In the Name of Allah, the Most

Beneficent, the Most Merciful

National University
Of Computer and Emerging Sciences

CY2004: Cyber Security (3+0)

WEEK-2

Network

A network is a set of devices (nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network or share resources.

The effectiveness of a network depends on three characteristics.

1**.** ***Delivery***: The system must deliver data to the correct destination.

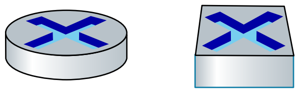
2. ***Accuracy***: The system must deliver data accurately.

3. ***Timeliness***: The system must deliver data in a timely manner.

The Internet: a “nuts and bolts” view

Billions of connected computing *devices*:

- *hosts = end systems*
- running *network apps* at Internet’s “edge”

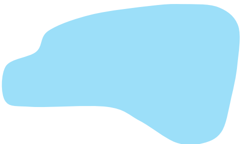


Packet switches: forward packets (chunks of data)

- *routers, switches*

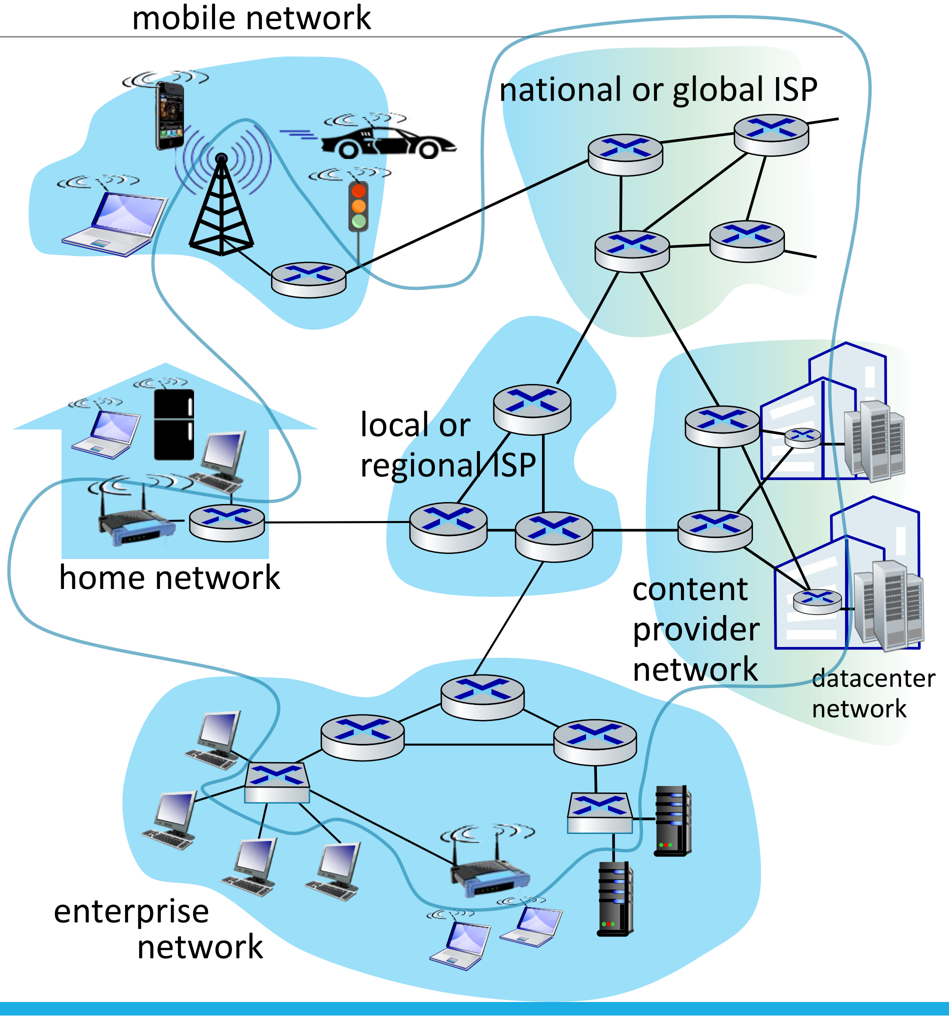
Communication links

- fiber, copper, radio, satellite
- transmission rate: *bandwidth*



Networks

- collection of devices, routers, links: managed by an organization



“Fun” Internet-connected devices

Amazon Echo

Internet refrigerator

IP picture frame

Pacemaker & Monitor

Tweet-a-watt: monitor energy use

bikes

Web-enabled toaster + weather forecaster

Slingbox: remote control cable TV

Security Camera

cars

AR devices

Fitbit

scooters

diapers

Internet phones

Gaming devices

sensorized, bed mattress

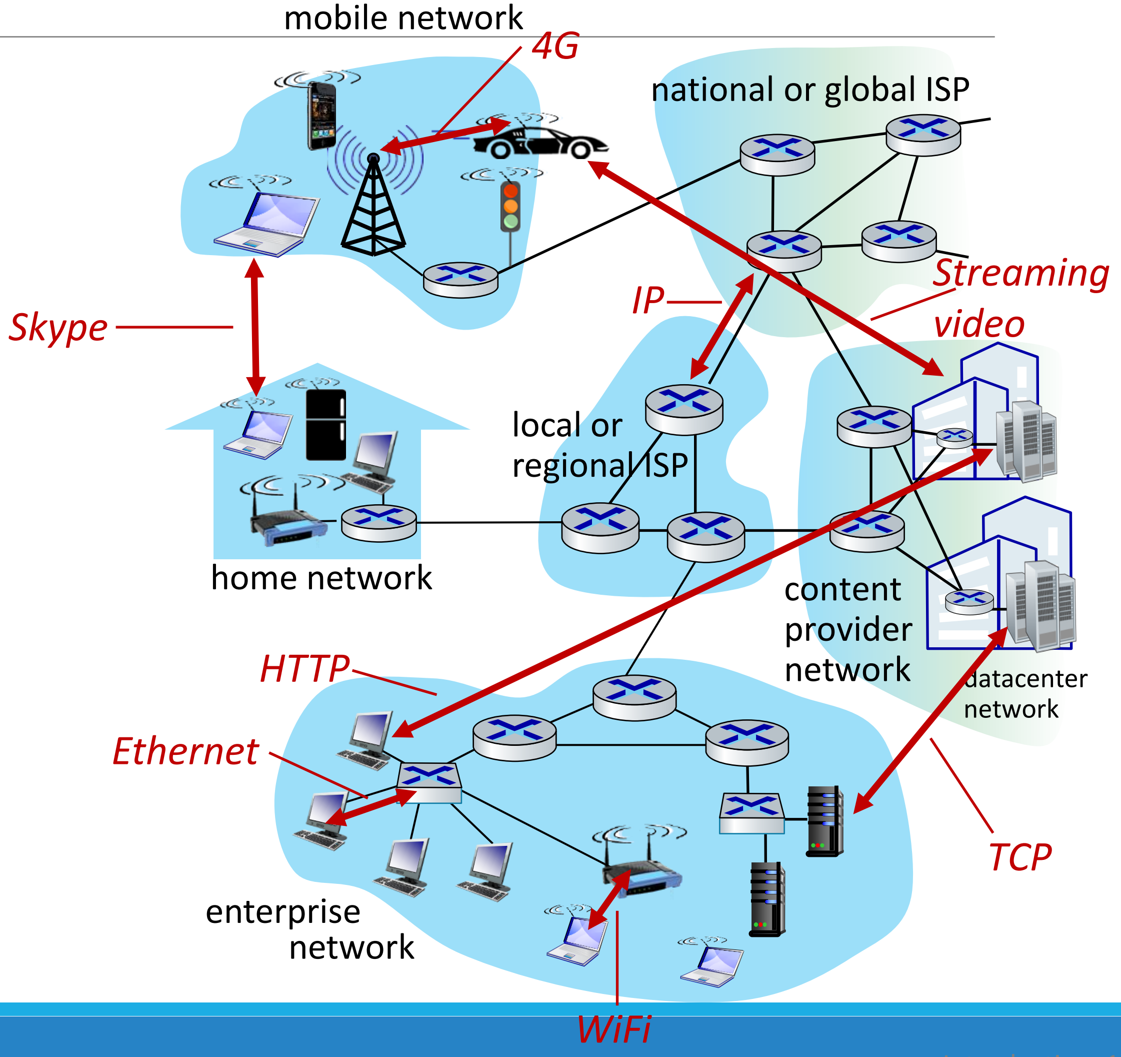
Others?

The Internet: a "nuts and bolts" view

Internet: "network of networks"

- ◦ Interconnected ISPs

- *protocols* are *everywhere*
  - control sending, receiving of messages
  - e.g., HTTP (Web), streaming video, Skype, TCP, IP, WiFi, 4/5G, Ethernet



What is security?

security

noun se·cu·ri·ty \si-ˈkyu̇r-ə-tē\

the quality or state of being secure: such as

a **:** freedom from danger : safety

b **:** freedom from fear or anxiety

c **:** freedom from the prospect of being laid off
<job *security*>

What is computer security?

Keeping systems, programs, and data "safe"

The CIA Triad*:

1. Confidentiality
2. Integrity
3. Availability

“Computer security studies how systems behave in the presence of *an adversary*.”

*Actively tries to cause the system to misbehave.

Confidentiality

- Keep data & resources hidden
  - Data will only be shared with authorized individuals
  - Sometimes – conceal the existence of data or communication
- Traditional focus of computer security
  - Usually accomplished with access control and encryption

Data confidentiality:

> “The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [i.e., to any unauthorized system entity].”
>
> – *RFC 4949, Internet Security Glossary*

Confidentiality vs. privacy

Privacy

- Limit what information can be shared with others
- Ability to send messages anonymously
- Control other’s use of information about you
- Freedom from intrusion

The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share its personal information with others.

See: HIPAA, personal information, Privacy Act of 1974
RFC 4949, Internet Security Glossary

Privacy is a reason for confidentiality

Secrecy: hiding the existence of information; the ability to conceal messages or exchange messages without anyone else seeing them

Privacy is increasingly harder to attain

- “Free services”
  - Facebook, Google, Twitter, LinkedIn, Instagram, TikTok, …
  - Information collection, browser cookies to track web access
- More data is online and widely accessible
  - No need to go to town hall to get real estate transactions
- Phone companies know every place you go
- Big data analytics
  - It’s increasingly easy to correlate data:
    Credit card spending, travel, jobs, marriages/divorces, kids, cars, …
- This can be good and bad

Privacy & data mining … on a national level

- U.S. credit scores
  - Credit reporting companies track employment, spending, home ownership, loan repayment, …
  - Credit scores affect ability to borrow money, buy a home
- China’s social credit system
  - Track trustworthiness of everyday citizens, corporations, and government officials
  - Track behavior
    - Frivolous spending, major & minor infractions (smoking in a no-smoking zone)
  - Boost public confidence and fight problems like corruption and business fraud

Integrity

- The trustworthiness of the data or resources
- Preventing unauthorized changes to the data or resources
- Data integrity
  - Property that data has not been modified or destroyed in an unauthorized or accidental manner
- Origin integrity
  - Authentication
- System integrity
  - The ability of a system to perform its intended function, free from deliberate or inadvertent manipulation

Often more important than confidentiality!

Availability

- Being able to use the data or resources
- Property of a system being accessible and capable of working to required performance specifications

Turning off a computer provides confidentiality & integrity but hurts availability

Denial of Service (DoS) attacks target availability

Basic Terminologies - Security

Why is vocabulary important?

There is a problem with vocabulary in this field. Many words have different context and meaning to different groups (e.g., the policy folks in the field).

- Many words are also misused by media.

Event - Could be anything

Incident - A malicious event

Adversary – One who misbehaves

Bug - An error that exists in the implementation-level (i.e. only exist in source code); very correctable

Flaw - An error at a much deeper level, particularly in the design, and likely in code level; can be very difficult and costly to correct

Hacker - A creative programmer; a positive connotation

Cracker - The bad guy, the attacker, what media coins "hacker" (the negative connotation). We'll use **attacker** in this class.

Basic Terminologies - Security

Black hat - An attacker with malicious intents

White hat - An attacker with good intents (i.e., the white knight)

Gray hat - An attacker with good and bad intents

Script kiddie or **skiddie** - Nuisance; not going away any time soon; 1337 (i.e., elite) wannabes; use scripts and exploits written by others and do not understand how they really work; always a lamer

Vulnerability - A security bug (thanks Giovanni Vigna); a weakness in a system that can potentially be exploited by an attacker

Exploiting or **exploitation** - The act of taking advantage of a vulnerability

Exploit - Software program that performs the exploiting

Risk - The likelihood that an attacker will take advantage of that vulnerability

Threat - The likelihood that an incident will happen

pwn3ed - Owned; successful exploitation; computer system completely compromised

Zero day - an undisclosed vulnerability that attackers can take advantage of. A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability—hence “zero-day.” https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html

Violating the CIA Triad: If You Were An Attacker, What Are Your Goals?

- Preventing enemies from communicating over network
- Steal information for attacker's benefit and get away with it
- Disruption of business, daily life, day-to-day operations
- Inserting information that "shouldn't be there”
- Destroy information, resources
- Gain access to a system and maintain access to system for a long time
- Monitoring people what they are doing (e.g., webcams)
- Challenging adversaries, pinpointing weaknesses
- For fun and profit (e.g., the black market)
- Spread propaganda
- Building a blueprint of weaknesses…
- …and keep it for future reference

What’s adversarial thinking?

“Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.”

- Bruce Schneier

Adversarial thinking disclaimer

Hopefully, you will learn to think like a criminal mastermind but behave like a gentleman/woman!

Adversarial thinking: key questions

Security goal: what security policy to enforce?

Threat model: who is the adversary? What actions can the adversary perform?

Mechanisms: What security mechanisms can be used to achieve the security goals given the adversarial model

Key security goals

Confidentiality: Data not leaked

Integrity: Data not modified

Availability: Data is accessible when needed

Authenticity: Data origin cannot be spoofed

You can apply adversarial thinking anywhere

Columbia ID cards

- Can you fake an ID card?

ATM machine

- How does the service person gets access to refill it with cash?

MTA metrocard

- Can you increase the card balance without paying?

Example: air travel

Print boarding pass at home

→

ID check by TSA

→

Boarding pass check at the gate

Adversarial thinking example: air travel

Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)

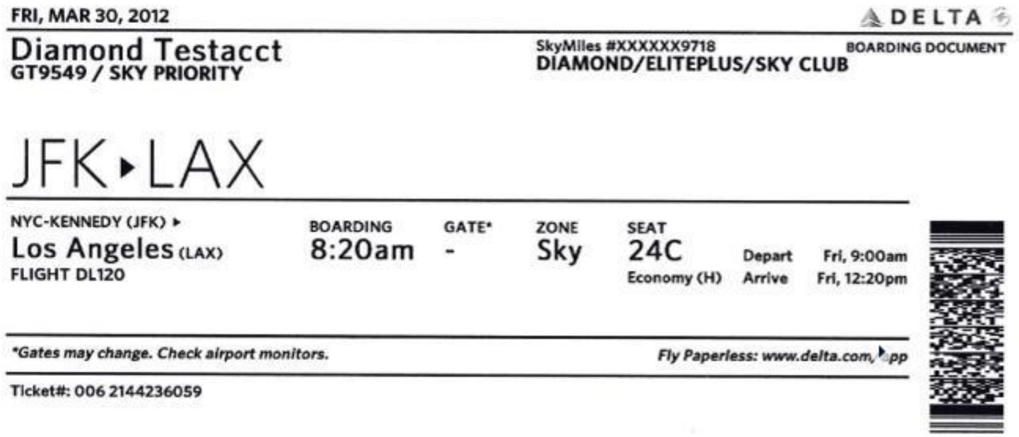
Mechanisms

- TSA checks validity of the ID (e.g., driver's license) and the boarding pass How?
- TSA matches name in the ID against the name in the boarding pass
- TSA ensures that the name is not on the no-fly list
- Gate agent checks whether the boarding pass is valid and has been checked by TSA How?

Can an attacker who is on the no-fly list fly?

What is the threat model?

Can an attacker create a fake boarding pass?



FRI, MAR 30, 2012 DELTA

Diamond Testacct
GT9549 / SKY PRIORITY

SkyMiles #XXXXXX9718
DIAMOND/ELITEPLUS/SKY CLUB

BOARDING DOCUMENT

JFK ▸ LAX

NYC-KENNEDY (JFK) ▸
Los Angeles (LAX)
FLIGHT DL120

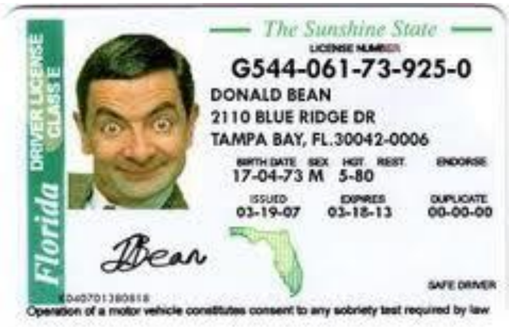
BOARDING	GATE*	ZONE	SEAT		
8:20am	-	Sky	24C Economy (H)	Depart Arrive	Fri, 9:00am Fri, 12:20pm

*Gates may change. Check airport monitors.

Fly Paperless: www.delta.com/app

Ticket#: 006 2144236059

Can an attacker fake a driver's license?



Florida DRIVER LICENSE CLASS E

The Sunshine State

LICENSE NUMBER
G544-061-73-925-0
DONALD BEAN
2110 BLUE RIDGE DR
TAMPA BAY, FL.30042-0006

BIRTH DATE	SEX	HGT	REST	ENDORSE
17-04-73	M	5-80		

ISSUED	EXPIRES	DUPLICATE
03-19-07	03-18-13	00-00-00

DBean

SAFE DRIVER

D040701380818

Operation of a motor vehicle constitutes consent to any sobriety test required by law

Security under different threat models

Security goal: Ensure that each person getting inside an airport has a valid boarding pass and is authorized to fly (i.e., not on the no-fly list)

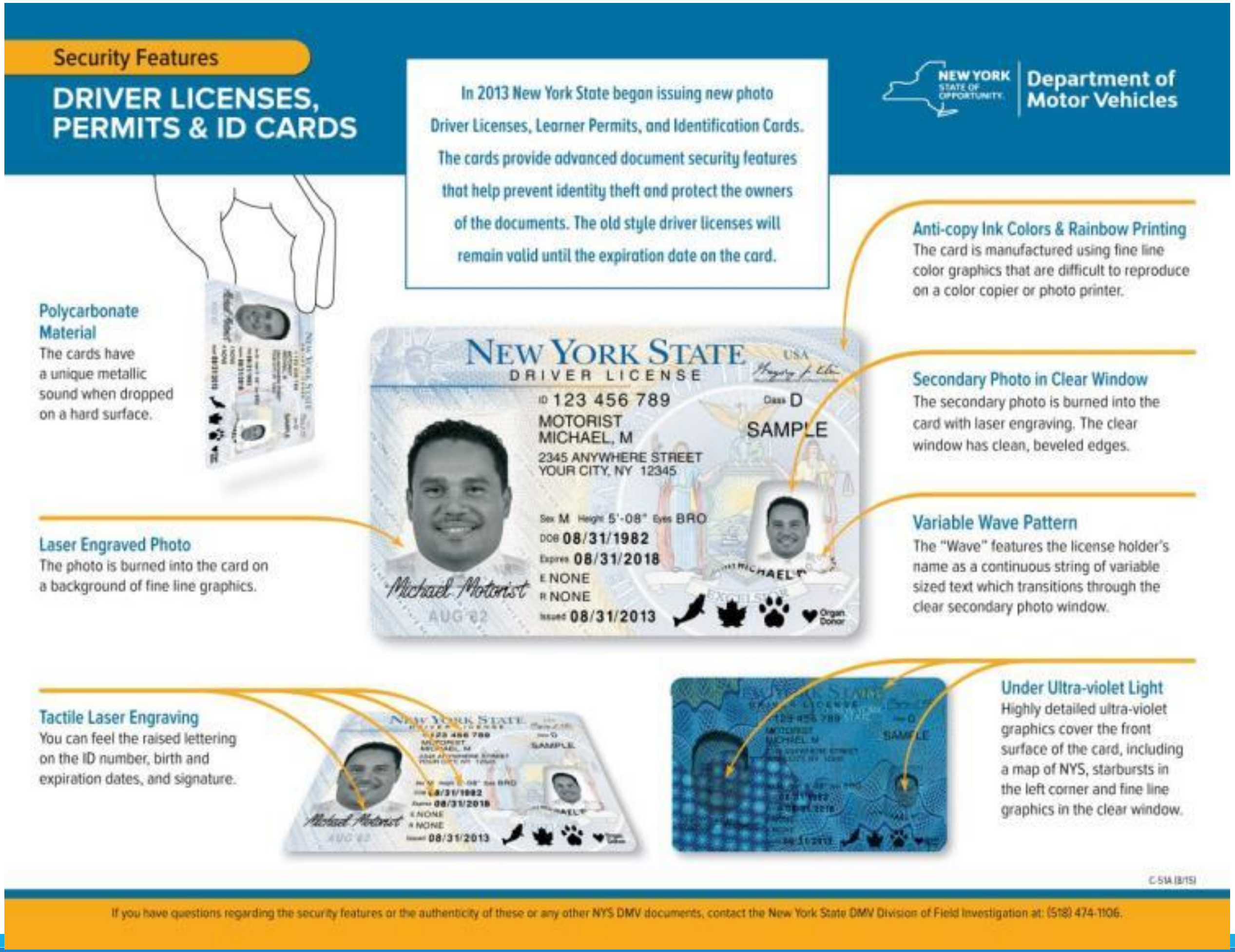
- What are the minimum requirements for someone to violate this goal in the current TSA system?
- The current TSA system is secure under which threat models?

Not all threat models are equal

Which one is harder and why?

- Creating a fake boarding pass
- Creating a fake driver’s license

Security measures in a driver’s license?



Security Features

DRIVER LICENSES, PERMITS & ID CARDS

In 2013 New York State began issuing new photo Driver Licenses, Learner Permits, and Identification Cards. The cards provide advanced document security features that help prevent identity theft and protect the owners of the documents. The old style driver licenses will remain valid until the expiration date on the card.

NEW YORK STATE OF OPPORTUNITY. | Department of Motor Vehicles

Polycarbonate Material
The cards have a unique metallic sound when dropped on a hard surface.

Anti-copy Ink Colors & Rainbow Printing
The card is manufactured using fine line color graphics that are difficult to reproduce on a color copier or photo printer.

Secondary Photo in Clear Window
The secondary photo is burned into the card with laser engraving. The clear window has clean, beveled edges.

Laser Engraved Photo
The photo is burned into the card on a background of fine line graphics.

Variable Wave Pattern
The "Wave" features the license holder's name as a continuous string of variable sized text which transitions through the clear secondary photo window.

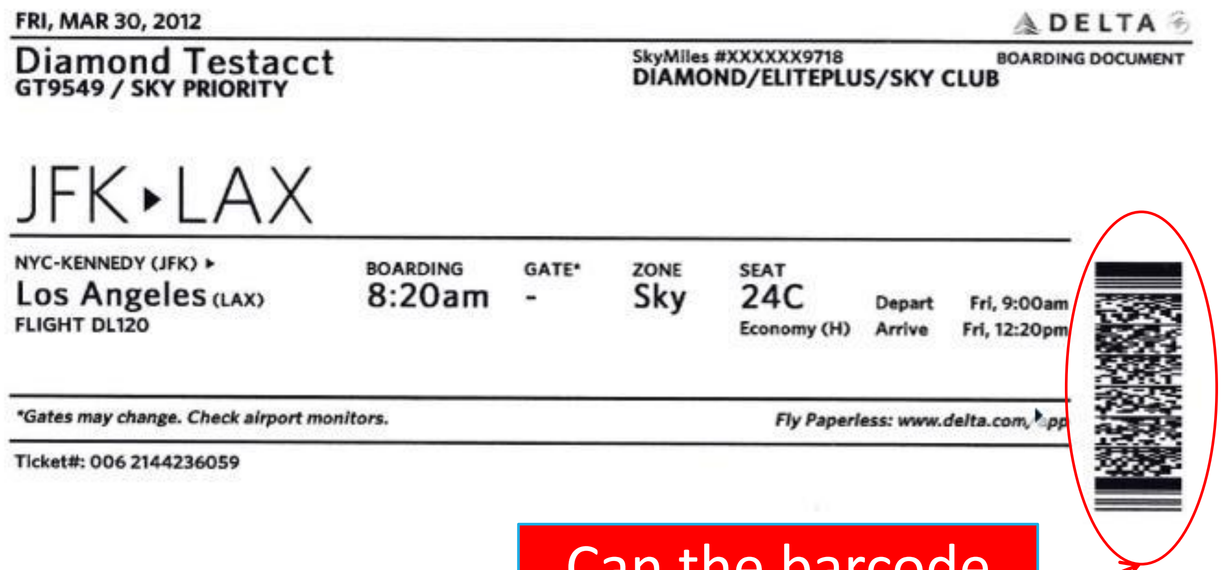
Tactile Laser Engraving
You can feel the raised lettering on the ID number, birth and expiration dates, and signature.

Under Ultra-violet Light
Highly detailed ultra-violet graphics cover the front surface of the card, including a map of NYS, starbursts in the left corner and fine line graphics in the clear window.

C-51A (8/15)

If you have questions regarding the security features or the authenticity of these or any other NYS DMV documents, contact the New York State DMV Division of Field Investigation at: (518) 474-1106.

Security measures in a boarding pass?



FRI, MAR 30, 2012

DELTA

Diamond Testacct
GT9549 / SKY PRIORITY

SkyMiles #XXXXXX9718
DIAMOND/ELITEPLUS/SKY CLUB

BOARDING DOCUMENT

JFK ▸ LAX

NYC-KENNEDY (JFK) ▸
Los Angeles (LAX)
FLIGHT DL120

BOARDING	GATE*	ZONE	SEAT		
8:20am	-	Sky	24C	Depart	Fri, 9:00am
			Economy (H)	Arrive	Fri, 12:20pm

**Gates may change. Check airport monitors.*

Fly Paperless: www.delta.com/app

Ticket#: 006 2144236059

Can the barcode be faked?

Air travel revisited:
a different security goal

Print boarding pass at home

→

ID check by TSA

→

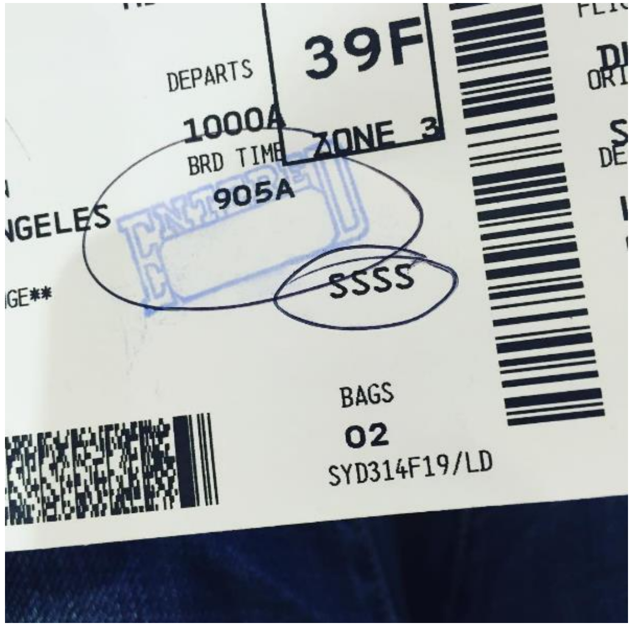
Boarding pass check at the gate

Security goal: everybody boarding an aircraft must pass through TSA security check

Everybody must go through TSA checks

How does the current TSA system ensure this?

What is an example threat model where this goal can be violated by an attacker?

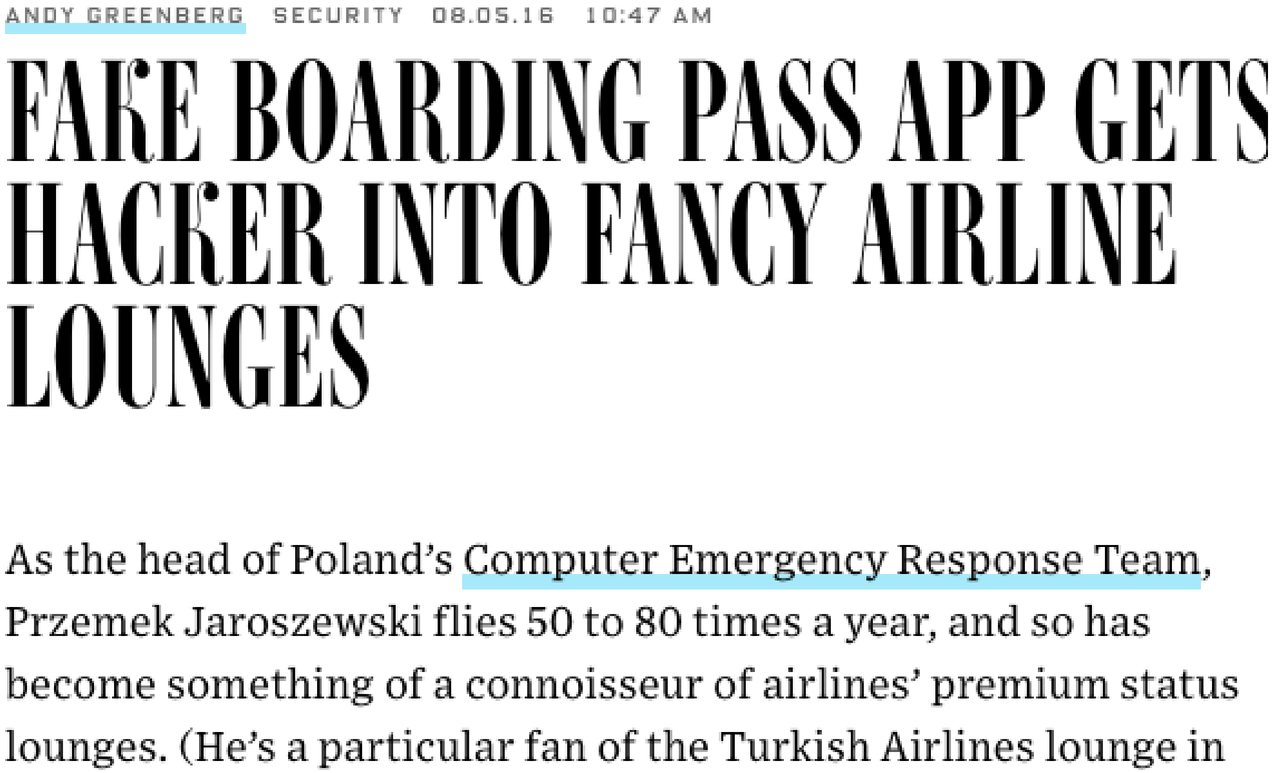


Yet another security goal

Only authorized travelers should be allowed to enter premium lounges

- How will the receptionist at the lounge know who is authorized?

What is the threat model for this attack?



ANDY GREENBERG SECURITY 08.05.16 10:47 AM

FAKE BOARDING PASS APP GETS HACKER INTO FANCY AIRLINE LOUNGES

As the head of Poland's Computer Emergency Response Team, Przemek Jaroszewski flies 50 to 80 times a year, and so has become something of a connoisseur of airlines' premium status lounges. (He's a particular fan of the Turkish Airlines lounge in

How will you fix it?

What about TSA Pre-Check?

How does TSA Pre-Check work?

- Passengers apply for Pre-Check
- TSA decide whether the passenger is eligible for Pre-Check or not and sends the information back to the Airline.
- The Airline encodes that information in a barcode that is on the issued boarding pass.

Hacking TSA Pre-Check

→

→

M1PUCK/COLWMR YXXXXXX PHXEWRUA XXX
294RXXXFXX 11F>30B

WWXXX BUA 0E016 3

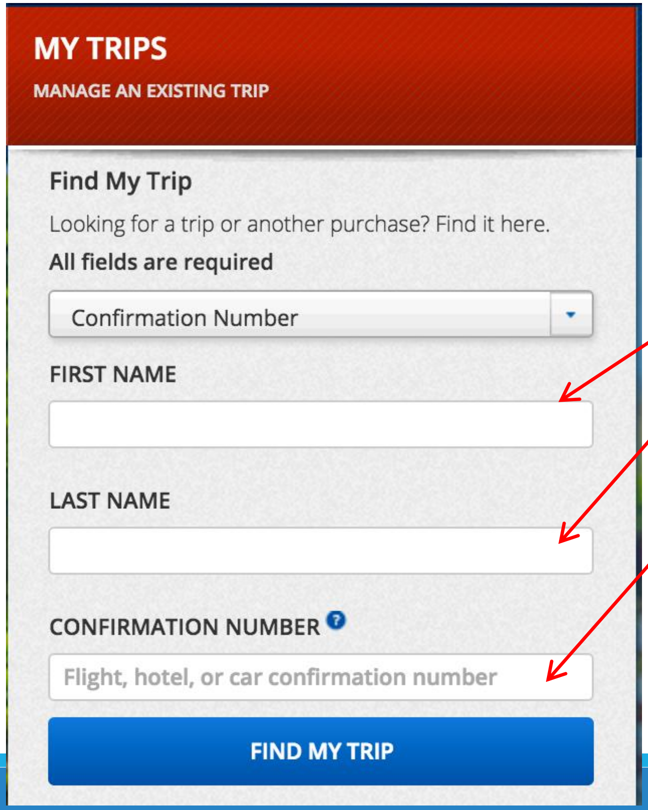
1 means no Pre-Check and
3 means Pre-Check

No encryption

Source: https://puckinflight.wordpress.com/2012/10/19/security-flaws-in-the-tsa-pre-check-system-and-the-boarding-pass-check-system/

Unintended side-effects of the boarding-pass design

What happens if someone else gets hold of your boarding pass?



MY TRIPS

MANAGE AN EXISTING TRIP

Find My Trip

Looking for a trip or another purchase? Find it here.

All fields are required

Confirmation Number

FIRST NAME

LAST NAME

CONFIRMATION NUMBER

Flight, hotel, or car confirmation number

FIND MY TRIP

All this information is in the boarding pass in cleartext

A different setting: money

Coins were introduced around 6/7th century BCE

- Make tokens out of scarce resources(gold and silvers)
- Apply a signature that is hard to copy (depends on the skills of the engravers)
- Harsh penalty for forgers

Modern crypto-currencies

Same principles!

- Scarce resource: computation
- Hard-to-forge data: cryptography (encryption)

Why the Rash of Incidents: Behind the Breaches and Attacks (thoughts from former students)

- Trust relationships, lots of implicit trust
- Data is very valuable
- Convenient to put everything online; sharing
- Lack of education; people are not being informed
- No barriers to entry
- Lack of deterrence
- Software vulnerabilities
- Misconfigurations
- Human elements, social engineering
- Scapegoating

Cybersecurity

“a computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems”.

“ the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to **strengthen the confidentiality, integrity and availability of these systems**.”

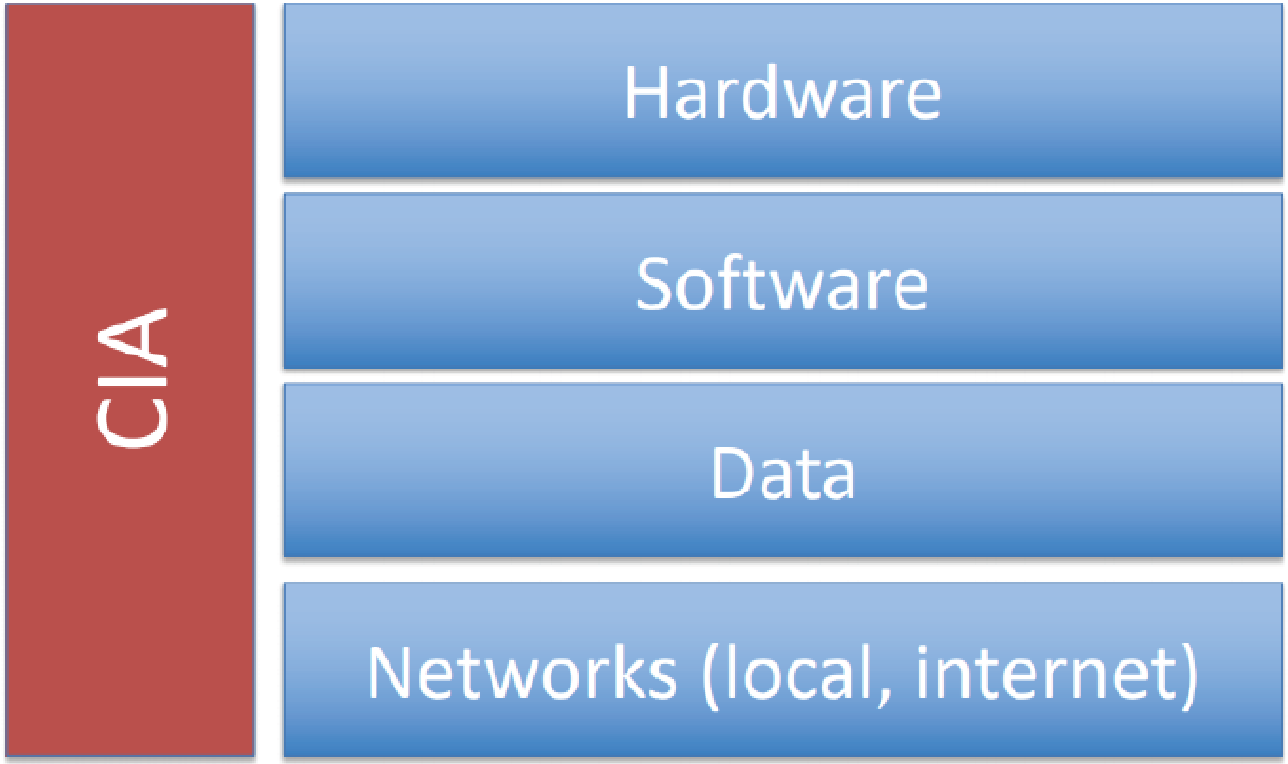
US National Institute of Standards –

Information Technology Laboratory

https://csrc.nist.gov/glossary/term/cybersecurity

Systems resources or assets

What are we trying to **protect**?



Further terms

- **Non-repudiation** – means one party cannot deny receiving a message or a transaction, nor can the other party deny sending a message or a transaction (only Ian could have sent that message)
- **Authenticity** – proving who you are and each input is from a trusted source **(the message was sent by Ian and is genuine)**
- **Accountability** – tracing the actions of an entity uniquely to that entity **(there is a record of who sent the message and controls exist on how that record is updated)**

What are we protecting against?

- **Weakness** in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

- Examples of vulnerabilities for Internet banking

  ○ I always use an easy to guess password

  ○ Internet banking gives anyone access if a longer than expected

password is entered

  ○ I do all of my internet banking using a PC at the local internet cafe

Threat and Attack

- A threat is any circumstance or event with the potential to

adversely impact the security properties of an information system

- events can be intentional or unintentional
- emphasis on potential effect

- An attack **is an attempt to gain unauthorised** access to system services, resources, or information, or **an attempt to compromise** system integrity, availability, or confidentiality.
  - always intentional in nature
  - exploits a vulnerability that exists in the system
  - successful attack is a threat that has happened

Examples of Threat and Attack

- Examples of vulnerabilities for Internet banking
  - I always use an easy to guess password
  - Internet banking gives anyone access if a longer than expected password is entered
  - I do all of my internet banking using a PC at the local internet café
- Threats and attacks:
  - Attacker guesses my password
  - Attacker enters very long password
  - Attacker installs a keylogger to collect my password

Passive versus active threats and attacks

- Threats and attacks can be passive or active in nature
- Passive make no change to the system
  - E.g. guessing my password
- Active makes changes to the system
  - E.g. enters a very long password

Insider vs. Outsider Threats and Attacks

- Threats and attacks can come from inside or outside an

organization

- Insider is usually user with legitimate access to a system

but misuses it

  - I take money from my own account and claims it was stolen

- Outsider requires taking over the privileges of an insider

  - Attacker guesses my password, uses it to access my account

and transfer money to themselves

Countermeasures

Countermeasures are any means taken to try and prevent a successful attack. These may be technical or operational in nature.

- Consider Internet banking:
  - Train the user to choose harder to guess passwords.
  - Reject passwords that are too long.
  - Always use a computer that only I can access.
- **Unsuccessful countermeasure** leads to **successful attack** and a security property being violated
  - E.g. I lose money from my account (integrity property)

Why it is had to get it right?

1. Select defenses by considering **many** different attacks.

2. Only **one** attack needs to succeed.

3. Need to place defense **at the right point** in the system.

4. May rely on **keeping secrets** but also sharing them.

5. Battle of wits between attacker and defender.

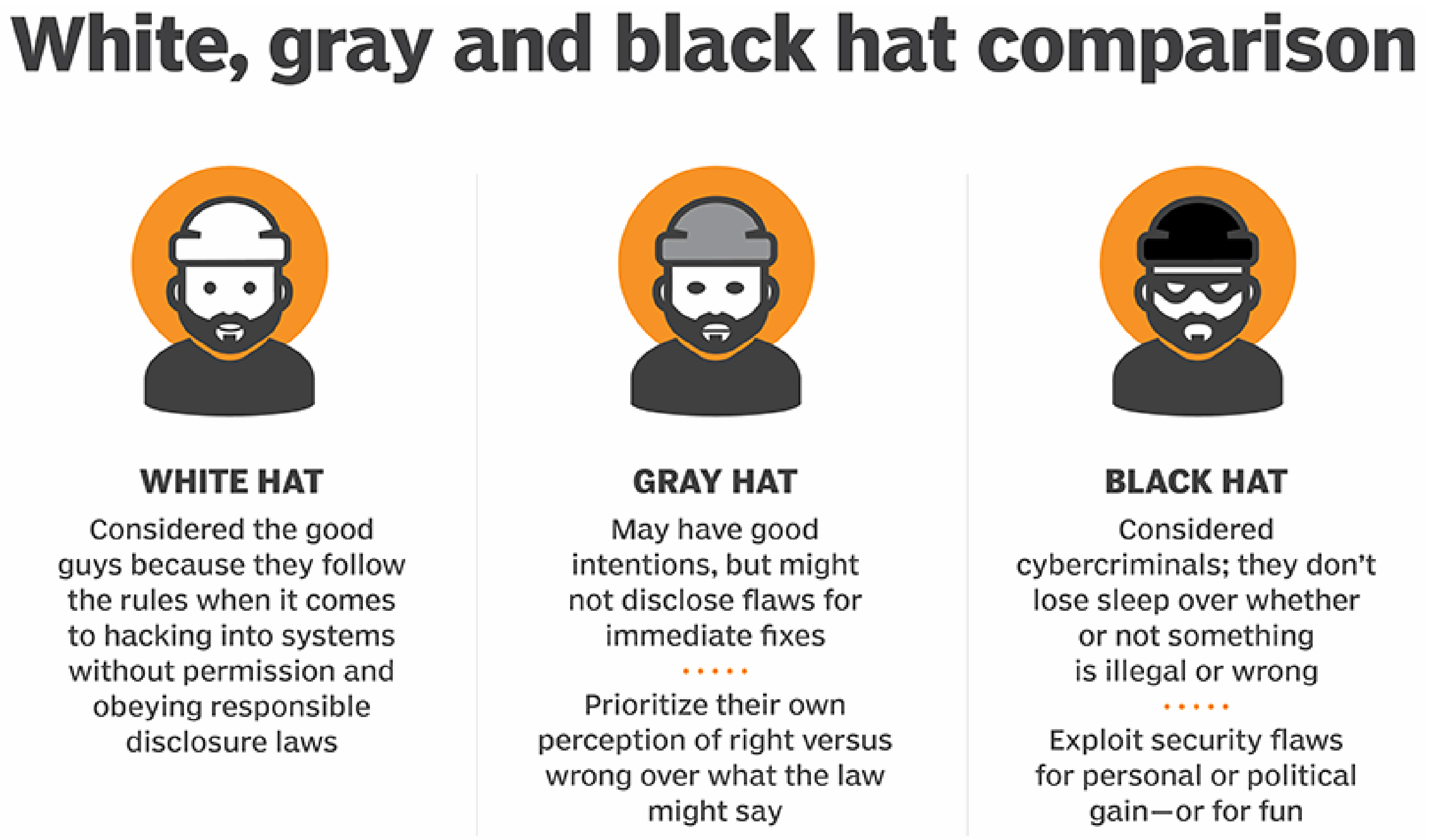
6. People **don’t** realize value until security failure.

7. Security requires **constant** monitoring.

8. Often added as an **afterthought**.

9. Strong security viewed as making system **hard to use**.

Who are the attackers?



White, gray and black hat comparison

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

Exploit security flaws for personal or political gain—or for fun

Types of Black Hat Hackers

- An adversary is a particular type of blackhat hacker.
- *Individual, group, organization or government that* ***conducts*** *or* ***has the intention*** *to conduct detrimental activities.*
- Lots of different types, with varying:
  - Ability
  - Resources
  - Motivations

Types of adversary: Cyber criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Typically they are young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

Types of adversary: Activists

Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes

- Also know as hacktivists

○ Skill level is often quite low

- Aim of their attacks is often to promote and publicize their cause

typically through:

○ Website defacement

○ Denial of service attacks

○ Theft and distribution of data that results in negative publicity or compromise of

their targets

THE ASSET THEY ARE INTERESTED IN IS YOUR ATTENTION

Types of adversary: State-sponsored organizations

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

APTs

An advanced persistent threat (APT) is a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illegal, long-term presence on a network in order to find patterns and relationship in highly sensitive data.

The targets of these attacks, which are very carefully chosen and researched, typically include large enterprises or governmental networks.

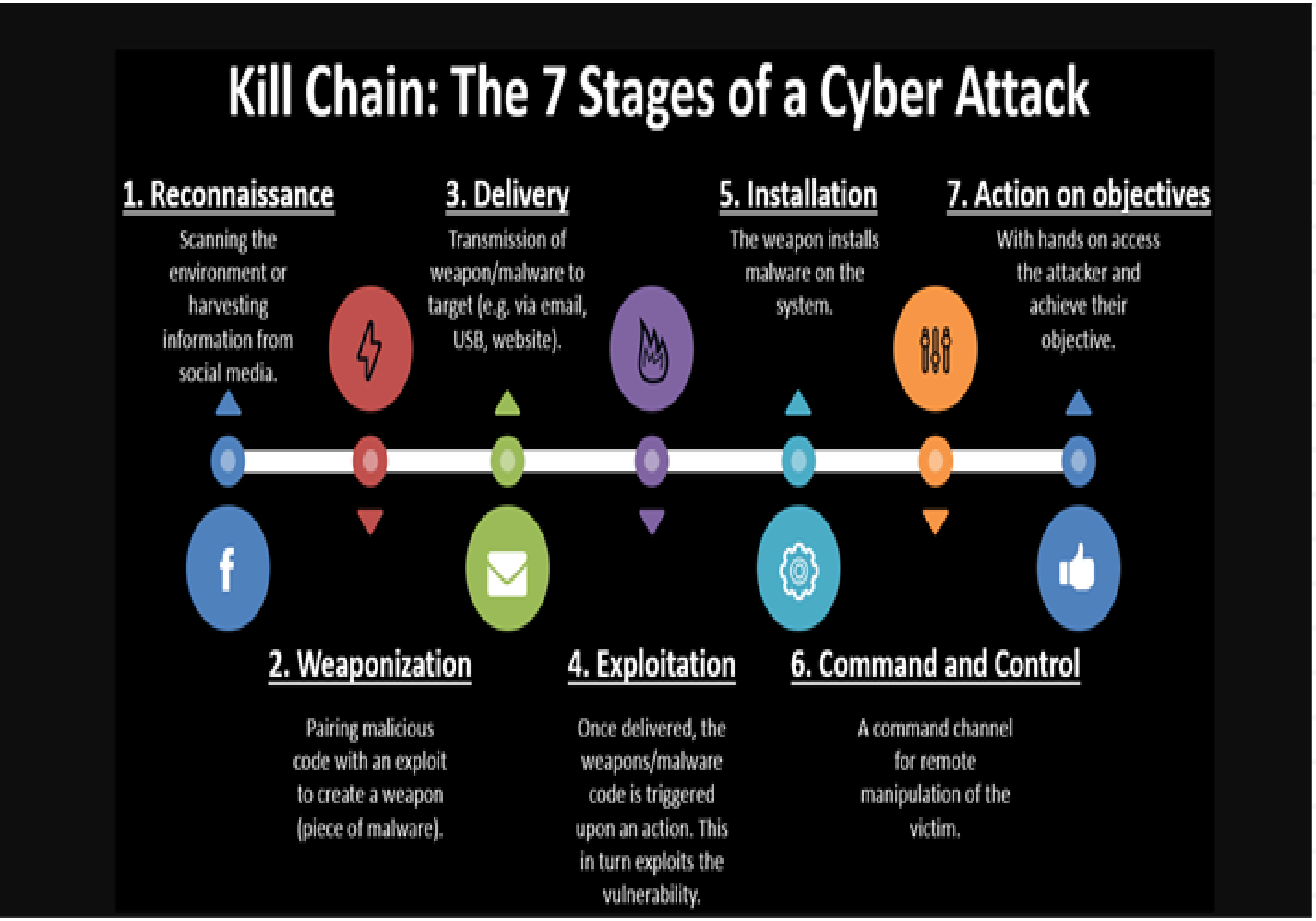
The consequences of such intrusions are vast, and include:

- Unauthorized access to classified information such as credit cards, bank accounts, passport details, etc.
- Sabotage the entire system, including the cloud, by deleting the complete database.
- Taking over the critical website and making major changes such as the stock market or hospital.
- Accessing essential systems with the credentials of the people.
- Access to sensitive or incriminating information through communication.
- Intellectual property theft (e.g., trade secrets or patents)

Types of APTs

Although there are many types of advanced persistent threats, the following are the most common:

1. **Social engineering:** It is possible to influence, manipulate, or trick an organization into revealing sensitive information.
2. **Phishing:** Cybercriminals typically send a fake message that contains a phishing website link that appears to come from a reputable company, a friend, or an acquaintance.
3. **Rootkits**: Hackers can take control of a target device with malware, such as rootkits.
4. Other APT attack examples are computer worms, bots, spyware, adware, ransomware, remote execution, web shell, rootkits, keylogger, and many more.



Kill Chain: The 7 Stages of a Cyber Attack

1. Reconnaissance
Scanning the environment or harvesting information from social media.

2. Weaponization
Pairing malicious code with an exploit to create a weapon (piece of malware).

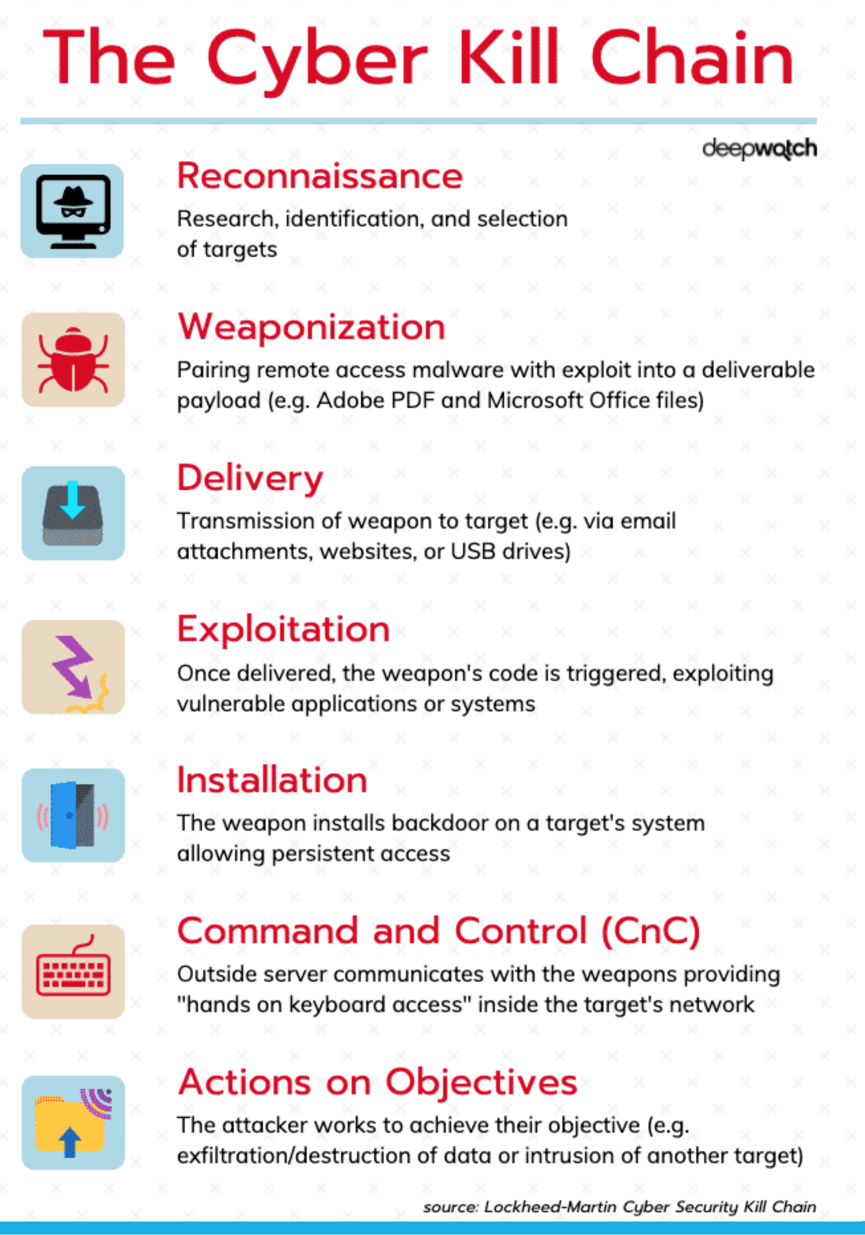
3. Delivery
Transmission of weapon/malware to target (e.g. via email, USB, website).

4. Exploitation
Once delivered, the weapons/malware code is triggered upon an action. This in turn exploits the vulnerability.

5. Installation
The weapon installs malware on the system.

6. Command and Control
A command channel for remote manipulation of the victim.

7. Action on objectives
With hands on access the attacker and achieve their objective.



The Cyber Kill Chain

Reconnaissance
Research, identification, and selection of targets

Weaponization
Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)

Delivery
Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)

Exploitation
Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems

Installation
The weapon installs backdoor on a target's system allowing persistent access

Command and Control (CnC)
Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network

Actions on Objectives
The attacker works to achieve their objective (e.g. exfiltration/destruction of data or intrusion of another target)

source: Lockheed-Martin Cyber Security Kill Chain