# SC3010
# Computer Security

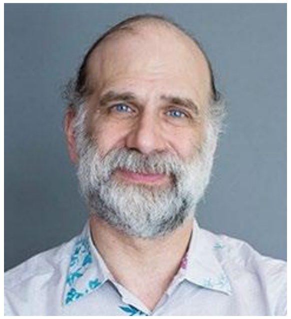
## Lecture 1: Introduction

# 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

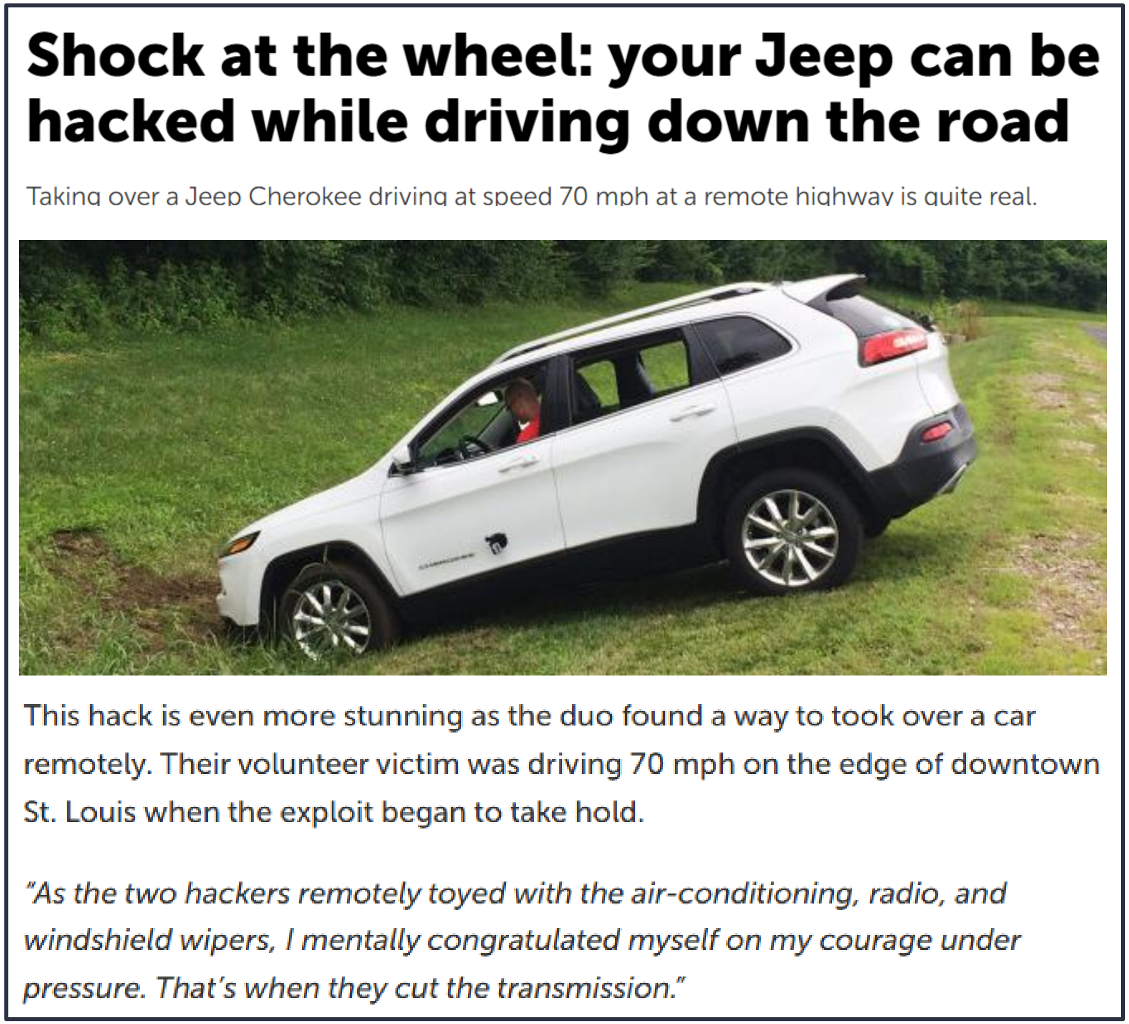
*"Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time … again and again. It is truly programming Satan's computer."*

# 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



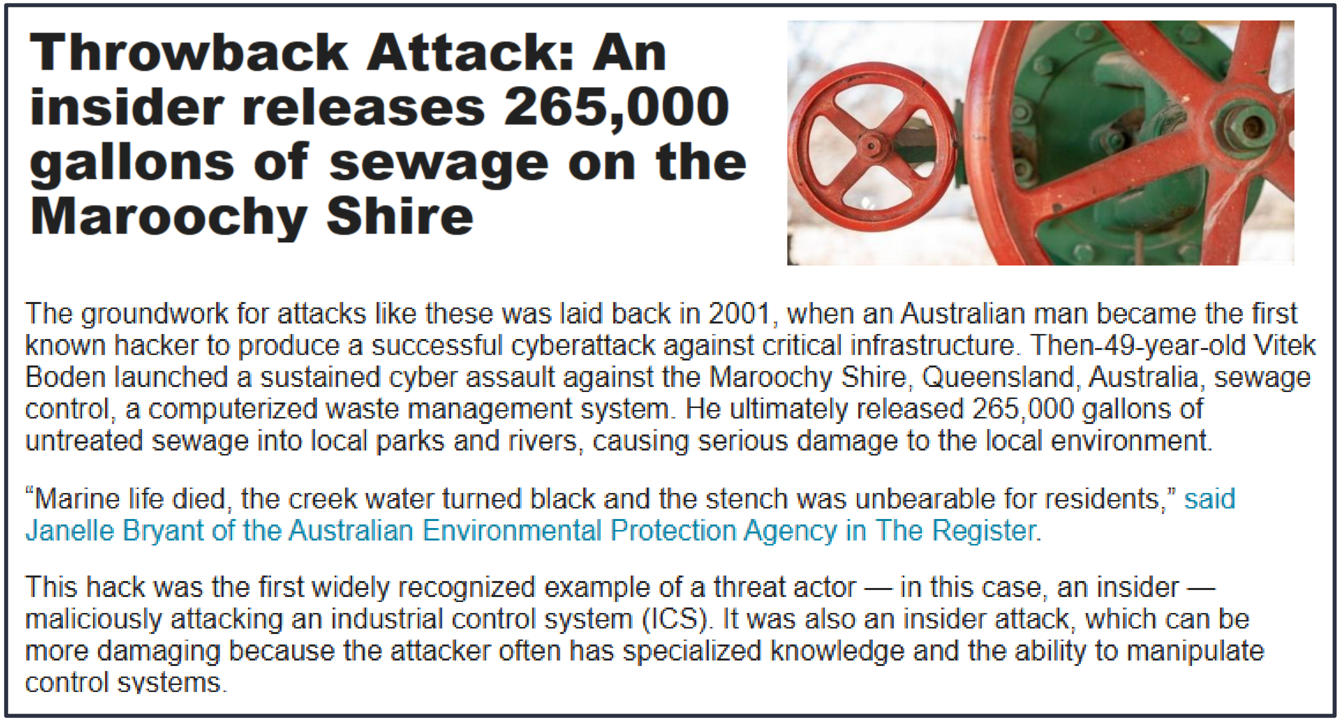
## Shock at the wheel: your Jeep can be hacked while driving down the road

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.

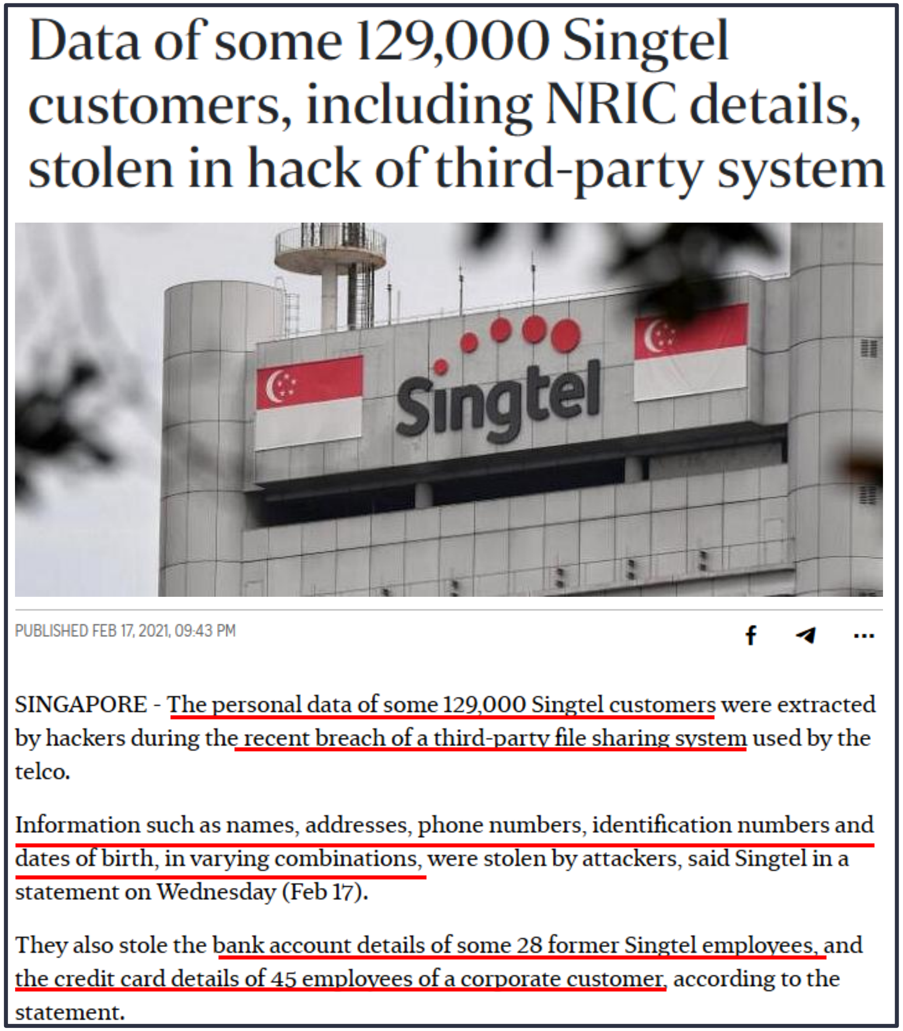
This hack was the first widely recognized example of a threat actor — in this case, an insider — maliciously attacking an industrial control system (ICS). It was also an insider attack, which can be more damaging because the attacker often has specialized knowledge and the ability to manipulate control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



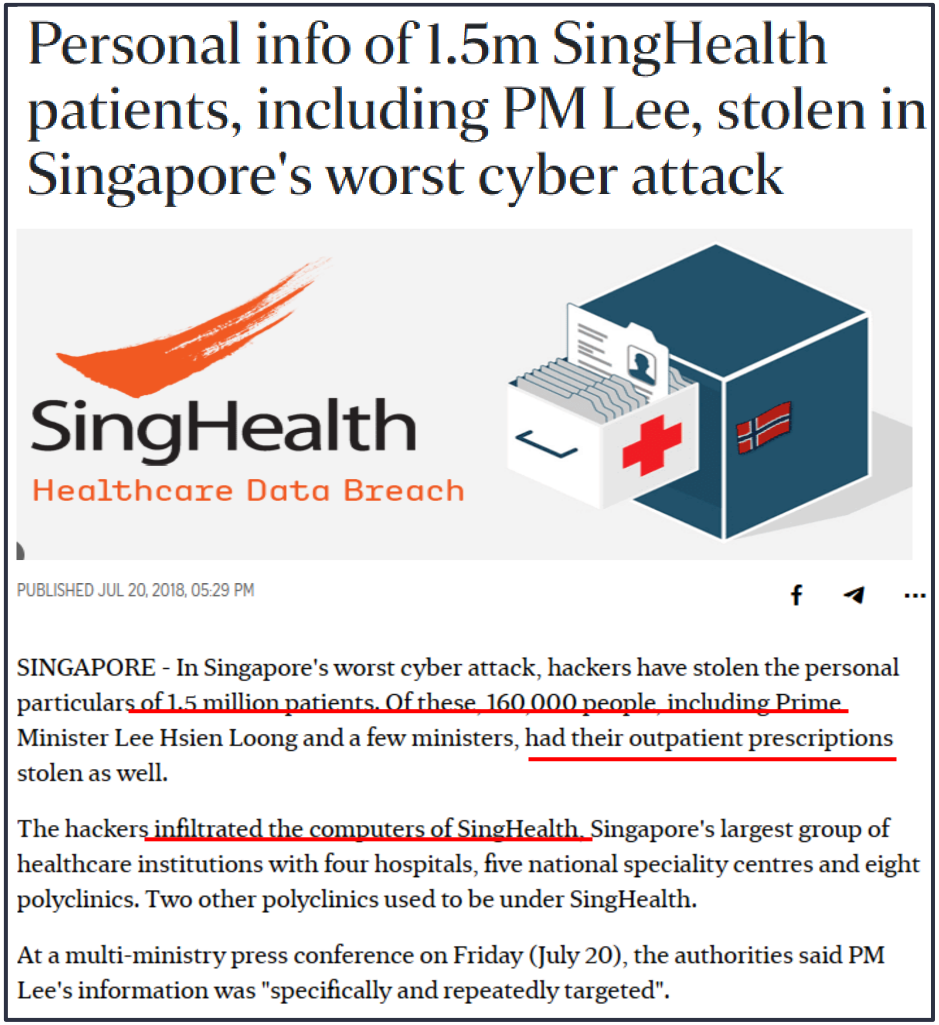
## Data of some 129,000 Singtel customers, including NRIC details, stolen in hack of third-party system

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

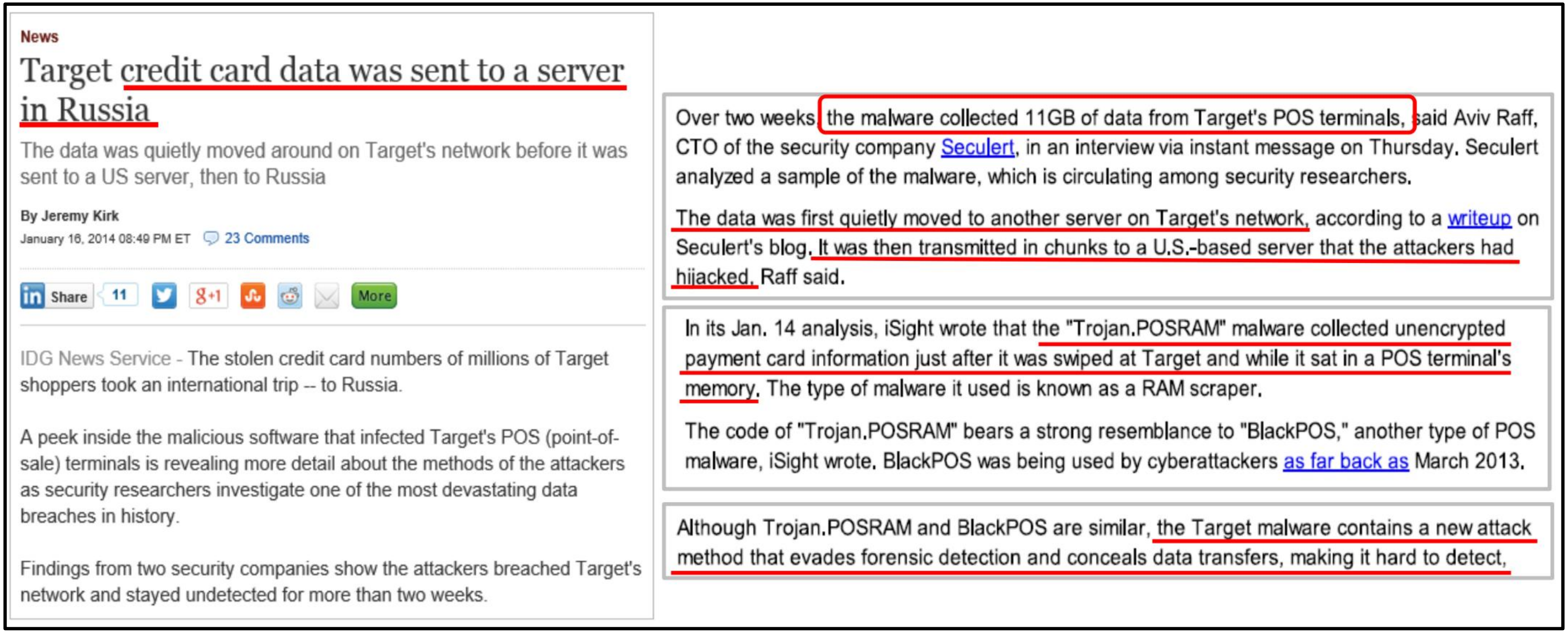
PUBLISHED JUL 20, 2018, 05:29 PM

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



## 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.

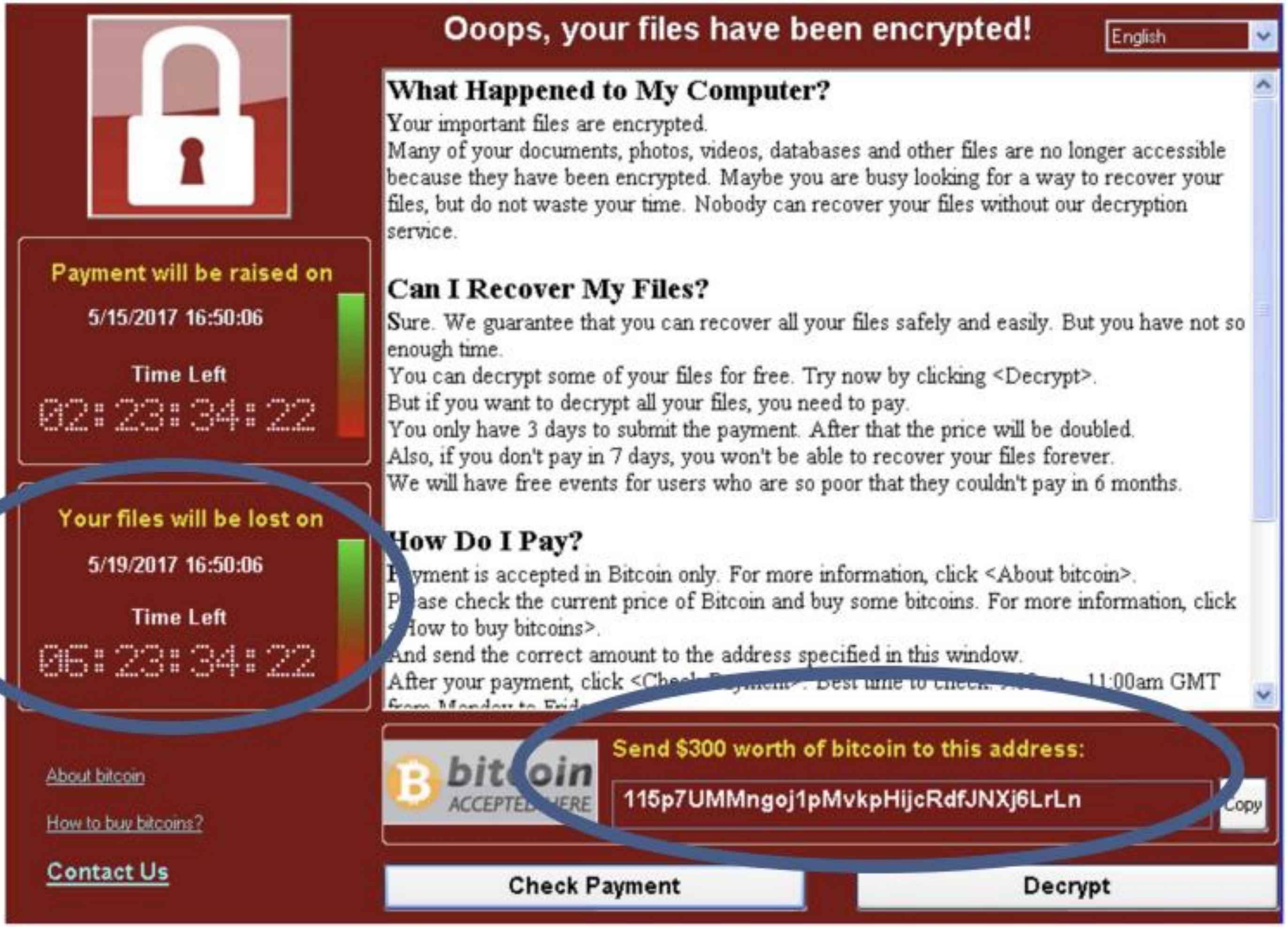
The data was first quietly moved to another server on Target's network, according to a writeup on Seculert's blog. It was then transmitted in chunks to a U.S.-based server that the attackers had hijacked, Raff said.

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,

# Case Study: WannaCry Ransomware



## 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 GMT from Monday to Frid

Payment will be raised on

5/15/2017 16:50:06

Time Left

02:23:34:22

Your files will be lost on

5/19/2017 16:50:06

Time Left

06:23:34:22

Send $300 worth of bitcoin to this address:

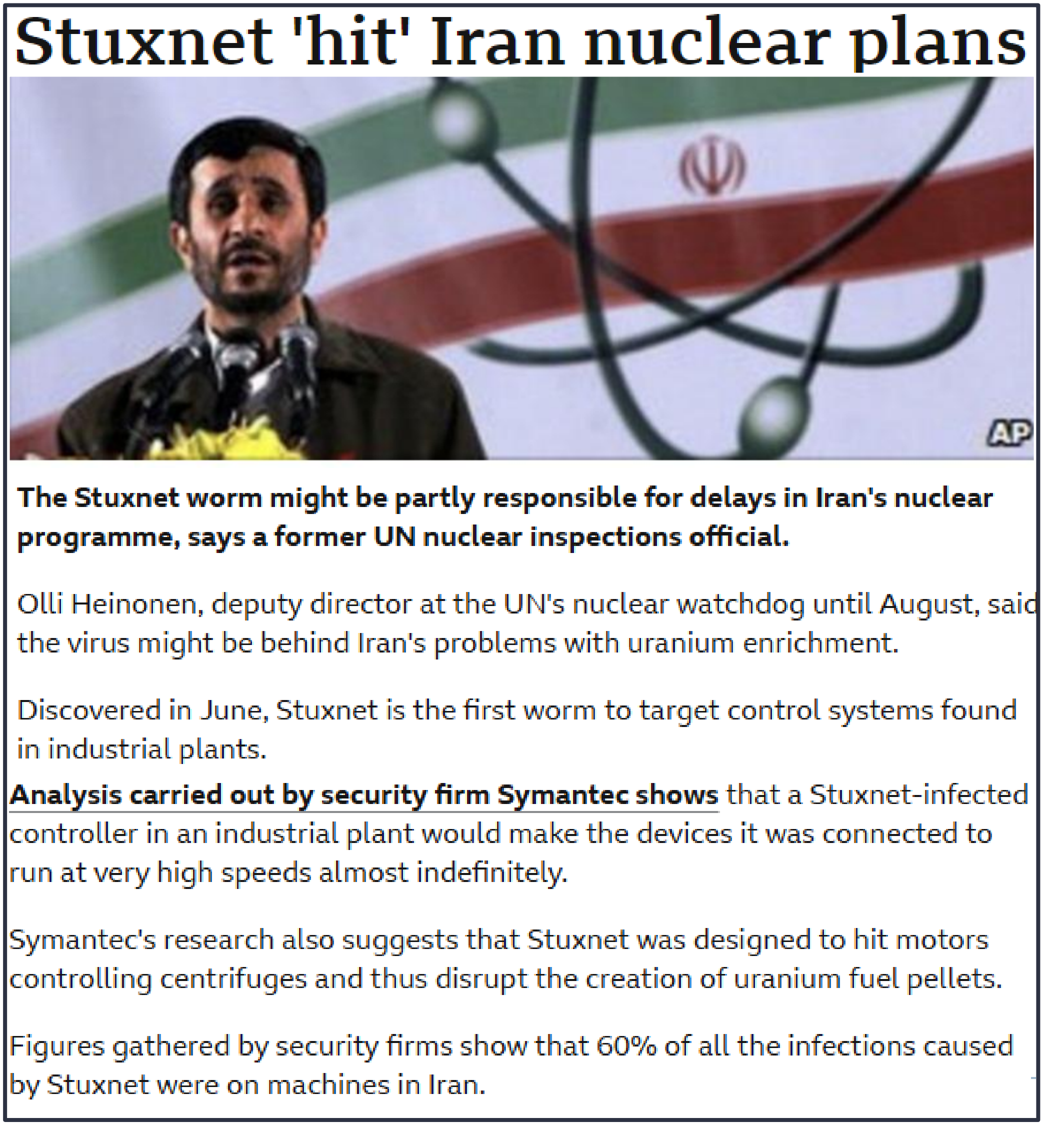
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

# Significance of Computer Security

## Critical to national security

- Cyber espionage: steal classified information from rival government or military systems, such as diplomatic strategies, defense plans, etc.
- Election interference: spread false information to influence public opinion, hack political campaigns, or manipulate voting systems.
- Cyber warfare: disrupt the military operations, or Distributed Denial of Service attacks against government services or infrastructure
- Supply chain attacks: target software or hardware suppliers to compromise the systems in government or defense agencies
- Cyber terrorism: launch attacks aimed at causing physical destruction or fear, such as targeting dams, chemical plants or hospitals

# Case Study: Stuxnet Malware



## Stuxnet 'hit' Iran nuclear plans

**The Stuxnet worm might be partly responsible for delays in Iran's nuclear programme, says a former UN nuclear inspections official.**

Olli Heinonen, deputy director at the UN's nuclear watchdog until August, said the virus might be behind Iran's problems with uranium enrichment.

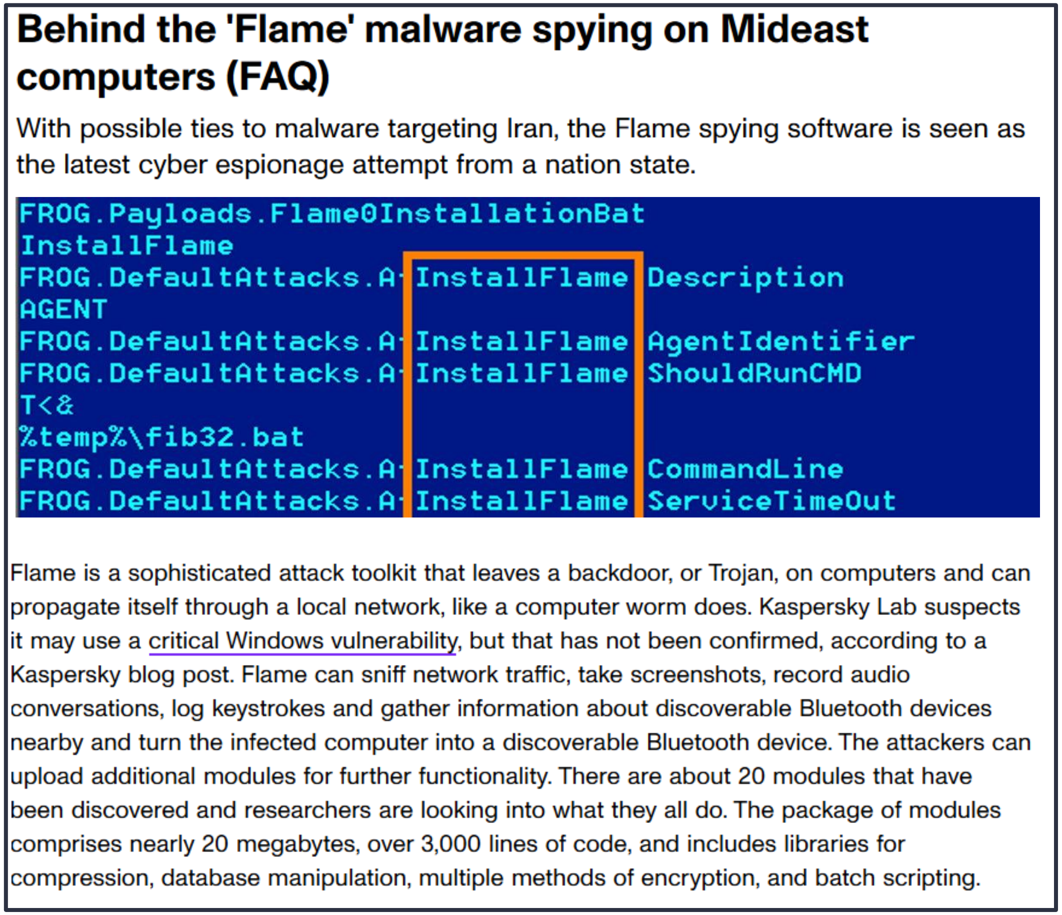
Discovered in June, Stuxnet is the first worm to target control systems found in industrial plants.

**Analysis carried out by security firm Symantec shows** that a Stuxnet-infected controller in an industrial plant would make the devices it was connected to run at very high speeds almost indefinitely.

Symantec's research also suggests that Stuxnet was designed to hit motors controlling centrifuges and thus disrupt the creation of uranium fuel pellets.

Figures gathered by security firms show that 60% of all the infections caused by Stuxnet were on machines in Iran.

# Case Study: Flame Spyware



## Behind the 'Flame' malware spying on Mideast computers (FAQ)

With possible ties to malware targeting Iran, the Flame spying software is seen as the latest cyber espionage attempt from a nation state.

```
FROG.Payloads.Flame0InstallationBat
InstallFlame
FROG.DefaultAttacks.A InstallFlame Description
AGENT
FROG.DefaultAttacks.A InstallFlame AgentIdentifier
FROG.DefaultAttacks.A InstallFlame ShouldRunCMD
T<&
%temp%\fib32.bat
FROG.DefaultAttacks.A InstallFlame CommandLine
FROG.DefaultAttacks.A InstallFlame ServiceTimeOut
```

Flame is a sophisticated attack toolkit that leaves a backdoor, or Trojan, on computers and can propagate itself through a local network, like a computer worm does. Kaspersky Lab suspects it may use a critical Windows vulnerability, but that has not been confirmed, according to a Kaspersky blog post. Flame can sniff network traffic, take screenshots, record audio conversations, log keystrokes and gather information about discoverable Bluetooth devices nearby and turn the infected computer into a discoverable Bluetooth device. The attackers can upload additional modules for further functionality. There are about 20 modules that have been discovered and researchers are looking into what they all do. The package of modules comprises nearly 20 megabytes, over 3,000 lines of code, and includes libraries for compression, database manipulation, multiple methods of encryption, and batch scripting.

# System Complexity Leads to Insecurity

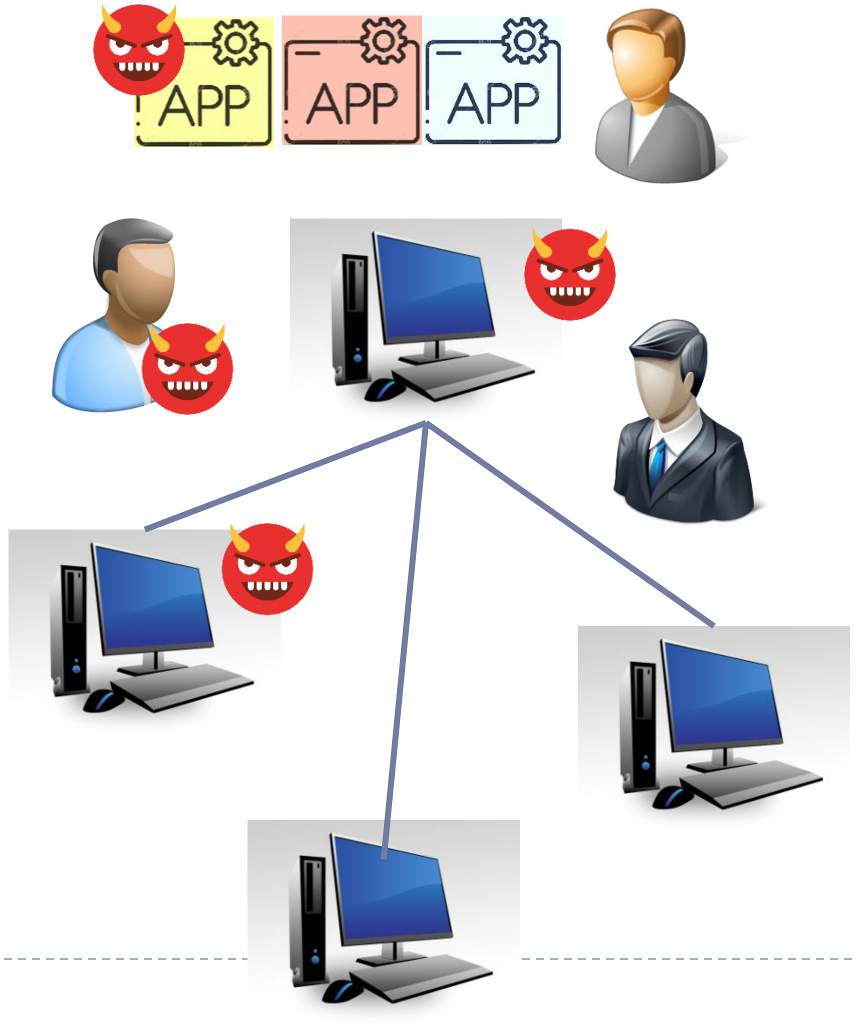
Provide a protected environment for data and their processing

**Standalone computer single user monoprogram**

- Physical security

**Standalone computer single user multiprogram**

- Physical security
- Process protection



**Standalone computer multiple user**

- Physical security
- Process protection
- Data protection
- User authentication

**Networked computer**

- Physical security
- Process protection
- Data protection
- User authentication
- Communication protection

# Human Factors Lead to Insecurity

## System Users

- Security features are not used correctly, e.g., misconfiguration.
- Users like convenience and may try to disable some security configurations that are not inconvenient

## System Developers

- Security features are not designed correctly; security components are not implemented correctly
- Developers are humans, and humans can make mistakes.

## External Parties

- Individual’s trust can be manipulated for profit, e.g., social engineering

# Basics of Cyber Security

**Threat Model**

- Trusted Computing Base (TCB)
- Attacker's assumption
- Security properties

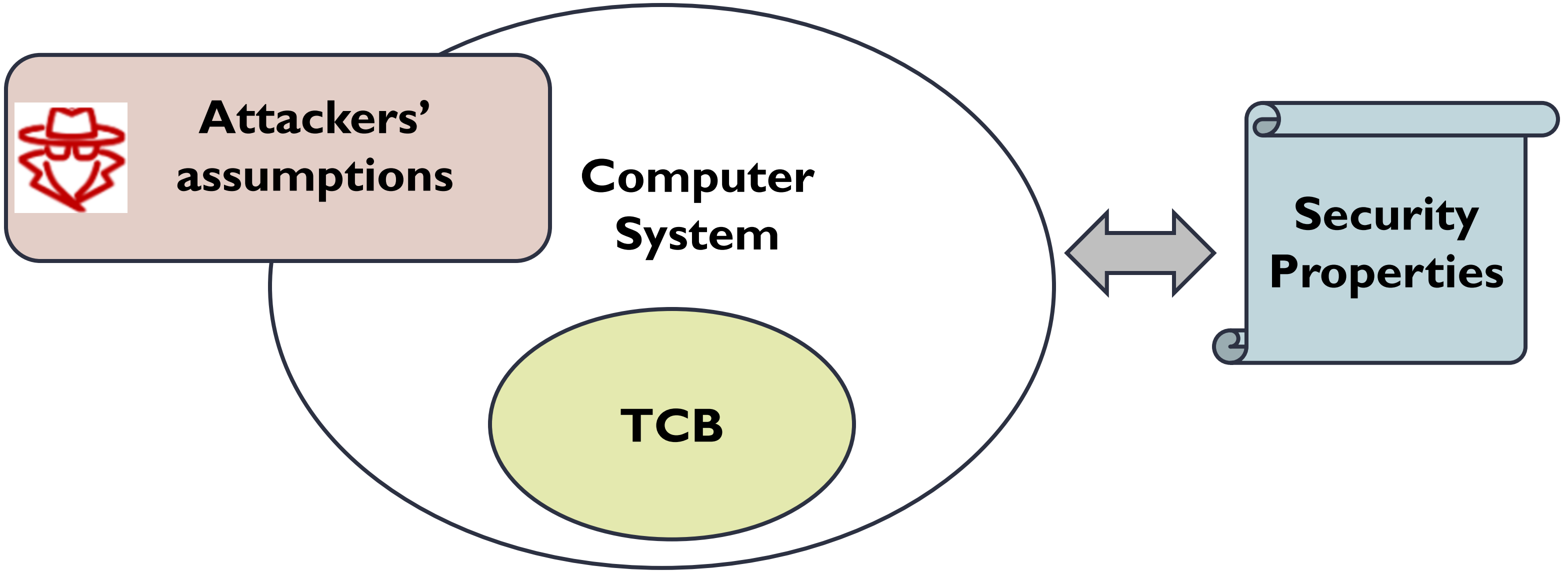
- **Security Strategies**

- **Design Principles of Computer Security**

# Threat Model

## Describe the adversaries and threats in consideration

- What is trusted and what is not trusted (TCB).
- For the untrusted entities, what resources, capabilities and knowledge they have; what actions they can perform.
- What security properties the system aim to achieve.



# Trust

The degree to which an entity is expected to behave:

- What the entity is expected to do:
  - Anti-malware can detect malicious programs;
  - System can prevent illegal account login, etc.
- What the entity is expected not to do:
  - The website will not expose your private data to third parties;
  - An application will not inject virus into your system.

Security cannot be established in a cyber system if no entities are trusted.

It is important to make clear what should be trusted. Otherwise, the designed security solutions may fail in practice.

# Trusted Computing Base (TCB)

A set of components (e.g., software, OS, firmware, hardware) that need to be trusted to ensure the security of the cyber system

Components outside of the TCB can be malicious and misbehave.

When we design a security solution, we need to

- Assume all the components inside the TCB are secure with valid justifications.
- Prevent any damages from any components outside of the TCB.

# TCB Design

## Design principles

- Unbypassable (completeness): there must be no way to breach system security by bypassing the TCB.
- Tamper-resistant (security): TCB should be protected against other parts outside the TCB. These parts cannot modify the TCB's code or state.
- Verifiable (or correctness): it should be possible to verify the correctness of TCB.

## Size of TCB

- A system with a smaller TCB is more trustworthy and easier to verify (we do not need to make too many assumptions, which may be violated). This follows the KISS (Keep It Simple, Stupid) principle
- Designing a secure system with a smaller TCB is more challenging (we need to consider more malicious entities)

# Attacker’s Assumption

## Type of attacker

- Active: manipulate or disrupt the systems, e.g., modifying data, injecting code
- Passive: observing and gathering information without interfering system

## Attacker’s knowledge

- Know the system’s design, architecture, source code, etc. ,
- Lack the detailed knowledge and must rely on probing or trial and error

## Attacker’s capability

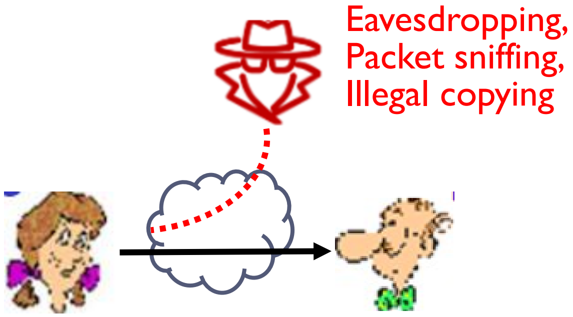
- How much computing resources can the attacker leverage?
- What parts of the system can the attacker interact with?
- Does the attacker have unlimited time or need to act quickly?

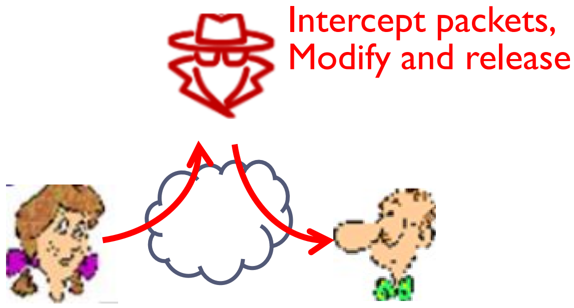
# Security Properties

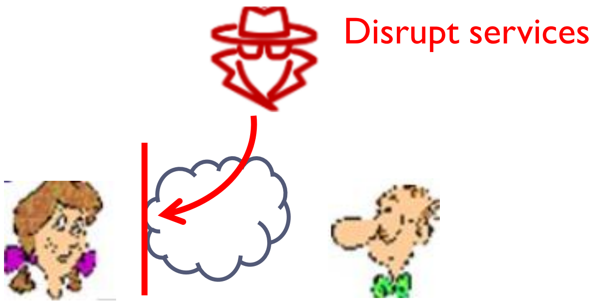
The security goals that we aim to achieve for the system.

Common security properties (CIA model)

- Confidentiality (C): prevent unauthorized disclosure of information. Sensitive information should not be leaked to unauthorized parties
- Integrity (I): prevent unauthorized modification of information. Critical system state and code cannot be altered by malicious parties
- Availability (A): prevent unauthorized withholding of information or resources. The resources should be always available for authorized users







# Security Properties

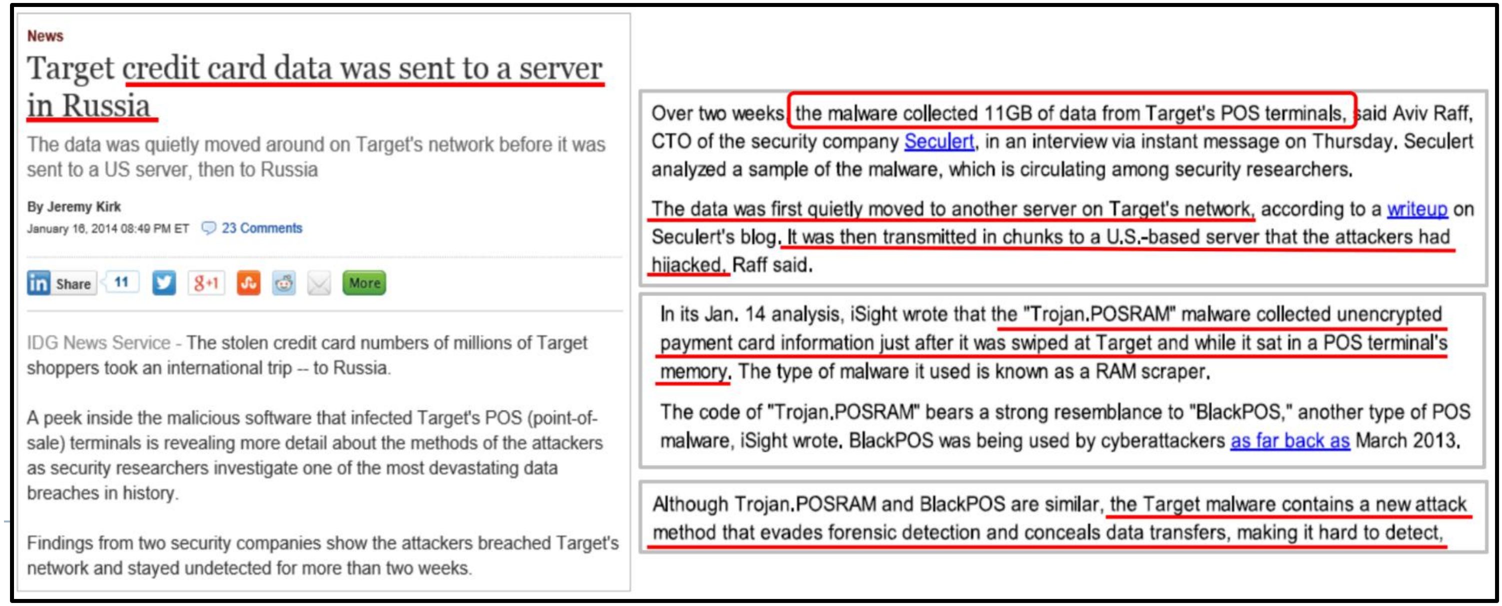
## Other properties

- Accountability: actions of an entity can be traced and identified
- Non-repudiation: unforgeable evidence that specific actions occur
- Authenticity: ensure the communicated entity is the correct entity.
- Anonymity or privacy: hide personal information and identity from being leaked to external parties.
- Verifiability: the system's operations can be independently verified.
- Freshness: the data or communications are current and not reused or replayed.
- Fault tolerance: the system can continue to function correctly despite failures.

# Case Study: Threat Model of Target Attack

## Threat Model

- Trusted Computing Base: the Target computer system including the OS and hardware is trusted. However, the malicious software is not trusted, which leaks the data to the attacker
- Adversarial capabilities and knowledge: the attacker can launch malware on the Target's POS, and collect the credit card data stored in the database.
- Security properties: we consider the confidentiality: protecting the system from leaking sensitive information.



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.

# Security Strategies

## Prevention

- Take measures that prevent your system from being damaged

## Detection

- Take measures so that you can detect when, how, and by whom your system has been damaged.

## Reaction

- Take measures so that you can recover your system or to recover from a damage to your system.
- Always assume that bad things will happen, and therefore prepare your systems for the worst-case outcome

# Design Principle: Least of Privilege

## Assign privileges carefully:

- Give each entity the minimal permissions to complete the task.
- Give the privilege when needed, and revoke the privilege after use
- The less privilege that a program has, the less harm it can do if it goes awry or becomes subverted.
- If granting unnecessary permissions, a malicious entity could abuse those permissions to perform the attack.

## Examples:

- Never perform personal activities using root or admin account in an OS
- A photo editing application on a smartphone is only allowed access to the gallery but not the microphone or location.

# Design Principle: Separation of Privilege

## Split the responsibility:

- To perform a privileged action, it require multiple parties to work together to exercise that privilege, rather than a single point of control or decision.
- Minimize the risk of misuse, error, or compromise by ensuring that no single entity has full control over critical processes

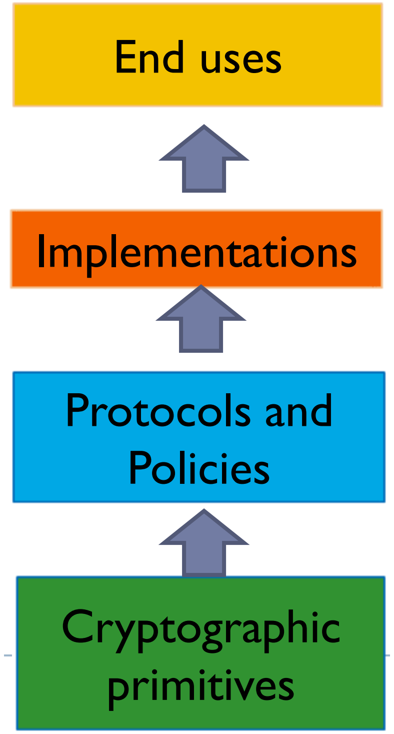
## Examples:

- In a financial system, transferring large sums of money requires approval from an employee (initiator), and additional approval from a manager (reviewer).
- A developer writes code but cannot directly deploy it to production; deployment is handled by a separate operations team

# Design Principles: Defense in Depth

## Multiple types of defenses should be layered together

- Increase the difficulty of attacking the entire system.
- The implementation cost could be high
- The entire effectiveness is often less than the sum of all defenses. There can be even conflicts among them!



End uses

Password managers, company policies…

Implementations

Firewalls, intrusion detection…

Protocols and Policies

TLS, IPsec, access control…

Cryptographic primitives

RSA, DSS, SHA-1…

# Design Principle: Security Through Obscurity

## Relying on secrecy or concealing the details of a system or its components to provide security

- If an attacker does not know how a system works, they are less likely to compromise it.
- This is often regarded as insufficient and unreliable as the sole basis for security. Attackers may reverse-engineer or uncover hidden details. We cannot solely rely on its obscurity to keep attackers away.

## Examples:

- A company hides sensitive files behind obscure URLs without implementing proper authentication. Attacker could discover the URL through guessing, web crawling or server logs.
- A software developer uses code obfuscation to hide the details of source code and potential vulnerabilities. Skilled attacker can deobfuscate or analyze the binary to discover the vulnerabilities.

# Design Principle: Kerckhoffs's Principle and Shannon's Maxim

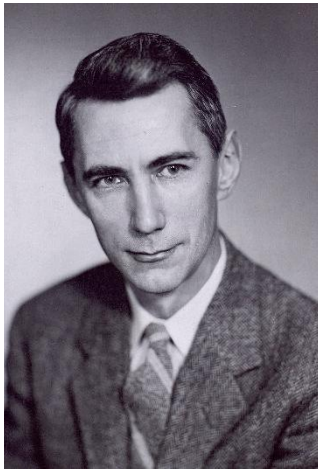
## Claude Shannon: "the enemy knows the system"

- The security of a system should not depend on the secrecy of its design or algorithms.
- It is always necessary to assume that the attacker knows every detail about the system you are designing, including algorithms, hardware, defenses, etc.
- This makes your system resilient even if the design or implementation becomes public knowledge

## Examples:

- Cryptography: the secrecy of the cryptographic key is the only thing that ensures security. If the key is kept confidential, the system remains secure

Auguste Kerckhoffs
Dutch linguist and
cryptographer



Claude Shannon
American mathematician and
cryptographer
Father of information theory