

An Introduction to Cybersecurity

CS 1000 - Explorations in Computing

Nov 26, 2018

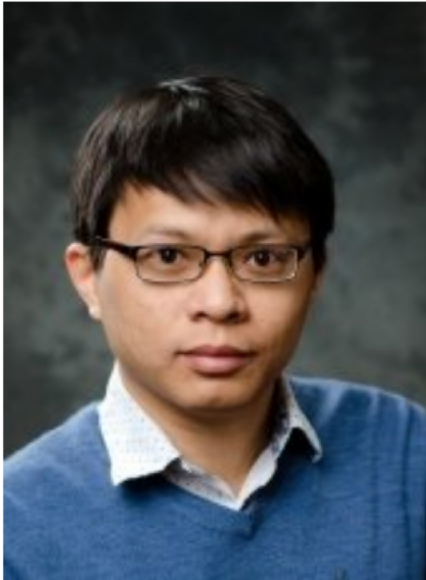
Bo Chen

bchen@mtu.edu

<https://cs.mtu.edu/~bchen>

<https://snp.cs.mtu.edu>

About Me



Bo Chen

Assistant Professor, Computer Science

906-487-3149

bchen@mtu.edu

Rekhi 301

Links of Interest

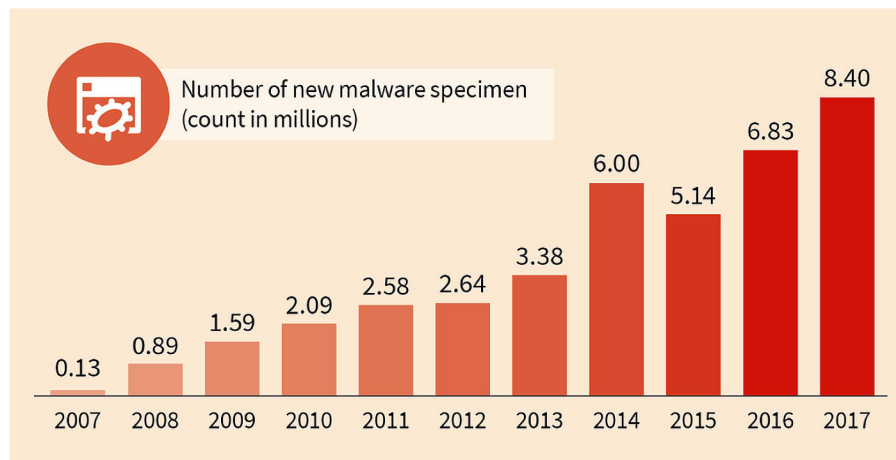
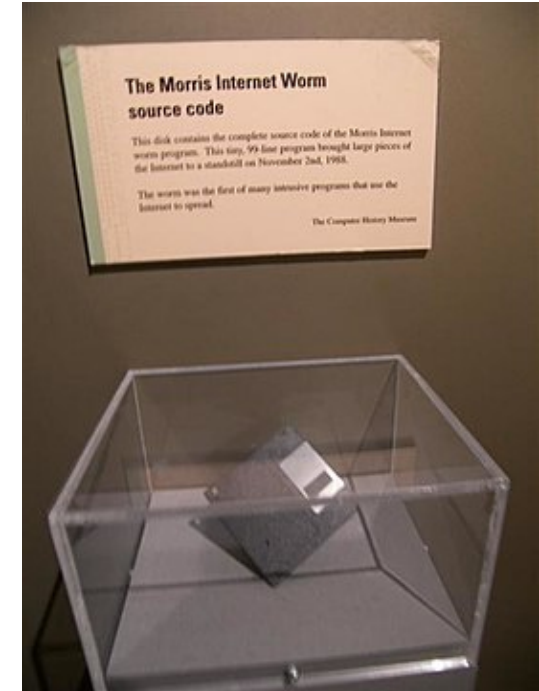
[Faculty Website](#)

Areas of Expertise

- Mobile Device Security
- Cloud Computing Security
- Named Data Networking Security
- Big Data Security
- Blockchain

All Starts from Malware and Hacks

- On November 2, 1988, a graduate student at Cornell University, Robert Morris, unleashed what became known as the Morris worm
 - Morris worm disrupted a large number of computers then on the Internet, guessed at the time to be **one tenth** of all those connected
- Malware and Hacks are here and there today



How to Combat Malware and Hacks?

- The answer is cybersecurity
- Make sure our systems and networks are protected
 - Any intruders can be detected, identified, and blocked
- Make sure the software we build is free of vulnerabilities
 - The attackers cannot exploit the vulnerabilities to intrude into our systems and networks
- Make sure our data are protected
 - Not disclosed to unauthorized parties
 - Not modified by unauthorized parties
 - Always available for use
 - Always recoverable

Outline

- Recent cybersecurity instances
- What is cybersecurity
- Why learning cybersecurity
- How to learn cybersecurity in MTU

Recent Cybersecurity Instances

2018 Data Breaches and Hacks

Facebook - Cambridge Analytica data scandal: 87 million user profiles were disclosed

- Various political organizations used information from Cambridge Analytica to attempt to influence public opinion:
 - 2015 and 2016 campaigns of United States politicians Donald Trump and Ted Cruz
 - 2016 Brexit (British exit from the European Union) vote
 - 2018 Mexican general election, 2018 for Institutional Revolutionary Party
- Successors: a company run by former officials at Cambridge Analytica, Data Propria, has been quietly working for President Donald Trump's 2020 re-election effort

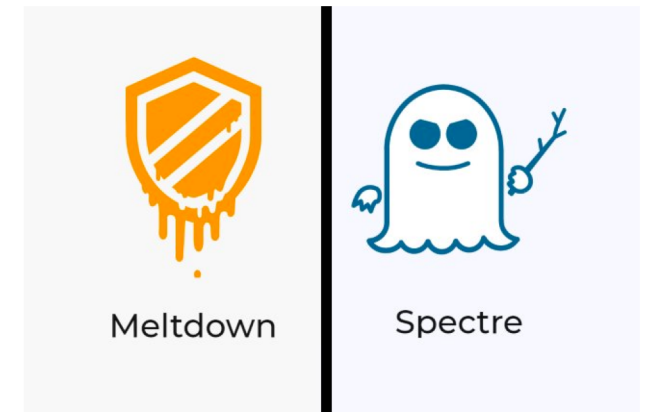


2018 Data Breaches and Hacks (cont.)

*Under Armour: a data breach of **150 million** accounts, with compromised data consisting of user names, the users' e-mail addresses and hashed passwords*



*Intel x86 microprocessors hardware vulnerabilities
Meltdown and Spectre*



More Data Breaches in 2018

- Saks Fifth Avenue / Lord & Taylor, 5 million credit card holders compromised
- British Airways, a data theft of about 380,000 customer records
- US Centres for Medicare & Medicaid Services (CMS), a data breach that exposed files of 75,000 individuals
- SingHealth, 1.5 million personal data compromised
- ...

2017 Data Breach and Hacks

Paradise Papers: 13.4 million confidential electronic documents relating to offshore investments that were leaked

- **1.4TB** in size, contains the names of more than 120,000 people and companies
- People: Prince Charles and Queen Elizabeth II, President of Colombia Juan Manuel Santos, and U.S. Secretary of Commerce Wilbur Ross, etc
- Companies: Facebook, Twitter, Apple, Disney, Uber, Nike, Walmart, Allianz, Siemens, McDonald's, and Yahoo! own offshore companies
 - Apple, Nike, and Facebook avoided billions of dollars in tax using offshore companies
- Panama papers in 2016



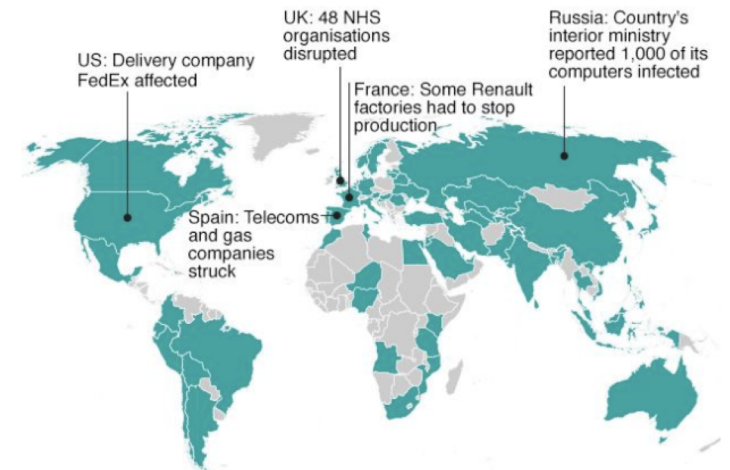
2017 Data Breach and Hacks (cont.)

WannaCry Ransomware Attacks

- Encrypt data in a victim computer, and demand a payment of around **\$300 USD in bitcoin** within three days, or **\$600 USD** within seven days
- A total of 327 payments totaling \$130,634.77 USD (51.62396539 XBT) had been transferred after the attack had subsided
- Estimated to have affected more than **200,000** computers across **150** countries, with total damages ranging from hundreds of millions to billions of dollars



Countries hit in initial hours of cyber-attack



*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Norway, where incidents have been reported since

2017 Data Breach and Hacks (cont.)

Equifax: 145,500,000 consumer records were leaked, the largest known data breach in history at the time

- In October 2017, the cities of Chicago and San Francisco and the Commonwealth of Massachusetts have filed enforcement actions against Equifax



support through [social engineering](#), and the password recovery system of Apple which used this information.^[41] Related to his experience, Mat Honan wrote a piece outlining why passwords cannot keep users safe.^[42]

- In October 2012, a law enforcement agency contacted the South Carolina Department of Revenue (DoR) with evidence that Personally Identifiable Information (PII) of three individuals had been stolen.^[43] It was later reported that an estimated 3.6 million Social Security numbers were compromised along with 387,000 credit card records.^[44]

2013 [edit]

- In October 2013, [Adobe Systems](#) revealed that their corporate database was hacked and some 130 million user records were stolen. According to Adobe, "For more than a year, Adobe's authentication system has cryptographically hashed customer passwords using the [SHA-256](#) algorithm, including salting the passwords and iterating the hash more than 1,000 times. This system was not the subject of the attack we publicly disclosed on October 3, 2013. The authentication system involved in the attack was a backup system and was designated to be decommissioned. The system involved in the attack used [Triple DES](#) encryption to protect all password information stored."^[45]

Further information: [Adobe Systems § Source code and customer data breach](#)

- In late November to early December 2013, [Target Corporation](#) announced that data from around 70 million [credit](#) and [debit](#) cards was stolen. It is the second largest credit and debit card breach after the [TJX Companies data breach](#) where almost 46 million cards were affected.^[46]
- In 2013, [Edward Snowden](#) published a series of [secret documents](#) that revealed widespread spying by the United States [National Security Agency](#) and similar agencies in other countries.

2014 [edit]

- In August 2014, nearly 200 [photographs of celebrities](#) were posted to the image board website [4chan](#). An investigation by [Apple](#) found that the images were obtained "by a very targeted attack on user names, passwords and security questions".^[47]
- In September 2014, [Home Depot](#) suffered a data breach of 56 million credit card numbers.^[48]
- In October 2014, [Staples](#) suffered a data breach of 1.16 million customer payment cards.^[49]
- In November 2014 and for weeks after, [Sony Pictures Entertainment](#) suffered a data breach involving personal information about Sony Pictures employees and their families, e-mails between employees, information about executive salaries at the company, copies of (previously) unreleased Sony films, and other information. The hackers involved claim to have taken over 100 terabytes of data from Sony.^[50]

2015 [edit]

- In October 2015, the British telecommunications provider [TalkTalk](#) suffered a data breach when a group of 15-year-old hackers stole information on its 4 million customers. The stock price of the company fell substantially due to the issue – around 12% – owing largely to the bad publicity surrounding the leak.^[51]
- In July 2015, adult website [Ashley Madison](#) suffered a data breach when a hacker group stole information on its 37 million users. The hackers threatened to reveal usernames and specifics if Ashley Madison and a fellow site, [EstablishedMen.com](#), did not shut down permanently.^[52]
- In February 2015, [Anthem](#) suffered a data breach of nearly 80 million records, including personal information such as names, Social Security numbers, dates of birth, and other sensitive details.^[53]
- In June 2015, The [Office of Personnel Management](#) of the U.S. government suffered a data breach in which the records of 22.1 million current and former federal employees of the United States were hacked and stolen.^[54]

2016 [edit]

- In March 2016, the website of the [Commission on Elections](#) in the Philippines was [defaced](#) by hacktivist group, "[Anonymous Philippines](#)". A larger problem arose when a group called [LulzSec Pilipinas](#) uploaded COMELEC's entire database on Facebook the following day.^[55]
- In April 2016, news media carried information stolen from a successful network attack of the Central American law firm, [Mossack Fonseca](#), and the resulting "[Panama Papers](#)" sent reverberations throughout the world.^[56] Perhaps a justified vindication of illegal or unethical activity, this nonetheless illustrates the impact of secrets coming to light. The Prime Minister of Iceland was forced to resign^[57] and a major reshuffling of political offices occurred in countries as far-flung as Malta.^[58] Multiple investigations were immediately initiated in countries around the world, including a hard look at [international](#) or offshore banking rules in the U.S.^[59] Obviously the implications are enormous to the ability of an organization—whether a law firm or a governmental department—to keep secrets.^[60]
- In September 2016 [Yahoo](#) reported that up to 500 million accounts in 2014 [had been breached](#) in an apparent "state-sponsored" data breach. It was later reported in October 2017 that 3 billion accounts had been breached, accounting for every Yahoo account at the time.

2017 [edit]

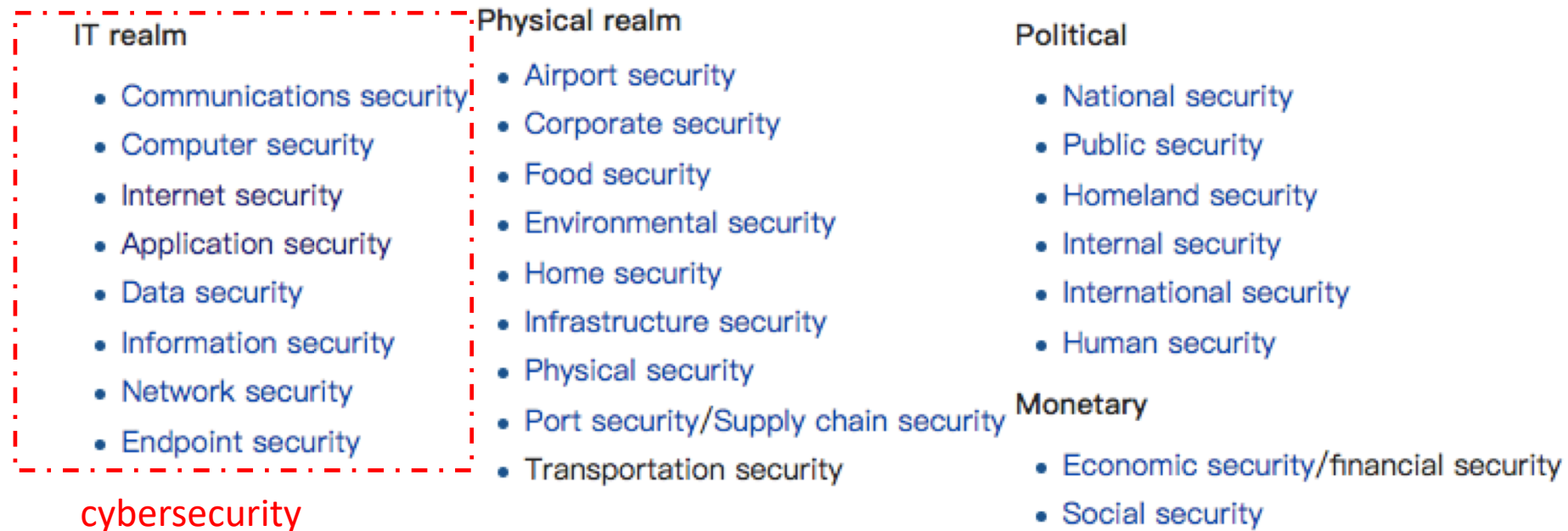
- [Vault 7](#), CIA's hacking techniques revealed in data breach.^[61]

What is Cybersecurity?

Security 101

The Definition of Security

- Security: **freedom from, or resilience against, potential harm** (or other unwanted coercive change) from external forces (*wikipedia*)
- Cybersecurity: **the protection of computer systems** from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide



Cybersecurity Objectives: CIA

Main security objectives:

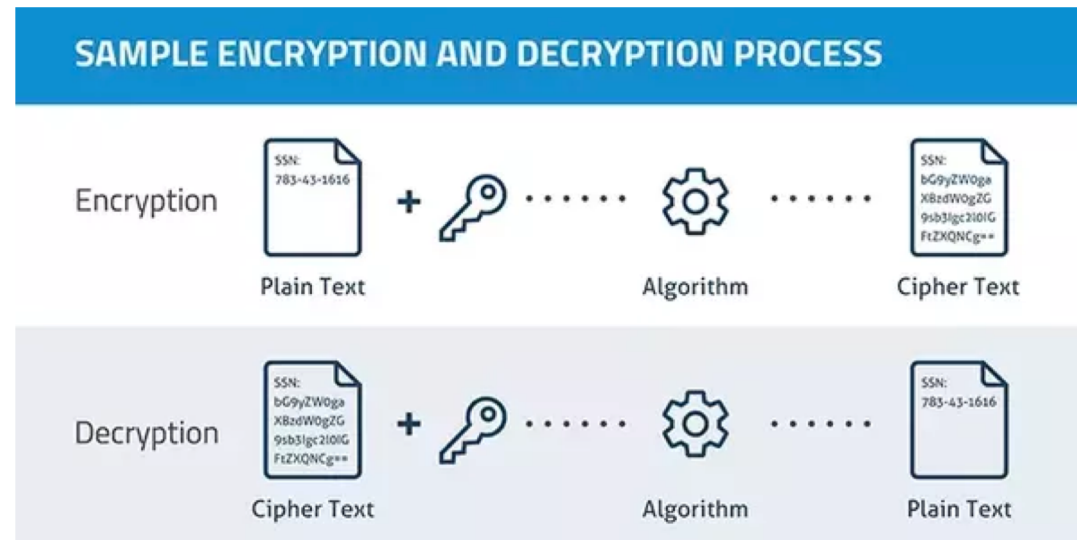
- **Confidentiality:** unauthorized users **cannot read** information
- **Integrity:** unauthorized users **cannot alter** information
- **Availability:** authorized users can **always access** information

Other security objectives:

- Authentication and identification
- Access control
- Non-repudiation: users cannot deny actions
- Privacy
- Anonymity
- ...

Confidentiality

- *The concealment of information or resources*
 - Information is not made available or disclosed to unauthorized individuals, entities, or processes
 - E.g., your bank accounts, private photos, etc
- How to achieve confidentiality? Encrypt the data using a secret key, and only the authorized entities can obtain the secret key to decrypt the data
 - AES
 - DES, 3DES



Integrity

- Maintaining and assuring the accuracy and completeness of data over its entire lifecycle
 - Data cannot be modified in an unauthorized or undetected manner
 - E.g., your emails, your electronic homework



Do to Ensure Integrity?

- Generate digest and perform integrity checking

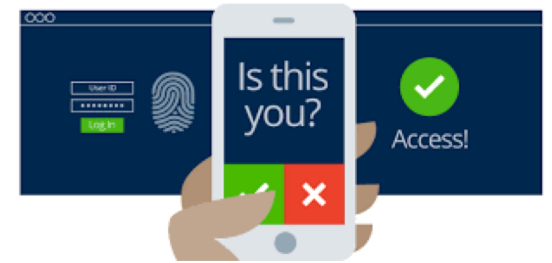


Availability

- For any information system to serve its purpose, the **service/ information** must be available when it is needed
 - This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly
- High availability systems aim to remain available at all times
 - Preventing service disruptions due to power outages, hardware failures, and system upgrades
 - Preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down

Authentication

- Authentication in physical world: are you **really** who you claim?
 - Confirm the identity of a person by validating his/her identity document (e.g., driver license, passport, student ID card)
- Authentication in computers:
 - Confirm whether a person is the owner of a smartphone
 - Confirm whether a person is a user of online banking
 - Confirm whether a website is authentic

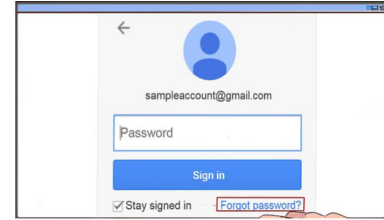


How to Do Authentication?

- Four general means for authenticating user's identity

- Something the individual knows

- Passwords



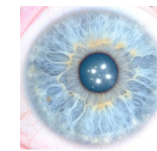
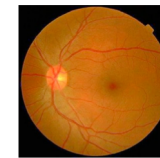
- Something the individual possesses, a *token*

- Memory card, smart card



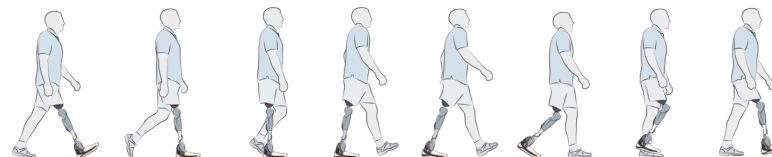
- Something the individual is

- Fingerprint, iris, retina, face



- Something the individual does (behavior pattern)

- Typing rhythm, gait, and voice



How to Do Authentication (cont.)?

- Multi-factor authentication (MFA)



Access Control

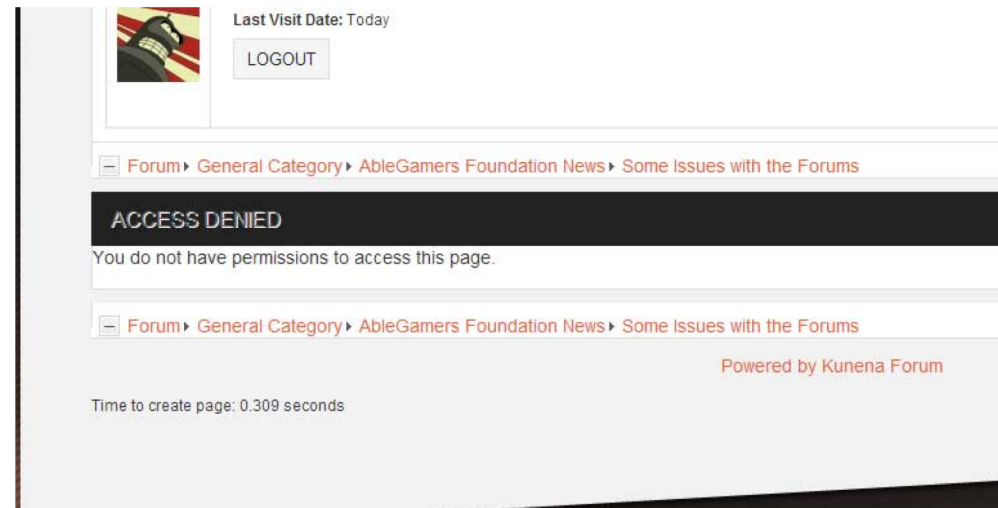
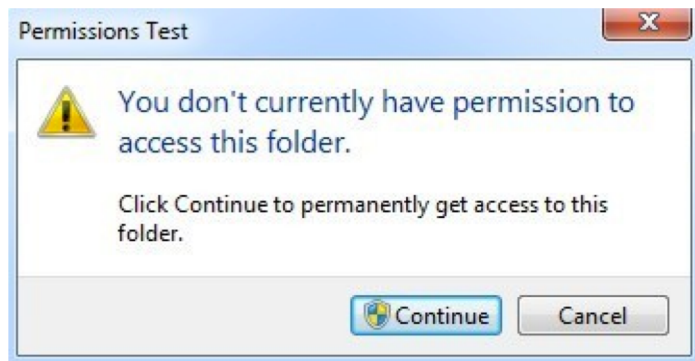
- Access control in physical world: the selective restriction of access to a place. It is a matter of **who**, **where**, and **when**.
 - Historically, this was partially accomplished through mechanical keys and locks



- Access control in computers: the selective restriction of access to computing resources (**who**, **what**, and **how**)
 - Who: users, programs, processes, etc.
 - What: computing resources like files, memory, I/O ports, etc.
 - How: how the computing resources can be “touched”

How to Do Access Control?

- Encrypting the protected computing resources using secret keys, and only disclose keys to those who are authorized
- The access control is enforced by systems (operating systems, database management systems, etc.) following permissions




```
osmc@osmc:~$ ls -al
total 37
drwxr-xr-x 7 osmc osmc 4096 Jul  4 03:11 .
drwxr-xr-x 3 root root 4096 Jan  1 1970 ..
-rw----- 1 osmc osmc  73 Jul  3 00:10 .bash_history
-rw-r--r-- 1 osmc osmc  220 Oct 18  2014 .bash_logout
-rw-r--r-- 1 osmc osmc 3515 Oct 18  2014 .bashrc
drwxr-xr-x 8 osmc osmc 4096 Jan  1 1970 .kodi
-rw-r--r-- 1 osmc osmc  675 Oct 18  2014 .profile
drwxr-xr-x 2 root root   0 Jan  1 1970 Movies
drwxrwxrwx 2 osmc osmc  64 Jul  4 00:49 Music
drwxr-xr-x 2 osmc osmc 4096 Apr 12 10:30 Pictures
drwxr-xr-x 2 osmc osmc 4096 Apr 12 10:30 TV Shows
osmc@osmc:~$ cd Music
-bash: cd: Music: Permission denied
osmc@osmc:~$
```

Why Learning Cybersecurity?

Great Job Market

- There will be **3.5 million** unfilled cybersecurity positions by 2021
 - According to Cybersecurity Jobs Report, sponsored by Herjavec Group
- The rate of growth for jobs in information security is projected at **37%** from 2012 to 2022
 - According to the Bureau of Labor Statistics
 - Much faster than the average for all other occupations

 Secure | <https://www.wsj.com/articles/its-a-good-time-to-find-a-cybersecurity-job-1527646081>

THE WALL STREET JOURNAL.

[Home](#) [World](#) [U.S.](#) [Politics](#) [Economy](#) [Business](#) [Tech](#) [Markets](#) [Opinion](#) [Life & Arts](#) [Real Estate](#) [WSJ. Magazine](#)

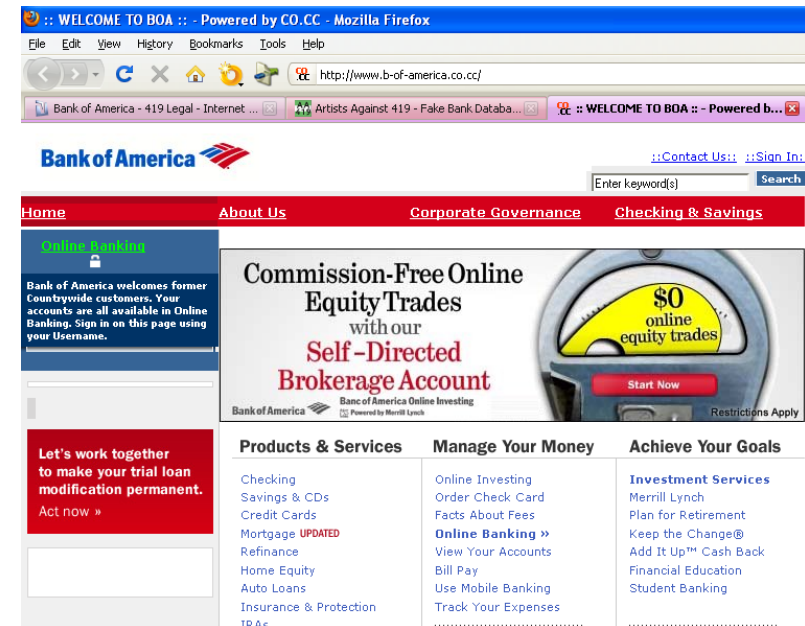
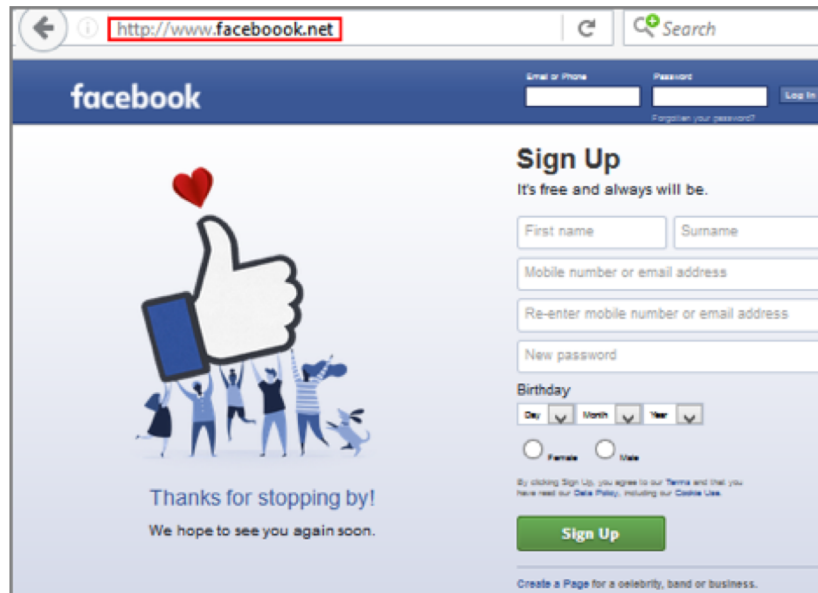
[BUSINESS](#) | [LEADERSHIP](#)

It's a Good Time to Find a Cybersecurity Job

There is a big gap between demand and supply. No degree required.

Protect Your Own Asset

- Reduce the possibility of exposure to potential hacks
 - Malicious code is here and there (malicious java scripts, applets, etc)
 - Make sure you trust the web sites before you go there
 - www.google.com is fine, but **www.go0gle.com** may not
 - Do you want to click the link **www.facebook.net**, or **www.b-of-America.co.cc**



Protect Your Own Asset (cont.)

- Reduce the possibility of exposure to potential hacks
- Be careful of phishing emails

From: Bank of America <crvdgi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients:;
Reply-To: crvdgi@comcast.net



Online Banking Alert

Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.

Please sign in to your account at <https://www.bankofamerica.com> to review and verify your account activity. After verifying your debit card transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.

© 2014 Bank of America Corporation. All rights reserved.

amazon Refund Notification

Due to a system error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

[Click Here to Update Your Address](#)

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
[Amazon.com](#)
Email ID: [REDACTED]

File Message

From: LinkedIn Accounts
To: Amy B; Bryan; Dennis B; Gary; Jim C; Geff H; Louise K; Patty; Ihor M; Ted N; Chris P;
Subject: Account suspended!

LinkedIn

Your LinkedIn account was suspended due to spam messages. To unlock your account open this link www.linkedin.nl/a

Thank you for using LinkedIn!

The LinkedIn Team

Security Technology Is Money Sometimes

Bitcoin price

De11

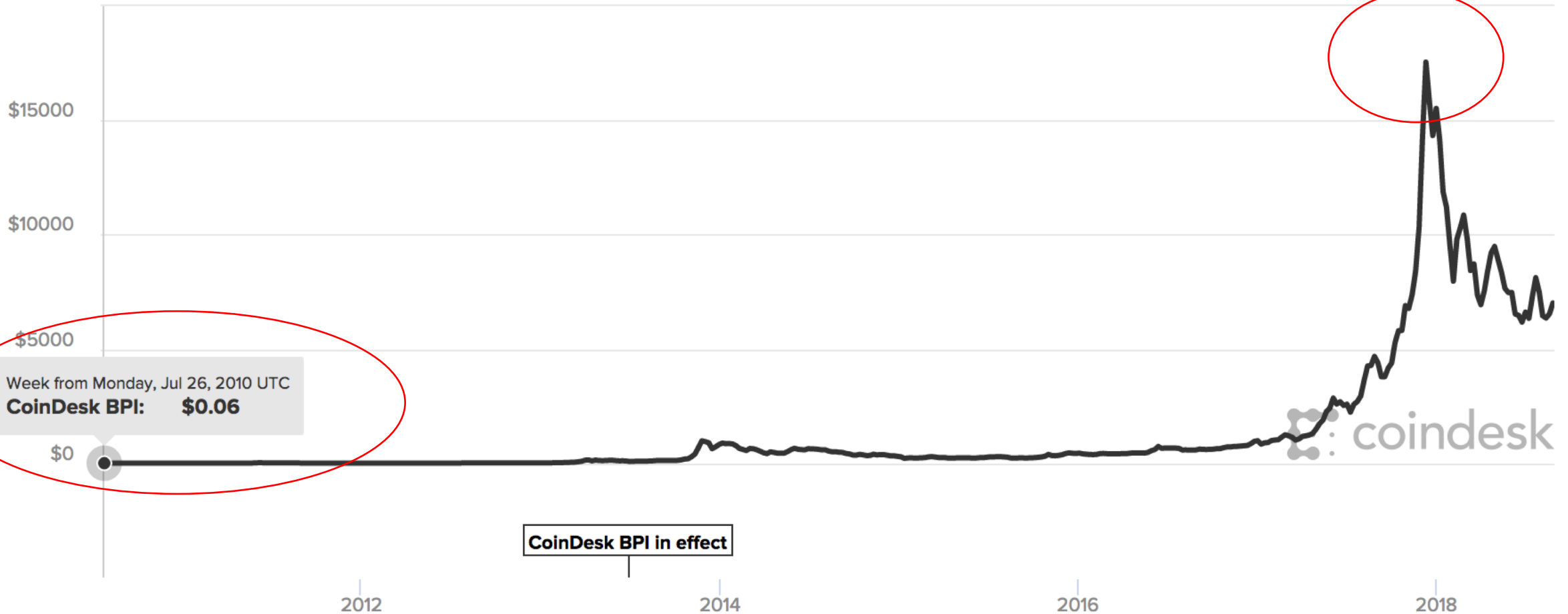
1h 12h 1d 1w 1m 3m 1y **All**

Jul 18, 2010

to

Aug 29, 2018

Export



Week from Monday, Jul 26, 2010 UTC
CoinDesk BPI: **\$0.06**

CoinDesk BPI in effect

coindesk

How to Learn Cybersecurity in MTU?

Security Courses in MTU

- CS 4471 - Computer Security
- CS 4740 - Development of Trusted Software
- MA 3203 - Cryptography
- EE 4723 - Network Security
- SAT 3812 - Cybersecurity I
- SAT 4812 - Cybersecurity II

Other Resources for Cybersecurity Learning

- NCL/CTF cybersecurity competition team @CS
 - <https://snp.cs.mtu.edu/education/#competition>
 - Alex Larkin (junior student) ranked 36th out of 3,350 participants in NCL Spring 2018 regular season
- Cyber security reading group @CS
 - <https://snp.cs.mtu.edu/education/#rg>
 - A forum consists of both graduate and undergraduate students. Students sit together biweekly to present and discuss the most recent security instances/research
- Security and Privacy (SnP) Lab @CS
 - <https://snp.cs.mtu.edu/>
 - Conduct research on data security, network security, web security, blockchain, etc.



Faculty Members in MTU Working on Cybersecurity



Jean Mayo
jmayo@mtu.edu



Bo Chen
bchen1@mtu.edu



Yu Cai
cai@mtu.edu



Guy Hembroff
hembroff@mtu.edu



Steven Goldsmith
sygoldsm@mtu.edu

