An Introduction to Cybersecurity

CS 1000 - Explorations in Computing

November 09, 2020

Bo Chen, PhD

Department of Computer Science

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

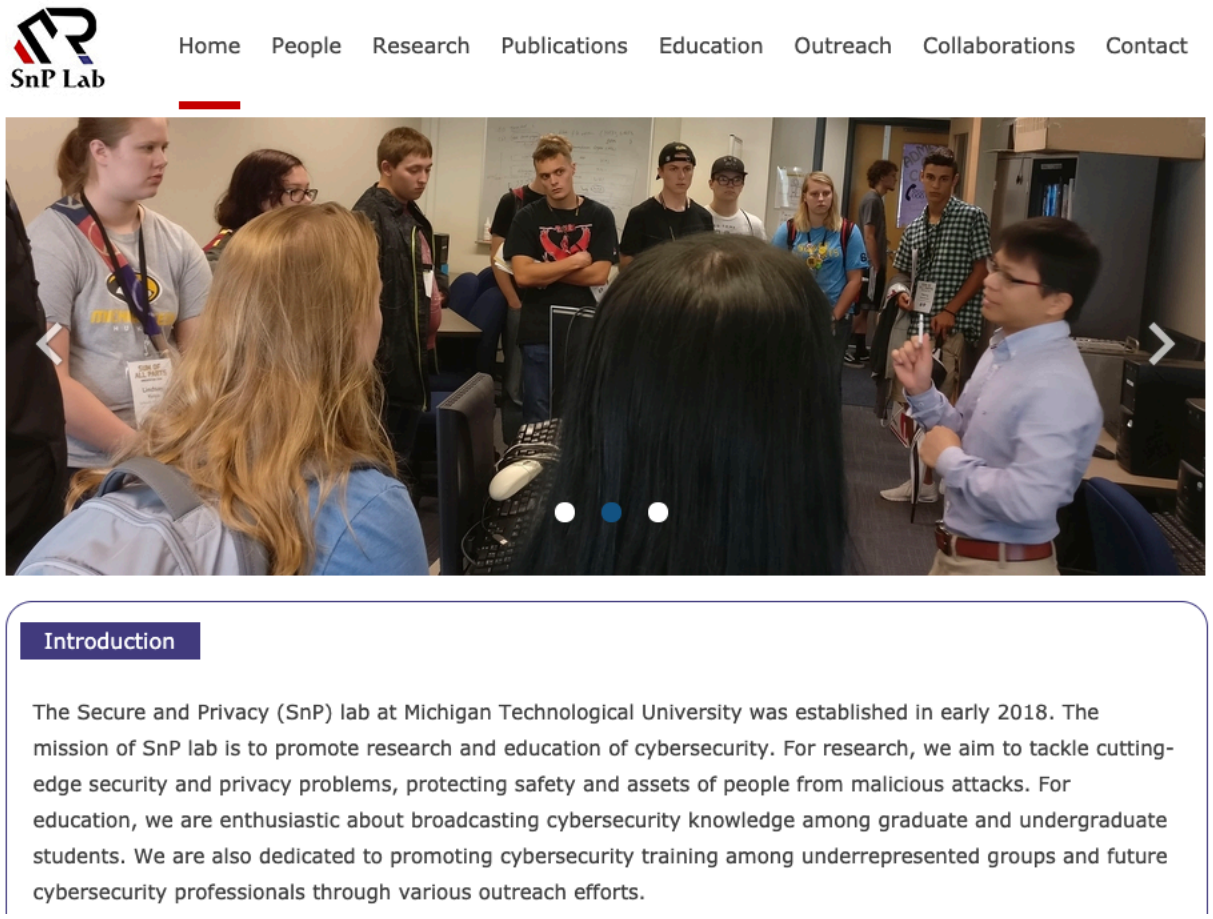
Faculty Website

Areas of Expertise

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

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

About MTU Security and Privacy (SnP) Lab



PhD Students

Niusen Chen

Wen Xie

Weijing You (UCAS)

Master Students

Shashank Reddy Danda

Jonah Schulte

Deepthi Tankasala

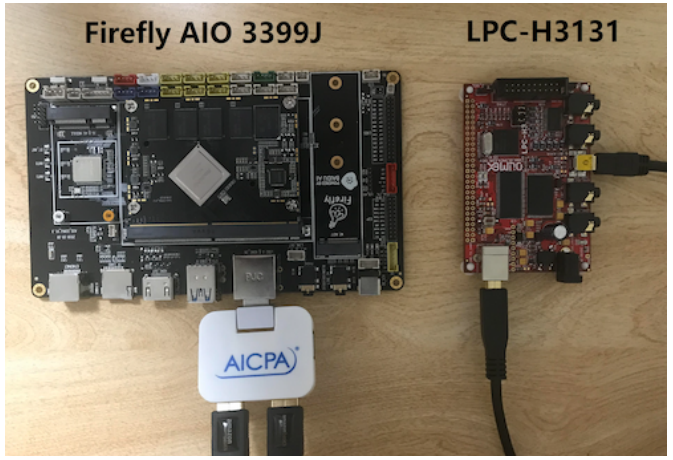
Undergraduate Students

Dominika Bobik

https://snp.cs.mtu.edu

About MTU Security and Privacy (SnP) Lab

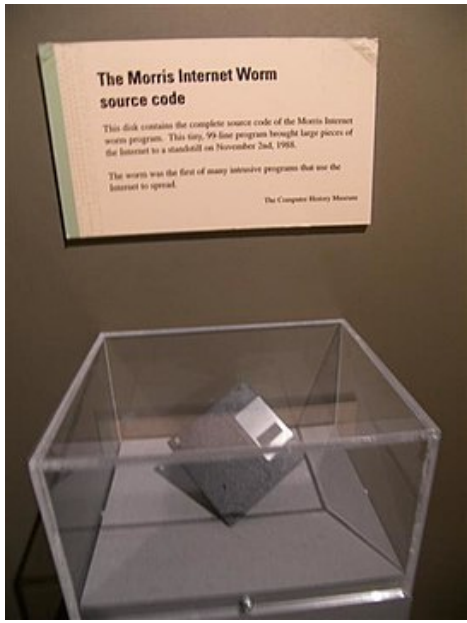
- Projects are currently funded by national science foundation, national security agency, etc.
  - Protecting sensitive data in mobile devices, IoT devices
  - Protecting critical data/ infrastructures outsourced to public clouds
  - Blockchain and information centric networking
  - Leveraging mobile devices for COVID-19 mitigation (recently)



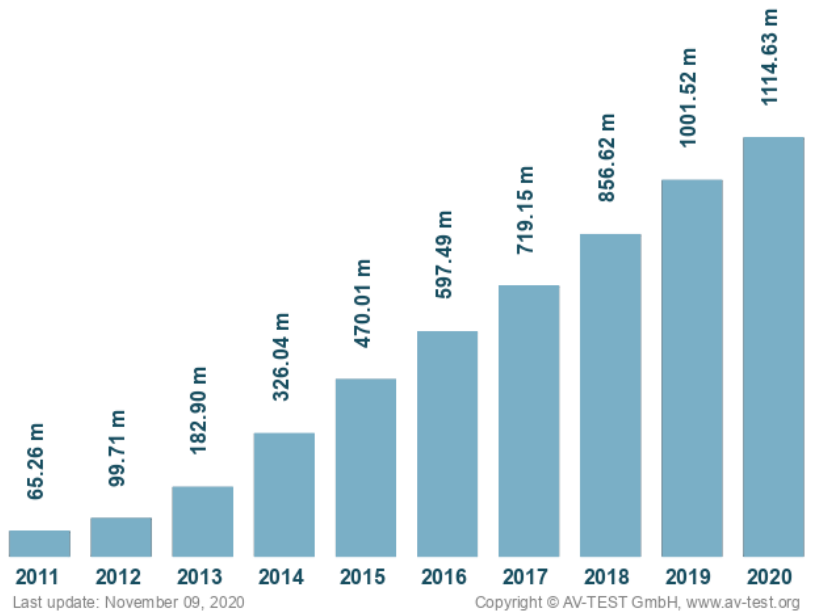
A Starting Video

- https://www.youtube.com/embed/ThBpRBpyxLI?start=0&end=50&version=3

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 10% of all those connected
- Malware and Hacks are here and there today



How to Combat Malware and Hacks?

- The answer is cybersecurity

- Ensure our systems and networks are well protected, such that any intruders can be detected, identified, and blocked
  - Make sure the software (code) 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 (a few basic things you should know about cybersecurity) – cybersecurity 101
- Why learning cybersecurity
- How to learn cybersecurity in MTU

Recent Cybersecurity Instances

Hacking Instances Just Happen

HEALTHCARE & PHARMA MAY 8, 2020 / 1:20 PM / UPDATED 6 MONTHS AGO

Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead - sources

REUTERS World Business Markets Breakingviews Video More

U.S. LEGAL NEWS MARCH 23, 2020 / 3:08 PM / UPDATED 7 MONTHS AGO

Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike

Early 2020

EMAIL SECURITY, SECURITY NEWS

Texas school district phished for $2.3 million

By **Doug Olenick** January 13, 2020

The Manor Independent School District fell victim to an apparent phishing scam to the

DATA BREACH, EMAIL SECURITY, HEALTH CARE, SECURITY NEWS

Breach of email accounts impacts 50,000 patients of Minnesota hospital

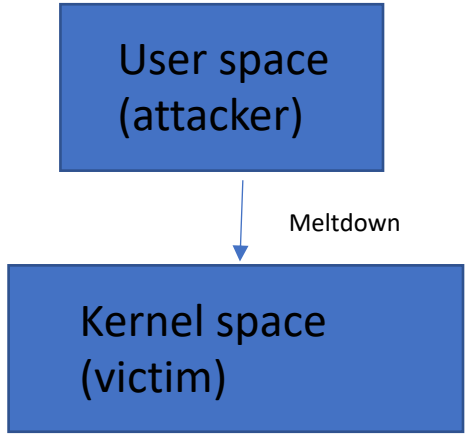
By **Bradley Barth** January 7, 2020

Data Breach Instances in 2019

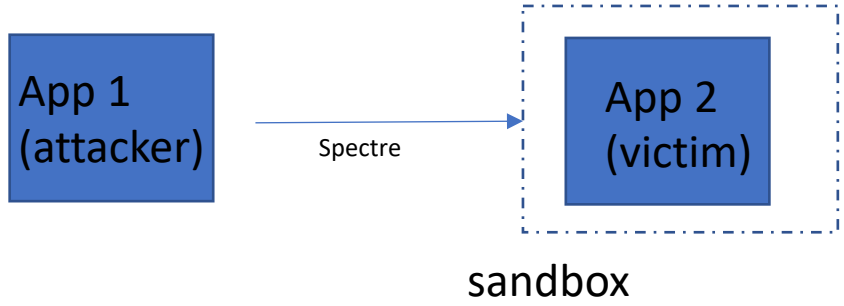
Entity	Year	Records	Organization type	Method
Adobe Inc.	2019	7.5 million	tech	poor security
Amazon Japan G.K.	2019	unknown	web	accidentally published
2019 Bulgarian revenue agency hack	2019	over 5,000,000	government	hacked
Canva	2019	140,000,000	web	hacked
Capital One	2019	106,000,000	financial	unsecured S3 bucket
Desjardins	2019	2,900,000	financial	inside job
DoorDash	2019	4,900,000	web	hacked
Facebook	2019	540,000,000	social network	poor security
Facebook	2019	1,500,000	social network	accidentally uploaded
Facebook	2019	267,000,000	social network	poor security
First American Corporation	2019	885,000,000	financial service company	poor security
Health Sciences Authority (Singapore)	2019	808,000	healthcare	poor security
Justdial	2019	100,000,000	local search	unprotected api
LifeLabs	2019	15,000,000	healthcare	hacked
Ministry of Health (Singapore)	2019	14,200	healthcare	poor security/inside job
Mobile TeleSystems (MTS)	2019	100,000,000	telecommunications	misconfiguration/poor security
Quest Diagnostics	2019	11,900,000	Clinical Laboratory	poor security
StockX	2019	6,800,000	retail	hacked

2018 – Intel Meltdown and Spectre

- Meltdown: affects Intel chips and lets hackers bypass the hardware barrier between applications run by users and the computer's memory, potentially letting hackers read a computer's memory and steal passwords.



- Spectre: affects chips from Intel, AMD and ARM and lets hackers potentially trick otherwise error-free applications into giving up secret information.



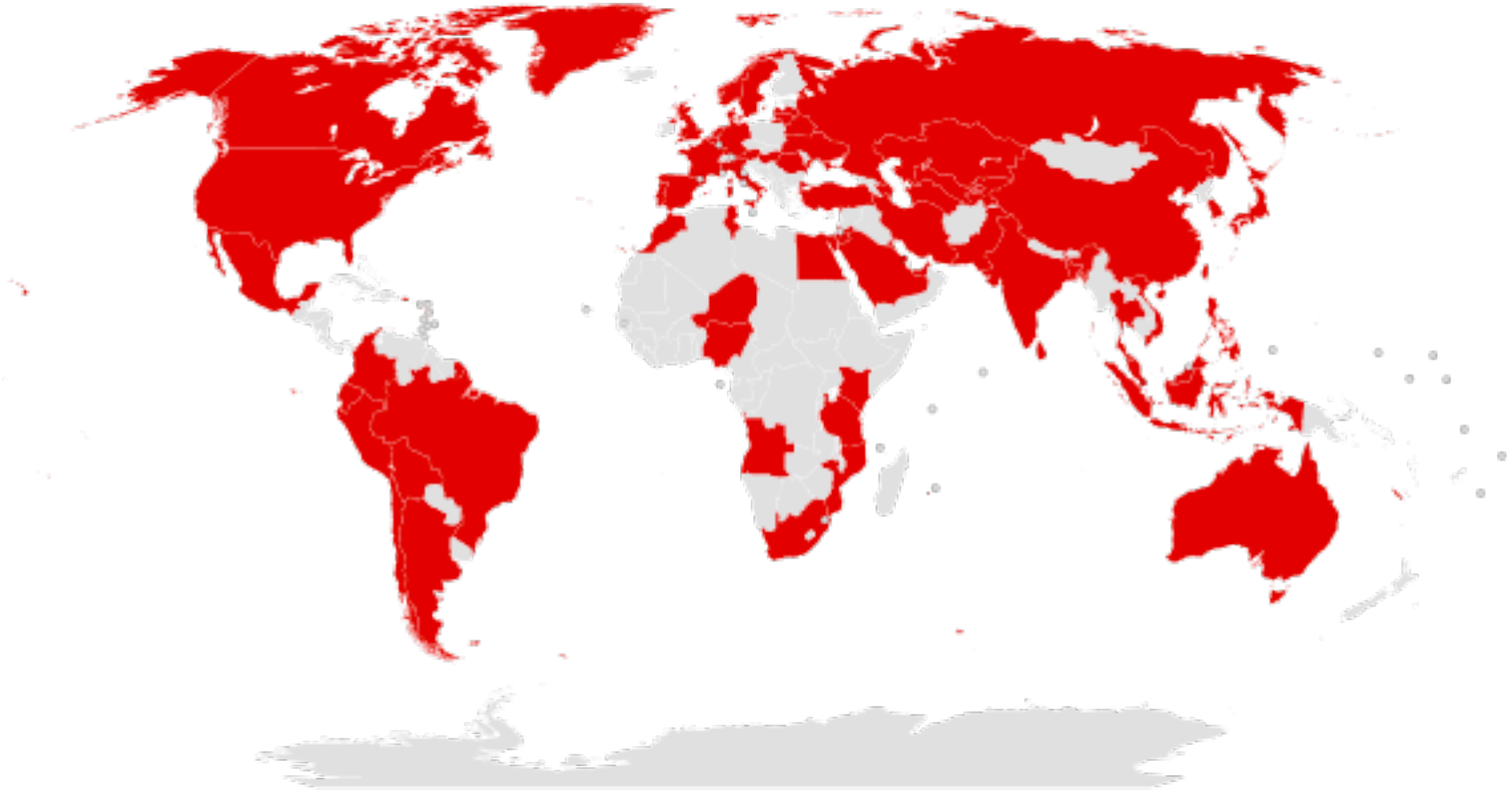
Data Breach Instances in 2018

Entity	Year	Records	Organization type	Method
Facebook	2018	50,000,000	social network	poor security
Google Plus	2018	500,000	social network	poor security
HauteLook	2018	28,517,244	retail	hacked
Marriott International	2018	500,000,000	hotel	hacked
MyHeritage	2018	92,283,889	genealogy	unknown
Orbitz	2018	880,000	web	hacked
Popsugar	2018	123,857	fashion	hacked
Quora	2018	100,000,000	Question & Answer	hacked
Reddit	2018	unknown	web	hacked
SingHealth	2018	1,500,000	government, database	hacked
Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked
Typeform	2018	unknown	tech	poor security
Under Armour	2018	150,000,000	Consumer Goods	hacked
United States Postal Service	2018	60,000,000	government	poor security
WordPress	2018			hacked

2017 - WannaCry

- WannaCry ransomware attack

Impact of WannaCry



Map of the countries initially affected

Data Breach Instances in 2017

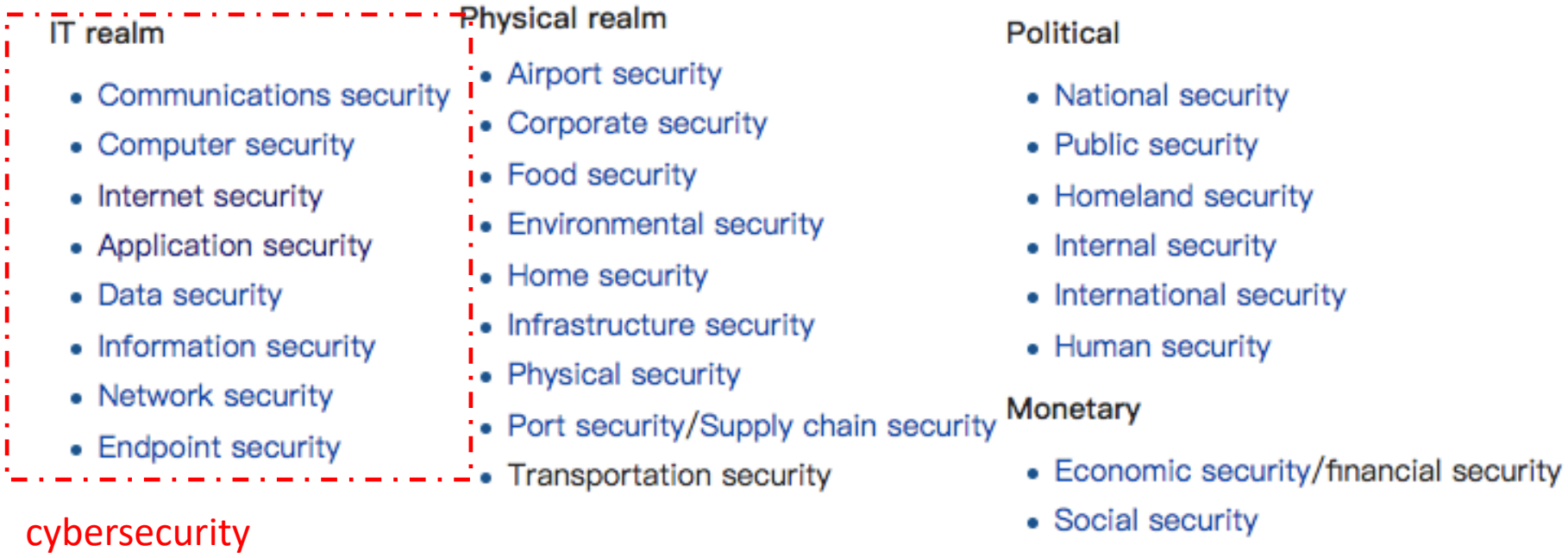
Entity	Year	Records	Organization type	Method
Bell Canada	2017	1,900,000	telecoms	poor security
Defense Integrated Data Center (South Korea)	2017	235 GB	military	hacked
Deloitte	2017	350 clients emails	consulting, accounting	poor security
Equifax	2017	143,000,000	financial, credit reporting	poor security
Grozio Chirurgija	2017	25,000	healthcare	hacked
Heathrow Airport	2017	2.5GB	transport	lost / stolen media
Taringa!	2017	28,722,877	web	hacked
Uber	2017	57,000,000	transport	hacked

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*) – **in physical space**
- 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 – **in cyber space**



Cybersecurity Objectives: CIA

Main security objectives:

- **C**onfidentiality: unauthorized users cannot read information
- **I**ntegrity: unauthorized users cannot alter information
- **A**vailability: the information must be available when it is needed

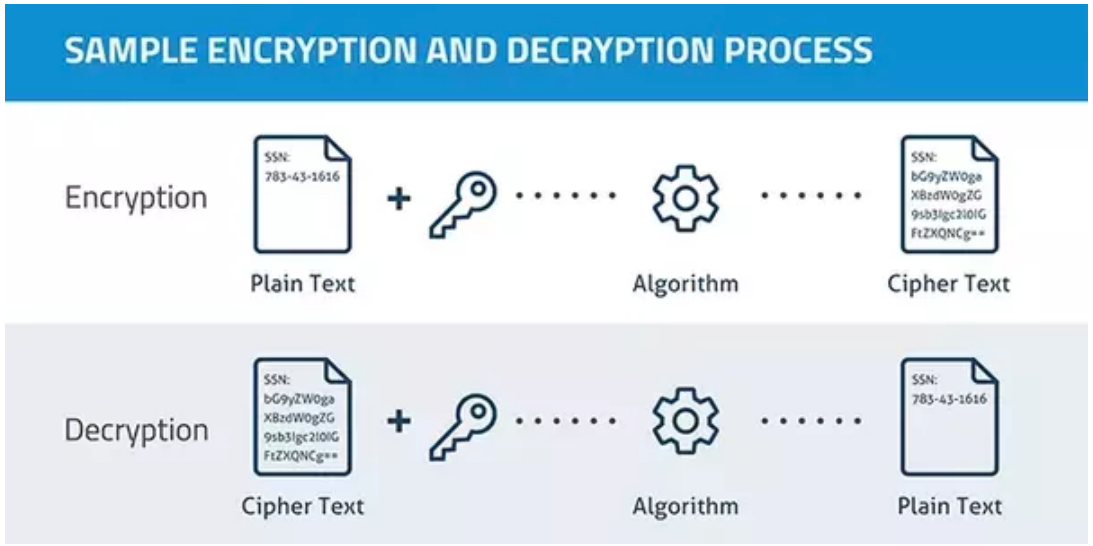
Other security objectives:

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

Confidentiality

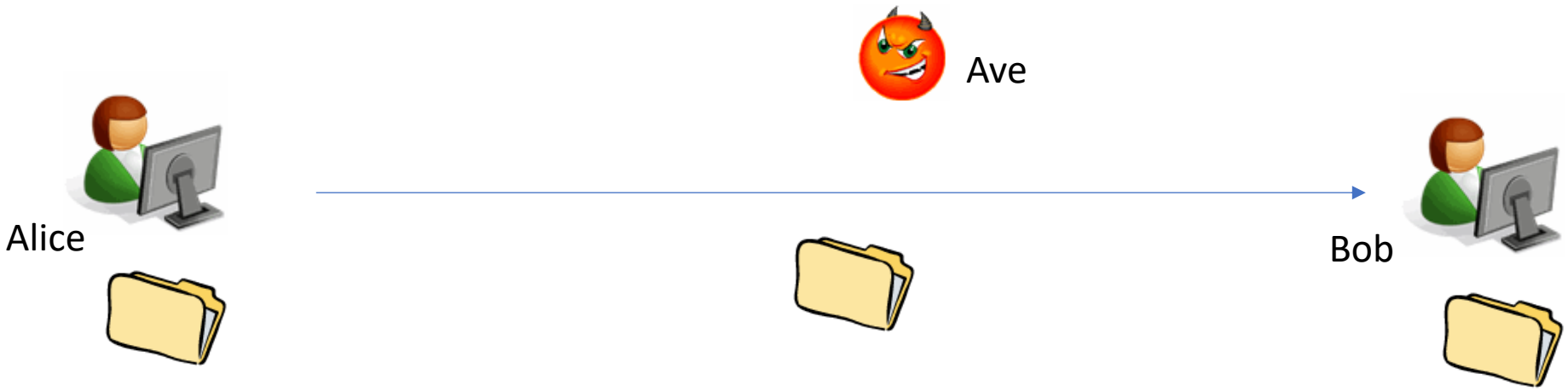
- *The concealment of information or resources*
  - Information is not made available or disclosed to unauthorized individuals, entities, or processes
  - E.g., your bank accounts, private photos, etc

- 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
  - Symmetric encryption: AES, DES, 3DES
  - Asymmetric encryption: RSA



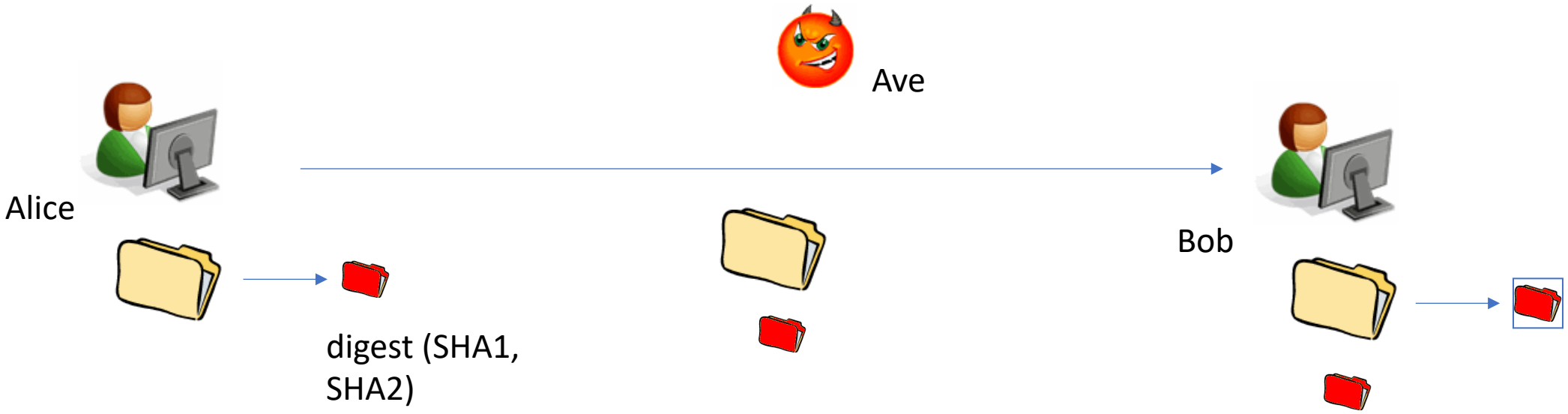
Integrity

- 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

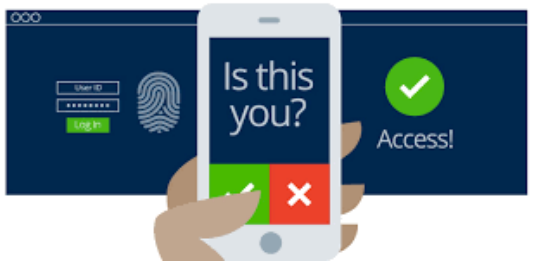
- For any information system to serve its purpose, the service/ information must be available when it is needed
  - This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning 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 and Identification

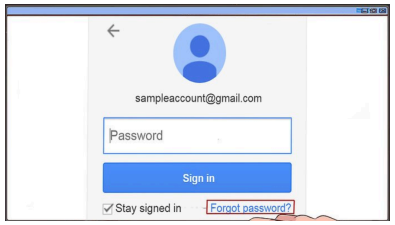
- Authentication in physical world: are you really who you claim?
  - Confirm the identity of a person by validating his/her identity document (e.g., driver license, passport, student ID card)

- 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

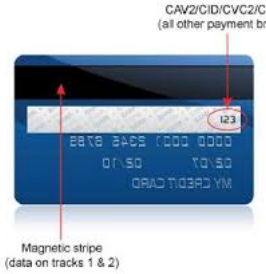


How to Do Authentication?

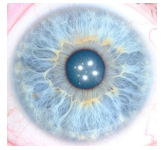
- Four general means for authenticating user's identity
  - Something the individual knows
    - Passwords

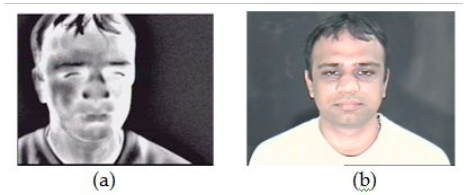


  - Something the individual possesses, a *token*
    - Memory card, smart card

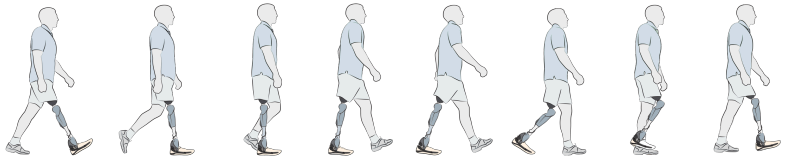


  - Something the individual is
    - Fingerprint, iris, retina, face





  - Something the individual does (behavior pattern)
    - Typing rhythm, gait, and voice



How to Do Authentication (cont.)?

- Multi-factor authentication (MFA) – used in our own IT systems in MTU

Access Control

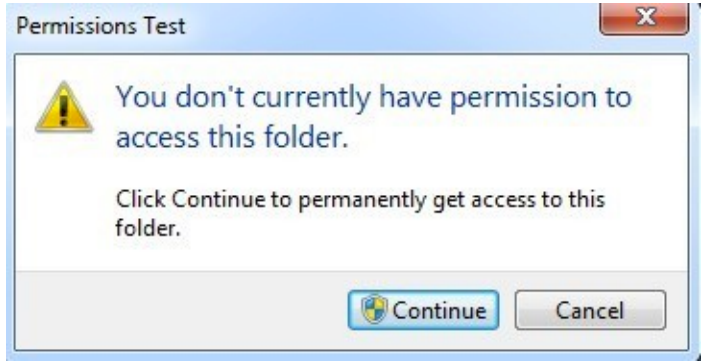
- Access control in physical world: the selective restriction of access to a place. It is a matter of who, where, and when.
  - Historically, this was partially accomplished through mechanical keys and locks

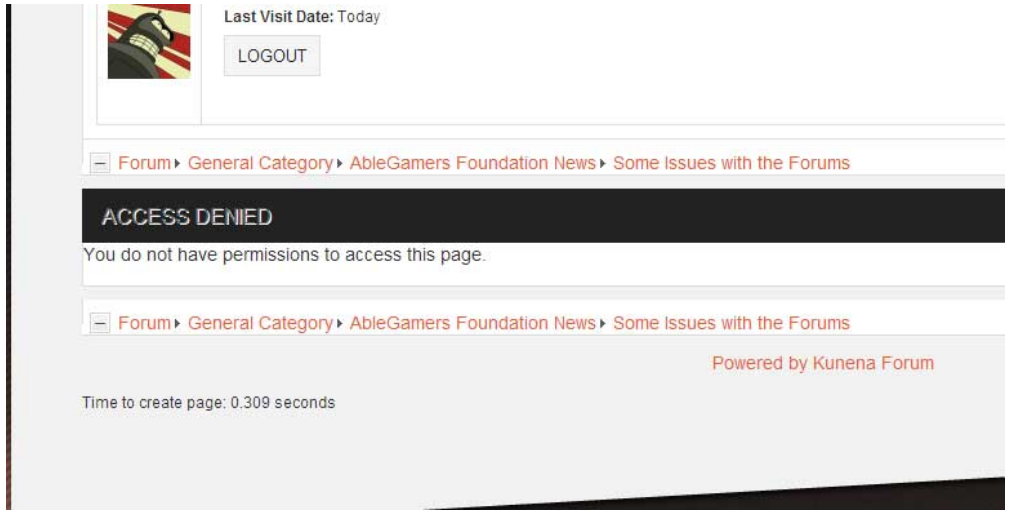
- Access control in computers: the selective restriction of access to computing resources (who, what, and how)
  - Who: users, programs, processes, etc.
  - What: computing resources like files, memory, I/O ports, etc.
  - How: how the computing resources can be “touched”

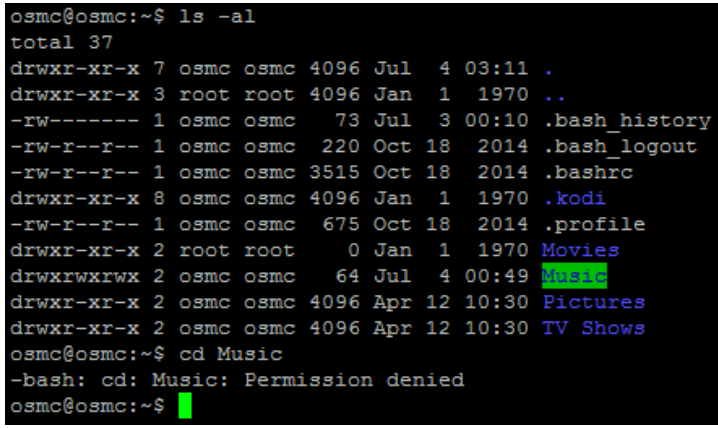
How to Do Access Control?

- 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

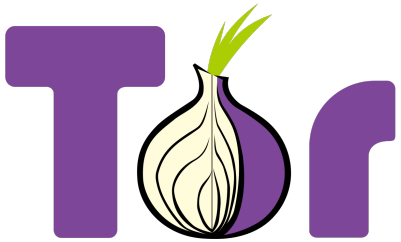






Anonymity - Tor

- Anonymity: a person remains non-identifiable, unreachable, or untrackable
- Is anonymity good or bad? What do you think?
- Internet now is not anonymized
  - Each IP address can be mapped to a particular Internet Service Provider (ISP), who can then provide information about what customer that IP address belongs to
- Tor is free software for enabling anonymous communication
  - A worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis
  - https://www.torproject.org/



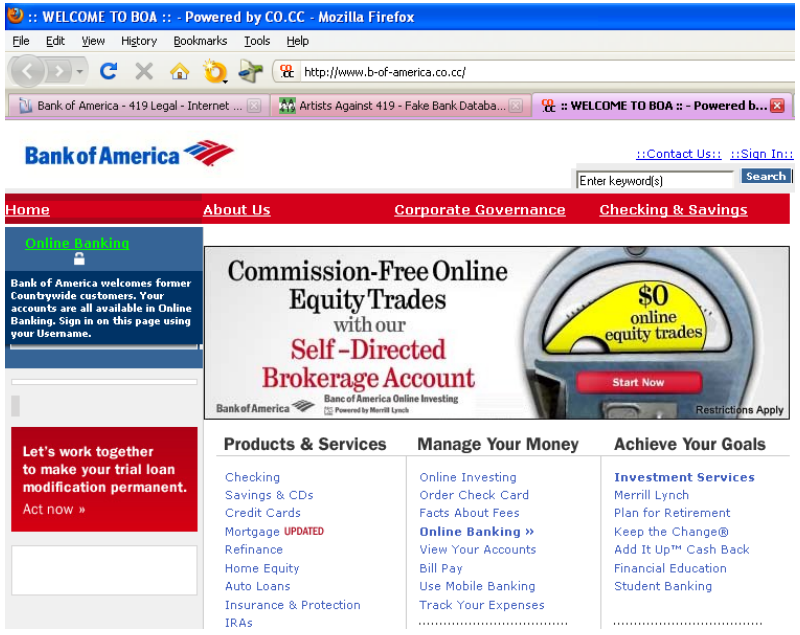
Why Learning Cybersecurity?

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

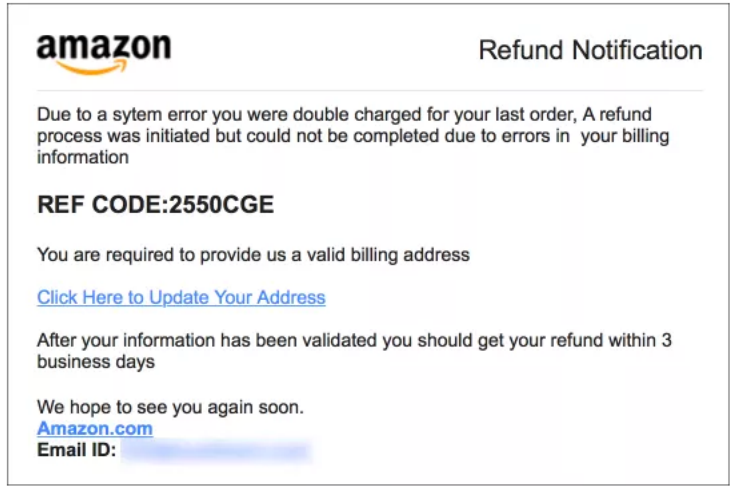
Protect Your Own Asset

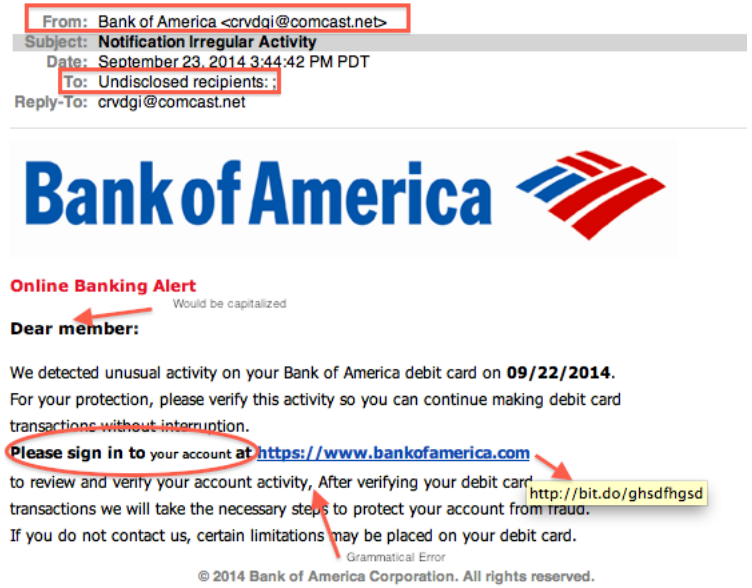
- Reduce the possibility of exposure to potential hacks
  - Malicious code is here and there (malicious java scripts, applets, etc.)
  - Make sure you trust the web sites before you go there (a lot of phishing website)
    - www.google.com is fine, but www.go0gle.com may not
    - Do you want to click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

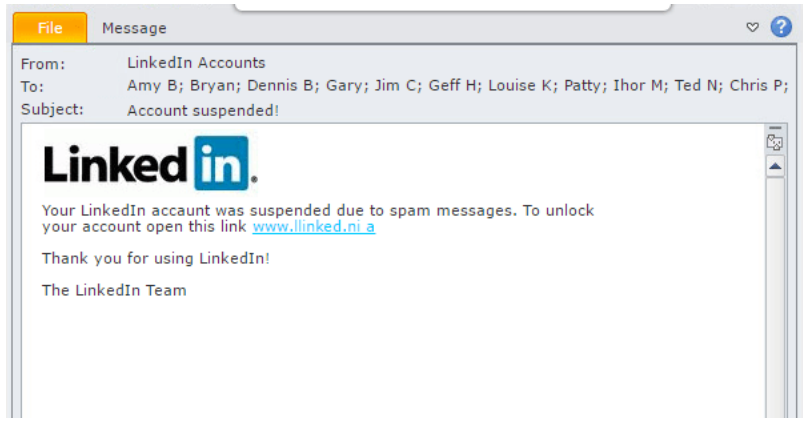


Protect Your Own Asset (cont.)

- Reduce the possibility of exposure to potential hacks
  - A lot of phishing emails

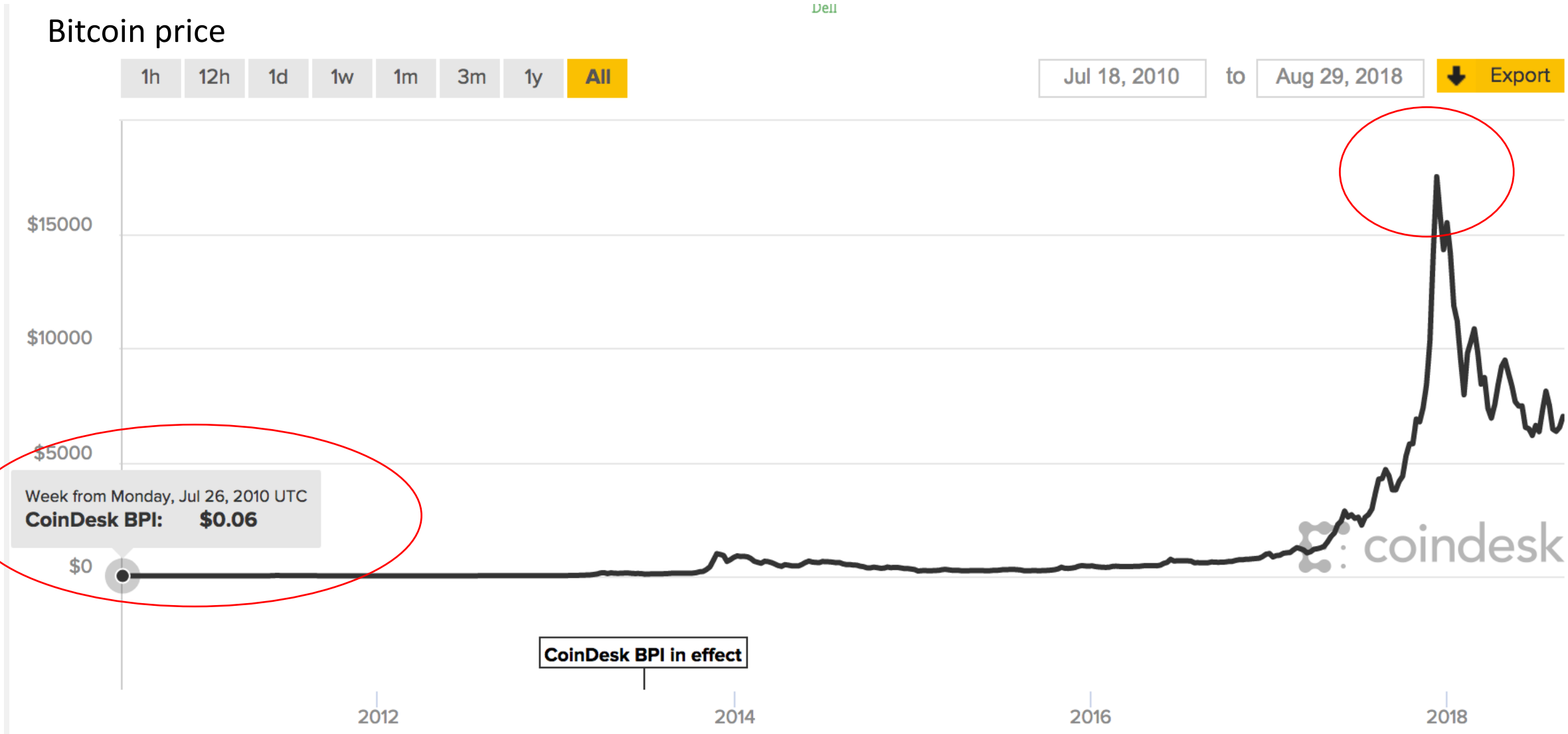






Security Technology Is Money Sometimes

Bitcoin price



How to Learn Cybersecurity in MTU?

Cybersecurity Programs in MTU

- Cybersecurity BS

Cybersecurity Programs in MTU

- Cybersecurity MS

Security Courses in MTU for Undergraduates

- 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

- MTU RedTeam
  - https://snp.cs.mtu.edu/education/#competition
  - 20+ undergraduate students which are enthusiastic for hacking and defending
  - Have been getting involved in various cybersecurity competitions including NCL cyber competition, CYPHERCON, etc.
  - 7 MTU undergraduates were ranked top 100 out of 6,000 participants in NCL Cyber competition in Fall 2020, and 3 team ranked top 100 out of (not finalized yet)

- 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

Faculty Members in MTU Working on Cybersecurity

Yu Cai

Professor, Applied Computing

Affiliated Professor, Computational Science and Engineering

cai@mtu.edu

906-487-1471

Area of Expertise

- Cybersecurity
- Computer Network

Guy Hembroff

Associate Professor, Applied Computing

Director, Health Informatics Graduate Program

Affiliated Associate Professor, Data Science

hembroff@mtu.edu
906-487-3248

Jeffrey Wall

Assistant Professor of Management Information Systems, College of Business

Richard and Joyce Ten Haken Faculty Fellow in Business

jdwall@mtu.edu

906-487-1707

Research Interests

- Information security behavior

Bo Chen

Assistant Professor, Computer Science

bchen@mtu.edu

906-487-3149

Rekhi 301

Links of Interest

Areas of Expertise

- Mobile Device Security
- Cloud Computing Security

Jean Mayo

Professor, Computer Science

Graduate Program Director, Computer Science

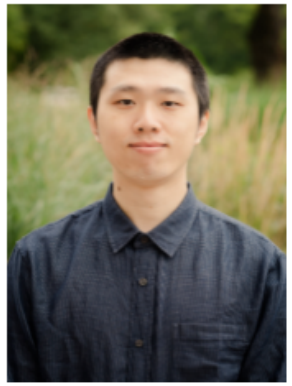
jmayo@mtu.edu

906-487-3157

Rekhi Hall 304

Area of Expertise

- Distributed Systems
- Operating Systems
- Security



Xiaoyong (Brian) Yuan

Assistant Professor, Applied Computing

Assistant Professor, Computer Science

xyyuan@mtu.edu

906-487-4303

Rekhi 111

Areas of Expertise

- Machine Learning
- Security and Privacy
- Cloud Computing

Acknowledgments

- Our cybersecurity research has been supported by US National Science Foundation under grant number 1928349-CNS and 1938130-CNS
- Our cybersecurity education has been supported by a few Gencyber grants from NSA and NSF (co-funded)

Q &A