SECURITY

SECURITY

SECURITY REFERS TO THE PROTECTION OF ASSETS

HMM... OKAY.. WHAT ARE ASSETS?

SECURITY

SECURITY REFERS TO THE PROTECTION OF ASSETS

TANGIBLE ASSETS

Physical assets, valuables such as jewelry, art, collections

Confidential data such as passwords, credit card numbers, bank account transactions etc

INTANGIBLE ASSETS

Reputation, Trust, Goodwill

SECURITY

SECURITY REFERS TO THE PROTECTION OF ASSETS

This is the one we're most interested in!

Confidential data such as passwords, credit card numbers, bank account transactions etc

SECURITY

We trust more and more of our personal information to websites

This makes things in our life very convenient but much more vulnerable

SECURITY

Hacking attacks and security breaches make headlines everyday!

SECURITY

They range from serious, large-scale attacks...

SECURITY

Credit and debit card accounts stolen in a recent data breach at retail giant Target have been flooding underground black markets in recent weeks, selling in batches of one million cards and going for anywhere from $20 to more than $100 per card, KrebsOnSecurity has learned.

Prior to breaking the story of the Target breach on Wednesday, Dec. 18, I spoke with a fraud analyst at a major bank who said his team had independently confirmed that Target had been breached after buying a huge chunk of the bank's card accounts from a well-known "card shop" — an online store advertised in cybercrime forums as a place where thieves can reliably buy stolen credit and debit cards.

There are literally hundreds of these shady stores selling stolen credit and debit cards from virtually every bank and country. But this store has earned a special reputation for selling quality "dumps," data stolen from the magnetic stripe on the backs of credit and debit cards. Armed with that information, thieves can effectively clone the cards and use them in stores. If the dumps are from debit cards and the thieves also have access to the PINs for those cards, they can use the cloned cards at ATMs to pull cash out of the victim's bank account.

In December 2015 Target the US retailer announced that 40 million debit and credit card number used in stores across the US

These numbers were then available for sale in shady stores selling cards

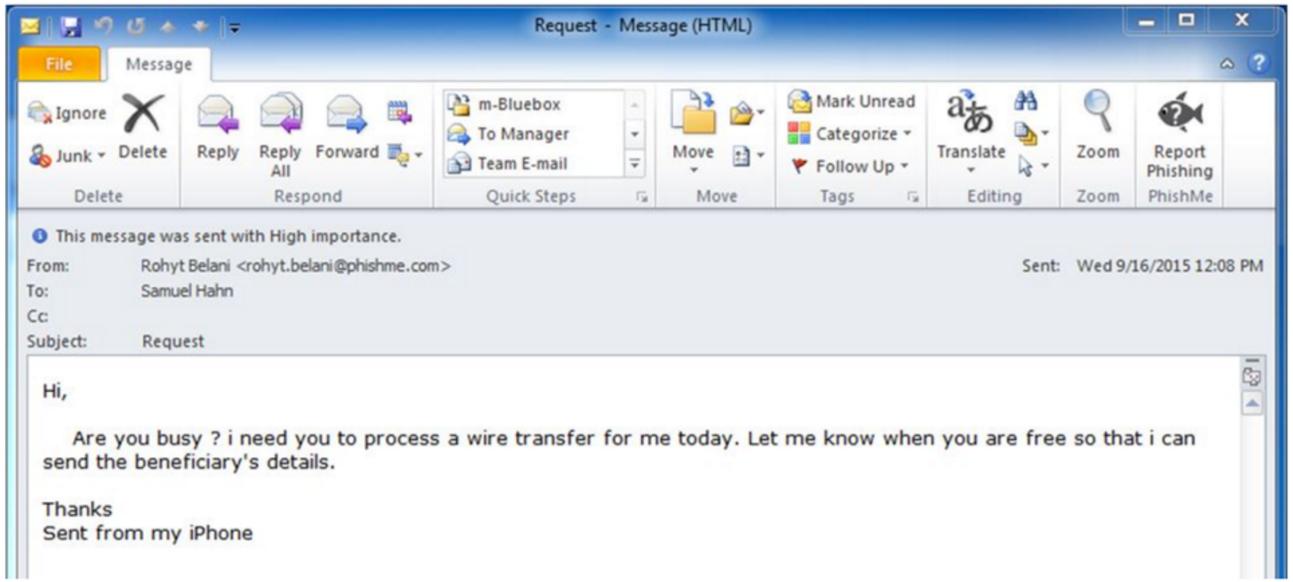
SECURITY

To simple ones...

SECURITY

The **U.S. Federal Bureau of Investigation** (FBI) this week warned about a "dramatic" increase in so-called "CEO fraud," e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams have cost organizations more than $2.3 billion in losses over the past three years.

In an alert posted to its site, the FBI said that since January 2015, the agency has seen a 270 percent increase in identified victims and exposed losses from CEO scams. The alert noted that law enforcement globally has received complaints from victims in every U.S. state, and in at least 79 countries.



A typical CEO fraud attack. Image: Phishme

A message from the CEO to someone in the org asking for money to be transferred

SECURITY

To the ridiculous... and life changing

SECURITY

Large caches of data stolen from online cheating site **AshleyMadison.com** have been posted online by an individual or group that claims to have completely compromised the company's user databases, financial records and other proprietary information. The still-unfolding leak could be quite damaging to some 37 million users of the hookup service, whose slogan is "Life is short. Have an affair."

The data released by the hacker or hackers — which self-identify as **The Impact Team** — includes sensitive internal data stolen from Avid Life Media (ALM), the Toronto-based firm that owns AshleyMadison as well as related hookup sites **Cougar Life** and **Established Men**.

Many prominent public personalities have been outed as a result of this breach

SECURITY BUILDING BLOCKS

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS
AUTHENTICATION

Who are you?

SECURITY BUILDING BLOCKS
AUTHENTICATION

This answers the question
"Who are you?"

This is used to uniquely identify the clients of your system - whether they are human or other services

SECURITY BUILDING BLOCKS

AUTHENTICATION

This answers the question "Who are you?"

This is used to uniquely identify the clients of your system - whether they are human or other services

Authentication deals with identity - when you log into a website it knows who you are

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS
AUTHORIZATION

What can you do?

SECURITY BUILDING BLOCKS

AUTHORIZATION

This answers the question
"What can you do?"

For an already authenticated client -
What resources can she access?
What actions can she perform?

SECURITY BUILDING BLOCKS

AUTHORIZATION

This answers the question
"What can you do?"

For an already authenticated client
- What resources can she access?
What actions can she perform?

Can she edit this database?
Can she transfer money from account A to B?

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS
AUDITING

Did the user actually do that?

SECURITY BUILDING BLOCKS

AUDITING

This answers the question
"Did the user actually do
that?"

Auditing and logging is needed for non-repudiation - where a customer or a service cannot deny performing some action

SECURITY BUILDING BLOCKS

AUDITING

This answers the question "Did the user actually do that?"

Auditing and logging is needed for non-repudiation - where a customer or a service cannot deny performing some action

Did the user really pay for his book?
Did the user request 2 units of a mobile phone?

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS

CONFIDENTIALITY

Is the data safe?

SECURITY BUILDING BLOCKS

CONFIDENTIALITY

This answers the question
"Is the data safe?"

This refers to keeping data private such that unauthorized users cannot read or access it - whether this data is stored somewhere or in transit

SECURITY BUILDING BLOCKS

CONFIDENTIALITY

This answers the question "Is the data safe?"

This refers to keeping data private such that unauthorized users cannot read or access this data

Data is kept private using encryption or access control lists (ACLs)

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS

INTEGRITY

Can the data be modified?

SECURITY BUILDING BLOCKS

INTEGRITY

This answers the question
"Can the data be modified?"

This refers to whether data stored or in transit is safe from unauthorized changes either unintentional or malicious

SECURITY BUILDING BLOCKS

INTEGRITY

This answers the question "Can the data be modified?"

This refers to whether data stored or in transit is safe from unauthorized changes either unintentional or malicious

Integrity for stored data is via **permissions**, integrity for data in transit is achieved via **hashing** and message authentication codes

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS

AVAILABILITY

Does the system work for legitimate users?

SECURITY BUILDING BLOCKS

AVAILABILITY

This answers the question
"Does the system work for
legitimate users?"

Denying access to real users by overwhelming the system with requests or crashing the system is a security risk

SECURITY BUILDING BLOCKS

AVAILABILITY

This answers the question "Does the system work for legitimate users?"

Denying access to real users by overwhelming the system with requests or crashing the system is a security risk

Denial of service attacks are usually legitimate requests but in such volume that the system cannot handle it

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

INTEGRITY

AUDITING

AVAILABILITY

CONFIDENTIALITY

SECURITY BUILDING BLOCKS

AUTHENTICATION

AUTHORIZATION

AUDITING

INTEGRITY

CONFIDENTIALITY

AVAILABILITY

Security issues can undermine any of these basic foundations

RISK, THREAT, VULNERABILITY AND ATTACK

RISK, THREAT, VULNERABILITY AND ATTACK

A risk is the likelihood of being attacked and of the attack being successful - this refers to a system's exposure

RISK, THREAT, VULNERABILITY AND ATTACK

A risk is the likelihood of being attacked and of the attack being successful - this refers to a system's exposure

A threat is an occurrence which can harm your system, this can be malicious or unintentional

RISK, THREAT, VULNERABILITY AND ATTACK

A risk is the likelihood of being attacked and of the attack being successful - this refers to a system's exposure

A threat is an occurrence which can harm your system, this can be malicious or unintentional

A vulnerability is a weakness in the system which makes a threat possible - poor design, mistakes, insecure coding techniques

RISK, THREAT, VULNERABILITY AND ATTACK

A risk is the likelihood of being attacked and of the attack being successful - this refers to a system's exposure

A threat is an occurrence which can harm your system, this can be malicious or unintentional

A vulnerability is a weakness in the system which makes a threat possible - poor design, mistakes, insecure coding techniques

An attack is an action which enacts a threat to exploit a vulnerability

RISK, THREAT, VULNERABILITY AND ATTACK

A risk is the likelihood of being attacked and of the attack being successful - this refers to a system's exposure

A threat is an occurrence which can harm your system, this can be malicious or unintentional

A vulnerability is a weakness in the system which makes a threat possible - poor design, mistakes, insecure coding techniques

An attack is an action which enacts a threat to exploit a vulnerability

WHAT CAUSES SECURITY VULNERABILITIES?

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code

2. The size and complexity of your application

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code
2. The size and complexity of your application

3. Web servers are inherently complex and have their own weaknesses

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code
2. The size and complexity of your application
3. Web servers are inherently complex and have their own weaknesses

4. Database servers and other systems the site integrates with have their own issues

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code
2. The size and complexity of your application
3. Web servers are inherently complex and have their own weaknesses
4. Database servers and other systems the site integrates with have their own issues

5. Sites have increasing complex interactions with users, with special permissions

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code
2. The size and complexity of your application
3. Web servers are inherently complex and have their own weaknesses
4. Database servers and other systems the site integrates with have their own issues
5. Sites have increasing complex interactions with users, with special permissions

6. Code in your site comes from different programmers, coded at different times with different approaches

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code

2. The size and complexity of your application

3. Web servers are inherently complex and have their own weaknesses

4. Database servers and other systems the site integrates with have their own issues

5. Sites have increasing complex interactions with users, with special permissions

6. Code in your site comes from different programmers, coded at different times with different approaches

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code

2. The size and complexity of your application

3. Web server software is inherently complex and have their own weaknesses

4. Database software and other external components have their own issues

5. Sites have increasing complex interactions with users, with special permissions

6. Code in your site comes from different programmers, coded at different times with different approaches

This is not a complete list - components become old, don't get patched and updated

WHAT CAUSES SECURITY VULNERABILITIES?

1. Poorly written code

2. The size and complexity of your application

3. Web servers are inherently complex and have their own weaknesses

4. Databases and operating systems also have their own issues

5. Sites have increasing complex interactions with users, with special permissions

6. Code in your site comes from different programmers, coded at different times with different approaches

The surface area of a site that can be hacked only grows over time if it's unchecked!

KNOWN AND UNKNOWN VULNERABILITIES

KNOWN AND UNKNOWN VULNERABILITIES

Not all hackers are highly skilled!

The majority tend to be copycats

KNOWN AND UNKNOWN VULNERABILITIES

A few hackers have the skills and perhaps the luck to find new vulnerabilities to exploit

KNOWN AND UNKNOWN VULNERABILITIES

A few hackers have the skills and perhaps the luck to find **new** vulnerabilities to exploit

This takes intense time, effort and possibly the coordinated effort of a team

KNOWN AND UNKNOWN VULNERABILITIES

A few hackers have the skills and perhaps the luck to find new vulnerabilities to exploit

This takes intense time, effort and possibly the coordinated effort of a team

These exploits are UNKNOWN

KNOWN AND UNKNOWN VULNERABILITIES

The vast majority of attacks are of **KNOWN** vulnerabilities

KNOWN AND UNKNOWN VULNERABILITIES

The vast majority of attacks are of **KNOWN** vulnerabilities

These become famous once they are applied - and thousands of copycat hackers try to use this across other sites

KNOWN AND UNKNOWN VULNERABILITIES

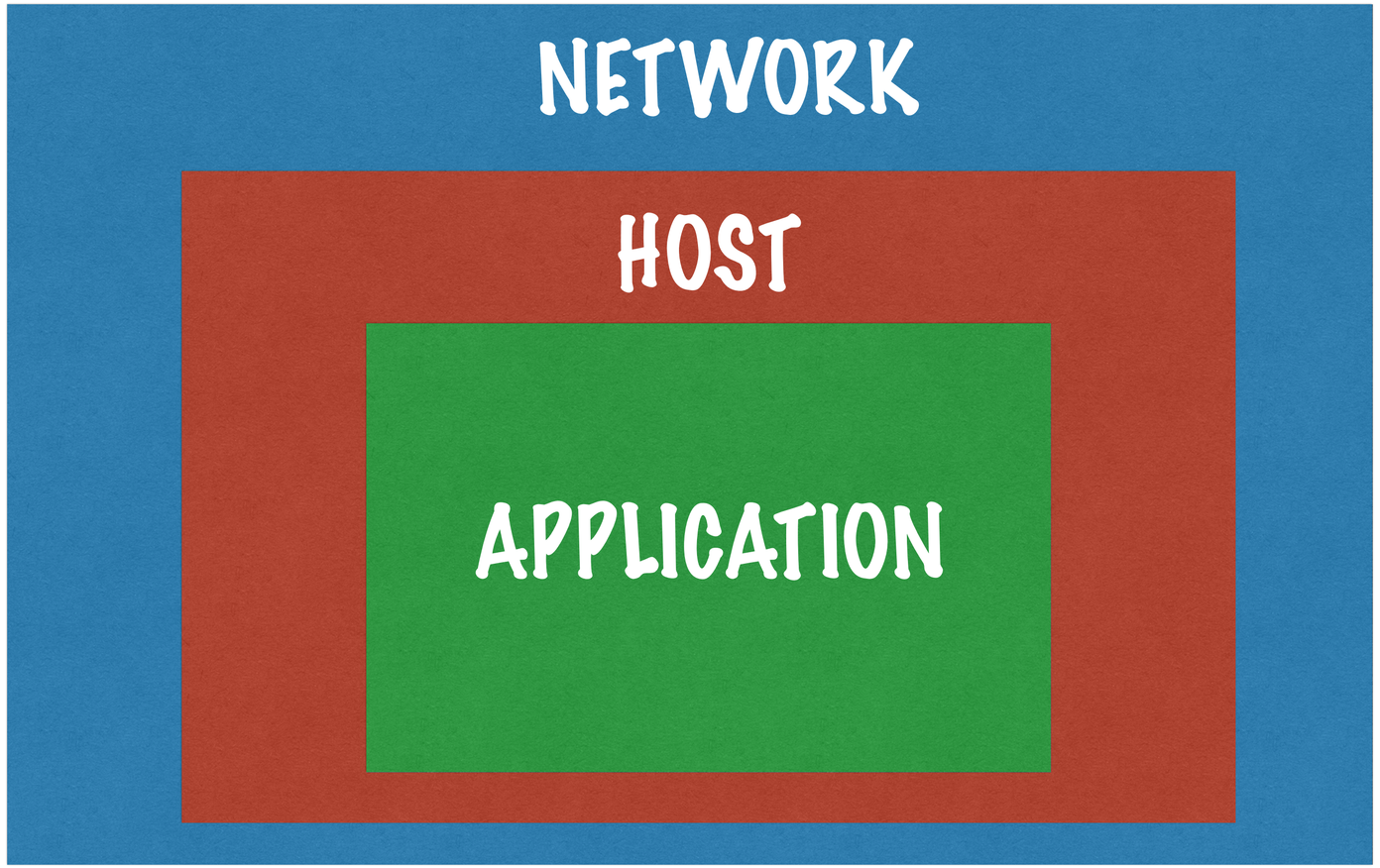
The vast majority of attacks are of **KNOWN** vulnerabilities

These become famous once they are applied - and thousands of copycat hackers try to use this across other sites

Your site is the most at risk from known exploits!

SO WHAT DO YOU SECURE?

SO WHAT DO YOU SECURE?



ALL OF THEM!

SO WHAT DO YOU SECURE?

In this class we'll mostly focus on application level security - the secure practices you follow when you write code in your website or application