CYBERSECURITY: ESSENTIALS

Daniel Medina — medina@nyu.edu

ADMINISTRATION

http://nyu.medina.io

Daniel Medina — medina@nyu.edu

Get an NYU Account: **http://start.nyu.edu**

ABOUT THE CLASS

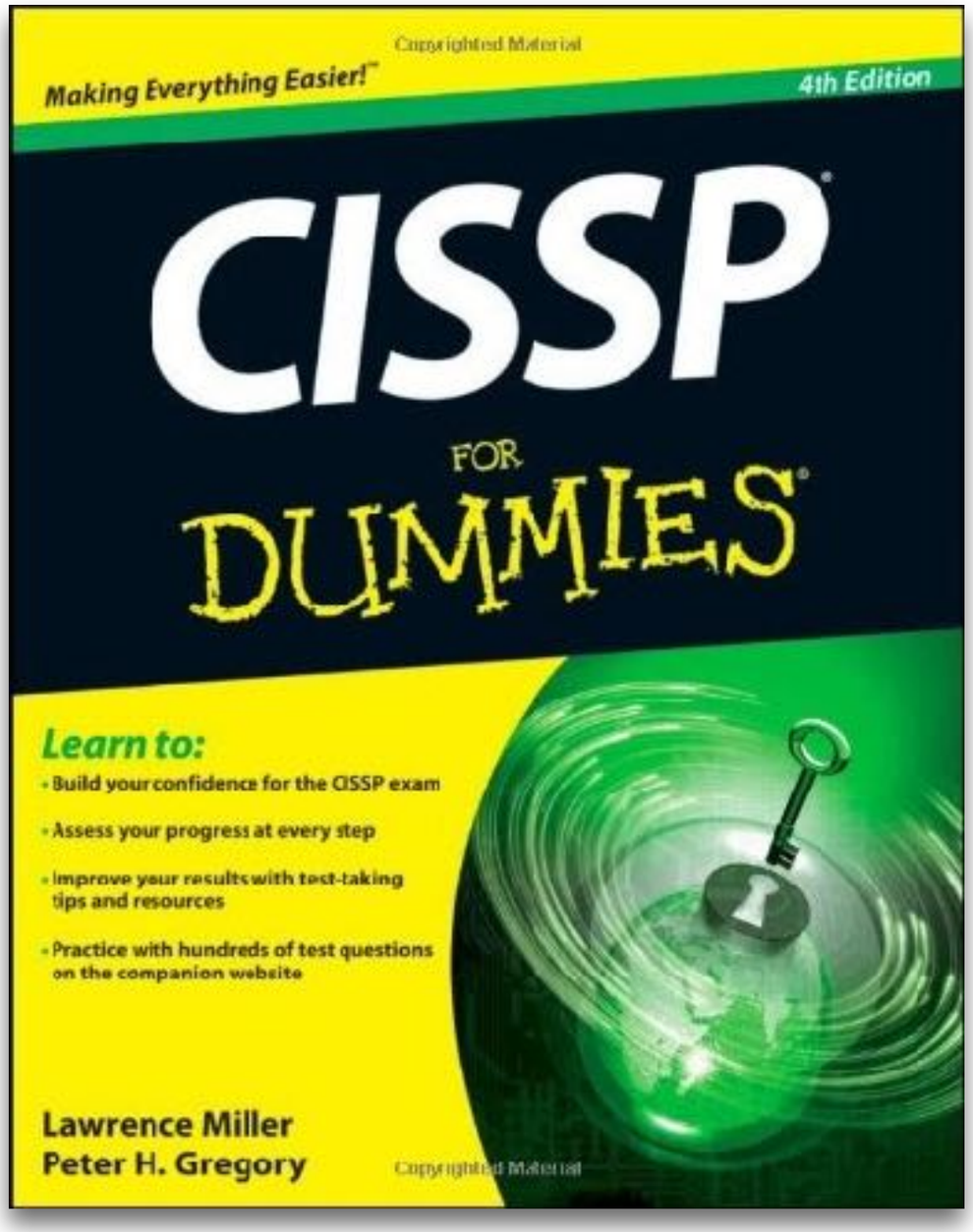
Syllabus available online

ABOUT THE CLASS

No required textbook

Many online readings

This one not bad for CISSP preparation >>>



ABOUT THE CLASS

Rough weekly topics:

- **Today**
- **Cryptography**
- **Access Controls**
- **Networks & Perimeters**
- **Application Security**
- **Audit & Incidents & Laws & Regulations**
- **Final Projects**

ABOUT ME

Daniel Medina

medina@nyu.edu

ABOUT ME

Background

Previously:

Systems Administrator, Network Developer,
Security Engineer in Academia & Wall Street
Security & TechOps Manager @ Tech Startup

Now:

Security Engineering Manager at global bank
Adjunct at NYU since 2007

ABOUT ME

Why am I here?

Taught while at university.
Wasn’t going to teach full-time.

Got “real job” at a bank
Missed university / academia

Adjunct at NYU since 2007
First class: *Perl Programming*

ABOUT THE CLASS

Why are we all here?

ABOUT YOU

Hi!

Name

Background

Why are you here?

INTERMISSION

[Intentionally Left Blank]

KrebsonSecurity
In-depth security news and investigation

18 Sources: Target Investigating Data Breach

DEC 13

Nationwide retail giant **Target** is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity. The sources said the breach appears to have begun on or around Black Friday 2013 — by far the busiest shopping day the year.

Update, Dec. 19: 8:20 a.m. ET: Target released a statement this morning confirming a breach, saying that 40 million credit and debit card accounts may have been impacted between Nov. 27 and Dec. 15, 2013.

Original story;

According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores.

Minneapolis, Minn. based **Target Brands Inc.** has not responded to multiple requests for comment. Representatives from **MasterCard** and **Visa** also could not be immediately reached for comment.

briankrebs
@briankrebs

Follow

RT @marcmaiffret: Target breach - Search of the word "security" on their leadership page returns 0 results. pressroom.target.com/leadership

Reply Retweet Favorite More

RETWEETS 13 FAVORITES 8

8:06 PM - 5 Feb 2014

Svieg @hugospns · 6h
@briankrebs @marcmaiffret I guess they want it to happen again so ... Not like the breach will have serious impact on them...
Details Reply Retweet Favorite More

The Zumarek @zumarek · 6h
.@briankrebs @marcmaiffret same with Careers ;)
Details Reply Retweet Favorite More

snorkel @snorkel42 · 6h
@briankrebs too lazy to check myself but do "any" major retailers have a security person on their exec page?
Details Reply Retweet Favorite More

SecFUD Busters @SecFUDBusters · 6h
@briankrebs @marcmaiffret – why on earth would a retailer need security? ;-)
Details Reply Retweet Favorite More

briankrebs
@briankrebs

Follow

Appropos of a previous tweet tonight, Target says its CISO is Brenda Bjerke ow.ly/tkzXl

Reply Retweet Favorite More

RETWEETS 2 FAVORITES 4

8:07 PM - 5 Feb 2014

Chris @obscuresec · 4h
@briankrebs I guess we know why @BrendaBjerke has been too busy for twitter.
Details Reply Retweet Favorite More

Adam H @AM7601 · 4h
@briankrebs and the CIO's bio looks like appointment made with 'previous tech experience optional'.
Details Reply Retweet Favorite More

The Zumarek @zumarek · 4h
@briankrebs Director has only broken stick and rotten carrot. In 2 years CIO/CISO will report directly to the board - this will fix a lot.
Details Reply Retweet Favorite More

John Bumgarner @JohnBumgarner · 3h
@briankrebs - At least @BrendaBjerke is one of your followers and retweeters.
Details Reply Retweet Favorite More

Dear Target Guests,

As you have probably heard, Target learned in mid-December that criminals forced their way into our systems, gaining access to guest credit and debit card information. As a part of the ongoing forensic investigation, it was determined last week that certain guest information, including names, mailing addresses, phone numbers or email addresses, was also taken.

Our top priority is taking care of you and helping you feel confident about shopping at Target, and it is our responsibility to protect your information when you shop with us.

We didn't live up to that responsibility, and I am truly sorry.

Please know we moved as swiftly as we could to address the problem once it became known, and that we are actively taking steps to respond to your concerns and guard against something like this happening again. Specifically, we have:

1. Closed the access point that the criminals used and removed the malware they left behind.
2. Hired a team of data security experts to investigate how this happened. That effort is ongoing and we are working closely with law enforcement.
3. Communicated that our guests will have zero liability for any fraudulent charges arising from the breach.
4. Offered one year of free credit monitoring and identity theft protection to all Target guests so you can have peace of mind.

In the days ahead, Target will announce a coalition to help educate the public on the dangers of consumer scams. We will also accelerate the conversation–among customers, retailers, the financial community, regulators and others–on adopting newer, more secure technologies that protect consumers.

I know this breach has had a real impact on you, creating a great deal of confusion and frustration. I share those feelings. You expect more from us and deserve better.

We want to earn back your trust and confidence and ensure that we deliver the Target experience you know and love.

We are determined to make things right, and we will.

Sincerely,

Gregg Steinhafel

Gregg Steinhafel, chairman, president and chief executive officer, Target

"I AM TRULY SORRY"

"WE HAVE HIRED... SECURITY EXPERTS"

Target CIO resigns following breach

Grant Gross, IDG News - Mar 5, 2014

Target CIO Beth Jacob has resigned following a data breach at the retailer that may have affected as many as 110 million U.S. residents.

Target is overhauling its information security practices, Gregg Steinhafel, the company's chairman, president and CEO, said in a statement. Target is searching for an interim CIO to help guide the company "through this transformation," he said.

In addition, **Target is elevating its CISO role and hiring for that position and for a chief compliance offer**, he added. The company has hired Promontory Financial Group "to help us evaluate our technology, structure, processes and talent as a part of this transformation," he said.

Target CEO steps down after massive data breach

By Associated Press

May 5, 2014 | 8:29am

Target CEO Gregg Steinhafel is stepping down five months after the company was hit by a massive cyber-attack.

Target CEO Gregg Steinhafel Resigns

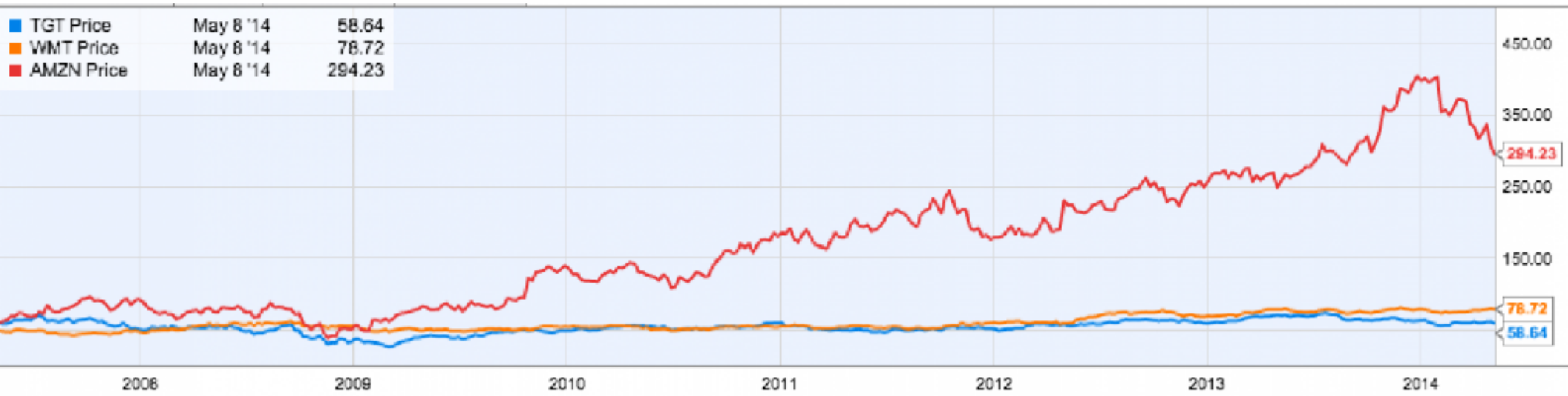
Clare O'Connor, Forbes - May 5, 2014

Target's CEO is the latest casualty of the widespread data breach that saw hackers steal personal data and credit card information from millions of customers.

On Monday, the Minneapolis-based retail chain announced that **35-year company veteran Gregg Steinhafel had stepped down effective immediately.**

Target's statement referred to Steinhafel's handling of the disastrous data breach that unfolded in December.

"He held himself personally accountable and pledged that Target would emerge a better company," said the statement. "We are grateful to him for his tireless leadership and will always consider him a member of the Target family."



WAPO: *TARGET'S CEO DIDN'T LEAVE BECAUSE OF… BREACH*

http://www.washingtonpost.com/news/wonkblog/wp/2014/05/08/targets-ceo-didnt-leave-because-of-a-cybersecurity-breach/

Target Names Brad Maiorino Senior Vice President, Chief Information Security Officer

MINNEAPOLIS — June 10, 2014

Today, Target Corp. (NYSE: TGT) announced it
Hired Brad Maiorino as senior vice president, ch
information security officer.

Maiorino joins Target effective June 16 and will
responsible for Target's information security an
technology risk strategy helping to ensure that t
company, its guests and team members are
protected from internal and external informati
security threats. He will report to Bob DeRodo
executive vice president and chief information
officer.

Maiorino comes to Target from General Motor
where he was the company's chief informatio
security and information technology risk office

BITS | Brad Maiorino, Target's New Cybersecurity Boss, Discusses Being a 'Glutton for Punishment'

Q. *The breach taught us that large companies are no longer confined, single entities that can hide behind a single firewall but sprawling networks of interconnected vendors. How do you even begin to defend that?*

A. Target already had a robust vendor security program and that is definitely a priority for me. But one of the principles I apply to information security isn't security-related at all. It's about simplification and consolidation. My geeky term for it is 'attack surface reduction.'

When you look at a multinational company, it makes DNA look simple. You don't need military-grade defense capabilities to figure out that you have too many connections. You have to simplify and consolidate those as much as possible and have adequate measures to detect and respond when those controls do fail.

http://bits.blogs.nytimes.com/2014/07/31/brad-maiorino-targets-new-cybersecurity-boss-discusses-being-a-glutton-for-punishment/

INTERMISSION

[Intentionally Left Blank]

YAHOO!®

An Important Message About Yahoo User Security

SEPTEMBER 2016

HTTPS://YAHOO-SECURITY.TUMBLR.COM/POST/150782028915

By Bob Lord, CISO

We have confirmed that a copy of certain user account information was stolen from the company's network in late 2014 in what we believe is a state-sponsored actor. The account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in some cases, encrypted or unencrypted security questions and answers. The ongoing investigation suggests that stolen information did not include unprotected passwords, payment card data, or bank account information; payment card data and bank account information are not stored in the system that the investigation has found to be affected. Based on the ongoing investigation, Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network. Yahoo is working closely with law enforcement on this matter.

We are taking action to protect our users:

"HASHED PASSWORDS (USING BCRYPT)"

- We are notifying potentially affected users. The content of the email Yahoo is sending to those users will be available at https://yahoo.com/security-notice-content beginning at 11:30 am (PDT).
- We are asking potentially affected users to promptly change their passwords and adopt alternate means of account verification.
- We invalidated unencrypted security questions and answers so they cannot be used to access an account.
- We are recommending that all users who haven't changed their passwords since 2014 do so.
- We continue to enhance our systems that detect and prevent unauthorized access to user accounts.
- We are working closely with law enforcement on this matter.

2+ YEAR OLD INTRUSION

"STATE-SPONSORED ACTOR"

OCTOBER 2016
HTTP://WWW.REUTERS.COM/ARTICLE/US-YAHOO-NSA-EXCLUSIVE-IDUSKCN1241YT

Some surveillance experts said this represents the first case to surface of a U.S. Internet company agreeing to an intelligence agency's request by searching all arriving messages, as opposed to examining stored messages or scanning a small number of accounts in real time.

It is not known what information intelligence officials were looking for, only that they wanted Yahoo to search for a set of characters. That could mean a phrase in an email or an attachment, said the sources, who did not want to be identified.

Reuters was unable to determine what data Yahoo may have handed over, if any, and if intelligence officials had approached other email providers besides Yahoo with this kind of request.

According to two of the former employees, Yahoo Chief Executive Marissa Mayer's decision to obey the directive roiled some senior executives and led to the June 2015 departure of Chief Information Security Officer Alex Stamos, who now holds the top security job at Facebook Inc.

IN 2015, STAMOS "RESIGNED AS CISO"

Important Security Information for Yahoo Users

DECEMBER 2016

HTTPS://YAHOO.TUMBLR.COM/POST/154479236569

By Bob Lord, CISO

Following a recent investigation, we've identified data security issues concerning certain Yahoo user accounts. We've taken steps to secure those user accounts and we're working closely with law enforcement.

What happened?

As we previously disclosed in November, law enforcement provided us with data files that a third party claimed was Yahoo user data. We analyzed this data with the assistance of outside forensic experts and found that it appears to be Yahoo user data. Based on further analysis of this data by the forensic experts, we believe an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts. We have not been able to identify the intrusion associated with this theft. We believe this incident is likely distinct from the incident we disclosed on September 22, 2016.

2+ YEAR OLD INTRUSION

For potentially affected accounts, the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected.

"HASHED PASSWORDS (USING MD5)"

Separately, we previously disclosed that our outside forensic experts were investigating the creation of forged cookies that could allow an intruder to access users' accounts without a password. Based on the ongoing investigation, we believe an unauthorized third party accessed our proprietary code to learn how to forge cookies. The outside forensic experts have identified user accounts for which they believe forged cookies were taken or used. We are notifying the affected account holders, and have invalidated the forged cookies. We have connected some of this activity to the same state-sponsored actor believed to be responsible for the data theft the company disclosed on September 22, 2016.

"FORGED COOKIES ALLOW ACCESS WITHOUT A PASSWORD"

"STATE-SPONSORED ACTOR"

INTEL | Thu Dec 15, 2016 | 12:11pm EST

Yahoo shares fall on worries new breach will kill Verizon deal

By **Greg Roumeliotis** and **Dustin Volz**

Yahoo Inc shares fell almost 5 percent on Thursday after the technology company disclosed a second massive data breach that raised fears Verizon might kill a deal to buy its core internet business.

Silicon Valley-based Yahoo said late on Wednesday that it had uncovered a 2013 cyber attack that compromised data of more than 1 billion user accounts, the largest breach in history.

That followed Yahoo's disclosure in September of a separate breach that affected over 500 million accounts, which the company said it believed was launched by different hackers.

Yahoo shares were down 4.8 percent at $38.93 in midday trade as the latest revelation cast new doubt on whether Verizon Communications Inc would proceed with a $4.83 billion agreement to buy Yahoo's core internet business, struck in July.

Verizon is now seeking to persuade Yahoo to amend the terms of the acquisition agreement to reflect the economic impact of the data breaches, according to people familiar with the matter.

DECEMBER 2016

HTTP://WWW.REUTERS.COM/ARTICLE/YAHOO-CYBER-IDUSL1N1EA1CI

http://www.investors.com/news/technology/yahoo-verizon-deal-closing-delayed-until-q2/

Yahoo (YHOO) late Monday reported Q4 earnings and revenue that topped Wall Street views, but it said the closing of its acquisition by **Verizon Communications** (VZ) would be delayed into the second quarter.

Yahoo reportedly faces an investigation by the U.S. Securities and Exchange Commission relating to two massive email breaches that the company disclosed last year, though they occurred in 2013 and 2014.

Verizon in July reached an agreement to buy the core Yahoo Web portal business for $4.83 billion. Verizon also assumed $1.1 billion in employee stock costs, bringing the total cost closer to $6 billion, though reportedly Verizon is looking to lower the price because of the breaches.

INTERMISSION

[Intentionally Left Blank]

SOME CONCEPTS

(Stuff that might be on the CISSP exam)

C I A

Confidentiality

Integrity

Availablility

RISK ASSESSMENT

What are we protecting?

What are the threats?

What costs would we bear?

ADVERSARY MODEL

careless user
bored hacker
criminal gang
hacktivist collective
disgruntled employee
industrial competitor
government agency

ADVERSARY MODEL

How might this adversary act?

ADVERSARY MODEL

What's easy to measure

vs

What's easy to test

vs

What would an adversary do to compromise a target?

ADVERSARY MODEL

APT

ADVERSARY MODEL

Advanced

Persistent

Threat

ADVERSARY MODEL

"We need that first crack and we'll look and look to find it. There's a reason it's called an **advanced persistent threat**; we'll poke and poke and wait and wait until we get in." — Rob Joyce

ADVERSARY MODEL

"We need that first crack and we'll look and look to find it. There's a reason it's called an **advanced persistent threat**; we'll poke and poke and wait and wait until we get in." — Rob Joyce, chief of Tailored Access Operations for the US National Security Agency

https://www.youtube.com/watch?v=bDJb8WOJYdA

I+AAA

Identification

Authentication

Authorization

Accounting

SOME REAL EXAMPLES

SOME REAL EXAMPLES

SOME REAL EXAMPLES

SOME REAL EXAMPLES

CITIBANK HACK BLAMED FOR ALLEGED ATM CRIME SPREE
HTTPS://WWW.WIRED.COM/2008/06/CITIBANK-ATM-SE/

SOME REAL EXAMPLES

SOME REAL EXAMPLES

SOME REAL EXAMPLES

SOME REAL EXAMPLES

SOME REAL EXAMPLES

WE’RE OUT OF SLIDES!

[Intentionally Left Blank]