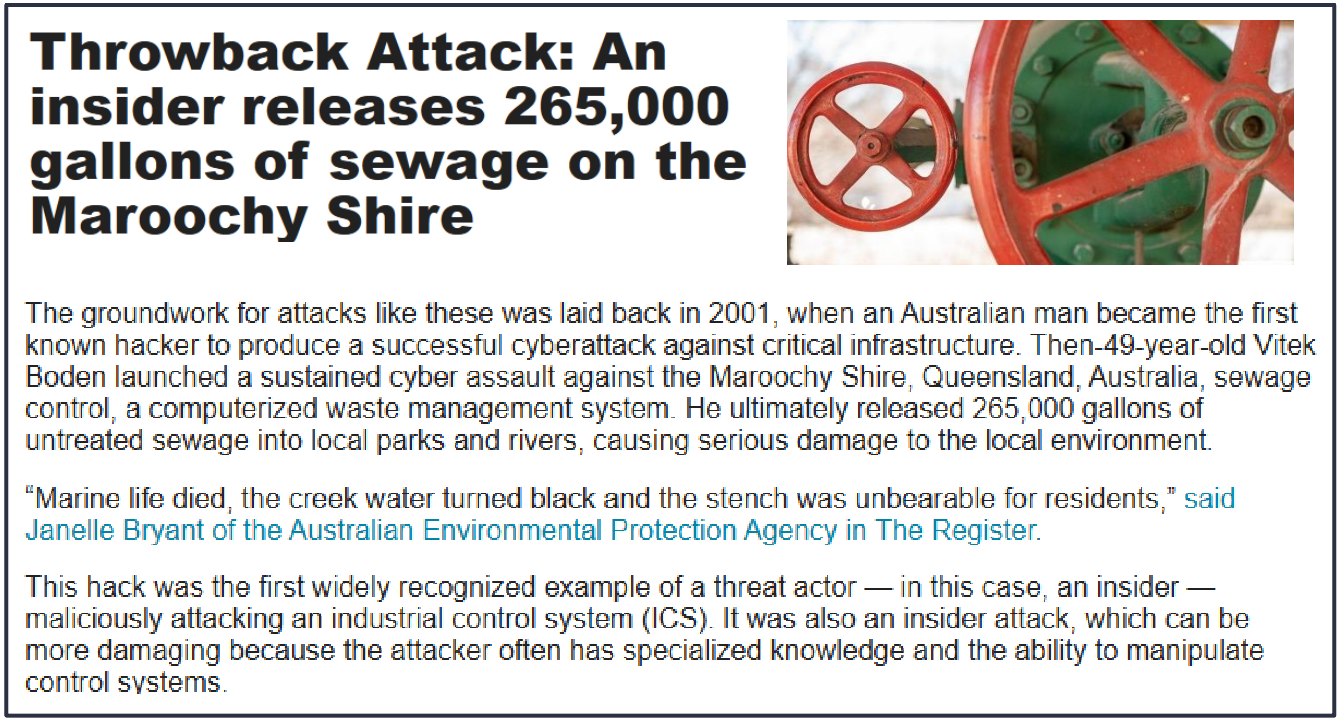
Shock at the wheel: your Jeep can be hacked while driving down the road

Taking over a Jeep Cherokee driving at speed 70 mph at a remote highway is quite real.

This hack is even more stunning as the duo found a way to took over a car remotely. Their volunteer victim was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

"As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission."

Case Study: Throwback Attack



Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire

The groundwork for attacks like these was laid back in 2001, when an Australian man became the first known hacker to produce a successful cyberattack against critical infrastructure. Then-49-year-old Vitek Boden launched a sustained cyber assault against the Maroochy Shire, Queensland, Australia, sewage control, a computerized waste management system. He ultimately released 265,000 gallons of untreated sewage into local parks and rivers, causing serious damage to the local environment.

“Marine life died, the creek water turned black and the stench was unbearable for residents,” said Janelle Bryant of the Australian Environmental Protection Agency in The Register.

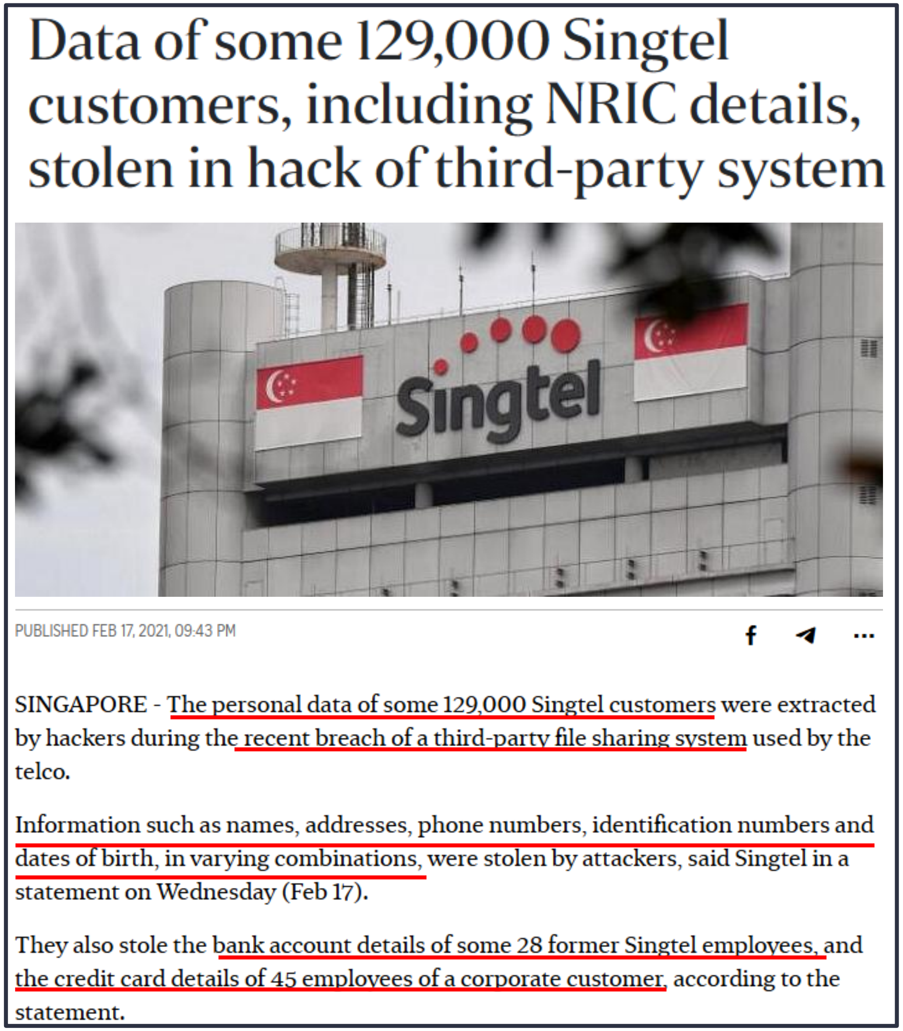
This hack was the first widely recognized example of a threat actor — in this case, an insider — maliciously attacking an industrial control system (ICS). It was also an insider attack, which can be more damaging because the attacker often has specialized knowledge and the ability to manipulate control systems.

Significance of Computer Security

Critical to personal privacy

- Database breaches: infiltrate companies to steal personal data
- Phishing: send deceptive emails, SMS, web links to trick users into revealing sensitive information, e.g., credentials, financial information, etc.
- Ransomware: encrypt personal files and demand payment for release
- Spyware: secretly monitor users' activities, including keystrokes, web browsing, communication, etc.
- Malicious mobile apps: unauthorized collection of location, contact, or other private data.
- Smart device exploitation: hack cameras, speakers, or thermostats to spy on individuals

Case Study: Data Breach in Singapore



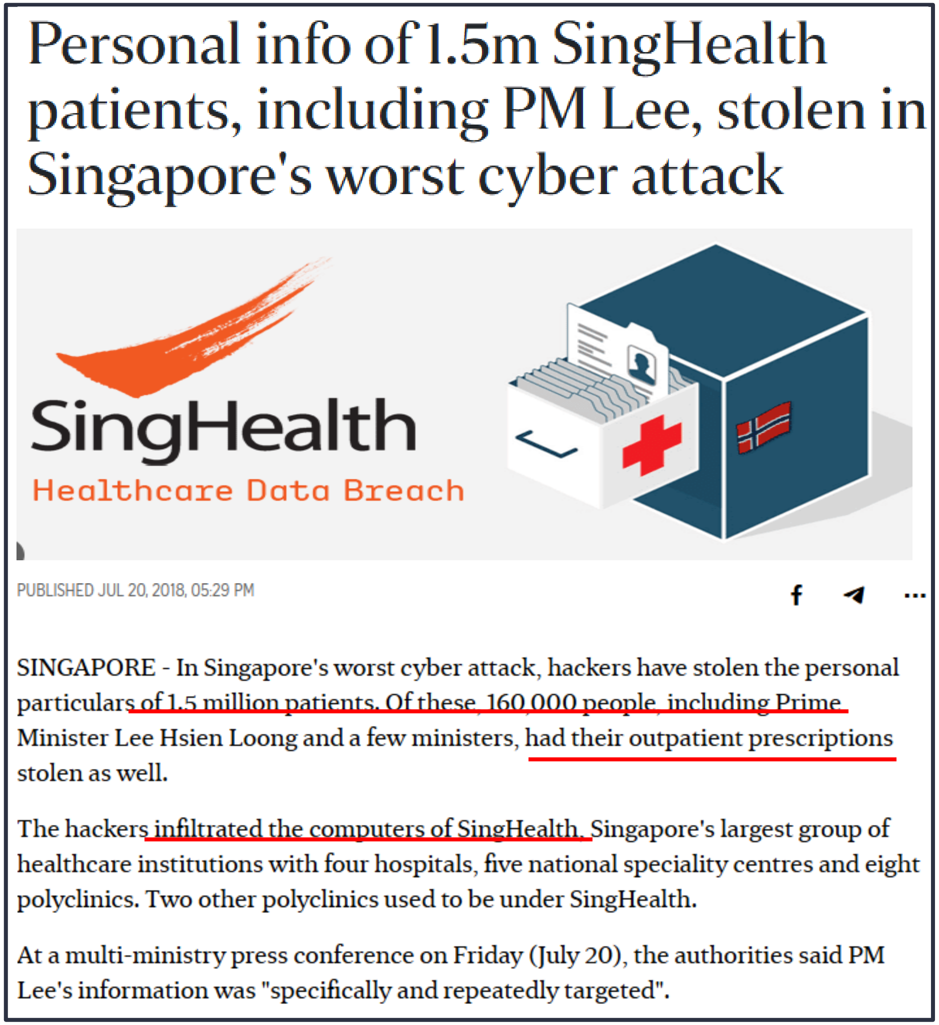
Data of some 129,000 Singtel customers, including NRIC details, stolen in hack of third-party system

PUBLISHED FEB 17, 2021, 09:43 PM

SINGAPORE - The personal data of some 129,000 Singtel customers were extracted by hackers during the recent breach of a third-party file sharing system used by the telco.

Information such as names, addresses, phone numbers, identification numbers and dates of birth, in varying combinations, were stolen by attackers, said Singtel in a statement on Wednesday (Feb 17).

They also stole the bank account details of some 28 former Singtel employees, and the credit card details of 45 employees of a corporate customer, according to the statement.



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

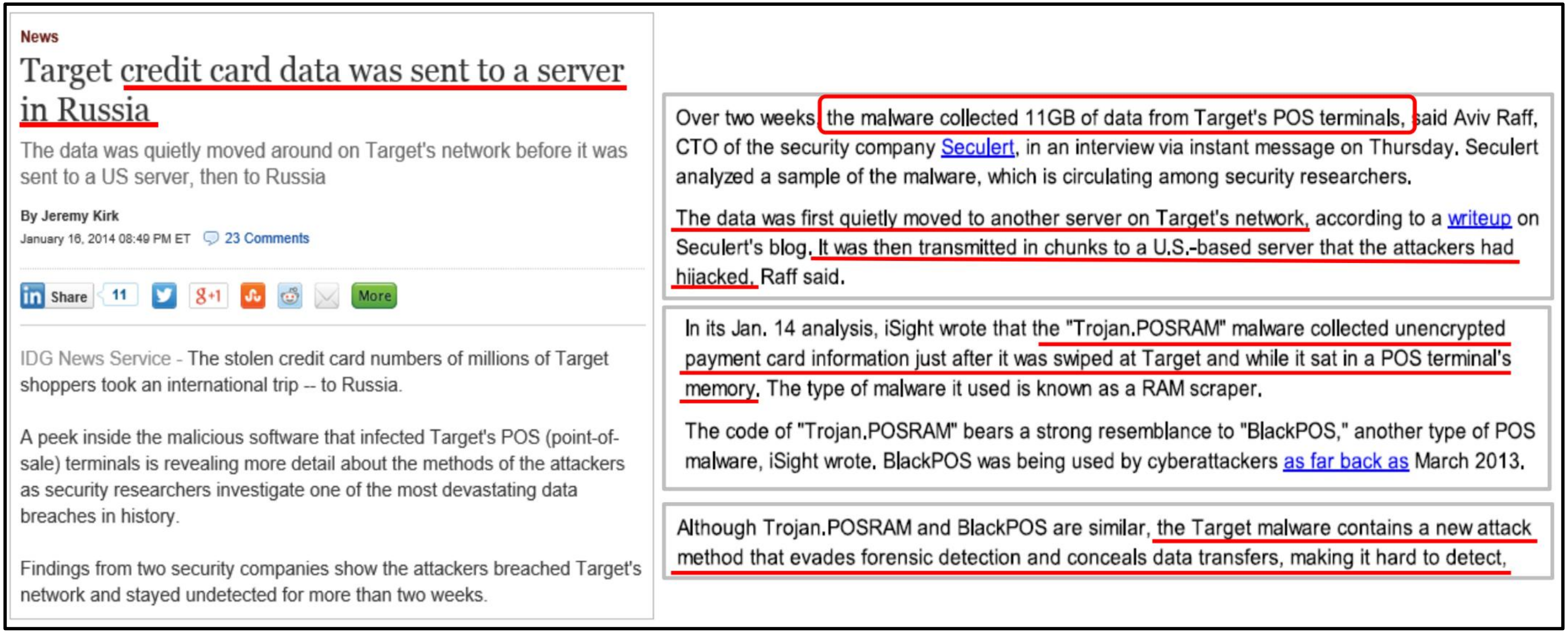
PUBLISHED JUL 20, 2018, 05:29 PM

SINGAPORE - In Singapore's worst cyber attack, hackers have stolen the personal particulars of 1.5 million patients. Of these, 160,000 people, including Prime Minister Lee Hsien Loong and a few ministers, had their outpatient prescriptions stolen as well.

The hackers infiltrated the computers of SingHealth, Singapore's largest group of healthcare institutions with four hospitals, five national speciality centres and eight polyclinics. Two other polyclinics used to be under SingHealth.

At a multi-ministry press conference on Friday (July 20), the authorities said PM Lee's information was "specifically and repeatedly targeted".

Case Study: Target Attack



News

Target credit card data was sent to a server in Russia

The data was quietly moved around on Target's network before it was sent to a US server, then to Russia

By Jeremy Kirk
January 16, 2014 08:49 PM ET 23 Comments

IDG News Service - The stolen credit card numbers of millions of Target shoppers took an international trip -- to Russia.

A peek inside the malicious software that infected Target's POS (point-of-sale) terminals is revealing more detail about the methods of the attackers as security researchers investigate one of the most devastating data breaches in history.

Findings from two security companies show the attackers breached Target's network and stayed undetected for more than two weeks.

Over two weeks, the malware collected 11GB of data from Target's POS terminals, said Aviv Raff, CTO of the security company Seculert, in an interview via instant message on Thursday. Seculert analyzed a sample of the malware, which is circulating among security researchers.

The data was first quietly moved to another server on Target's network, according to a writeup on Seculert's blog. It was then transmitted in chunks to a U.S.-based server that the attackers had hijacked, Raff said.

In its Jan. 14 analysis, iSight wrote that the "Trojan.POSRAM" malware collected unencrypted payment card information just after it was swiped at Target and while it sat in a POS terminal's memory. The type of malware it used is known as a RAM scraper.

The code of "Trojan.POSRAM" bears a strong resemblance to "BlackPOS," another type of POS malware, iSight wrote. BlackPOS was being used by cyberattackers as far back as March 2013.

Although Trojan.POSRAM and BlackPOS are similar, the Target malware contains a new attack method that evades forensic detection and conceals data transfers, making it hard to detect,