Spring 2019 MTU Workshop to Expose Undergraduate Women to Computer Science Research

Security Track

An Introduction of Cybersecurity and Flash Memory Security Research

Bo Chen

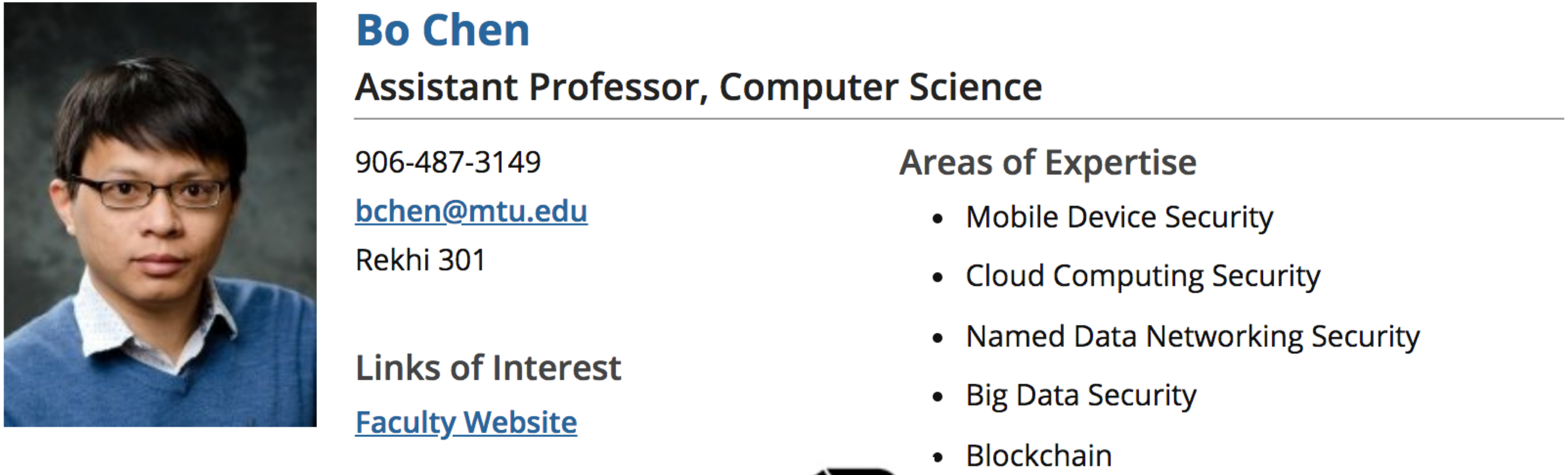
Assistant Professor, Department of Computer Science

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

Lab director: Security and Privacy (SnP) Lab

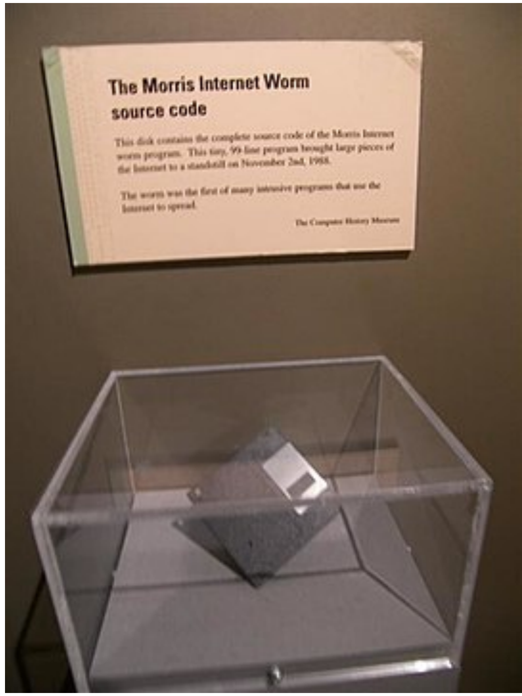
SnP Lab

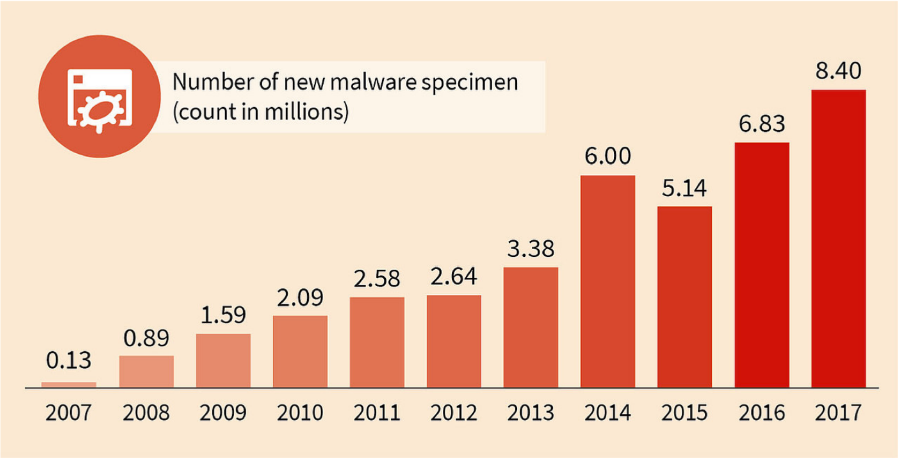
Co-advisor: CS cybersecurity reading group, MTU RedTeam
Faculty coach: MTU NCL cyber competition team (Alex Larkin places 17th out of 3,324 students/players in NCL Fall 2018 Regular Season)

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


The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intensive programs that use the Internet to spread.
The Computer History Museum



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
- Mobile devices and flash memory
- Flash memory security research

Recent Cybersecurity Instances

2018 Data Breaches and Hacks

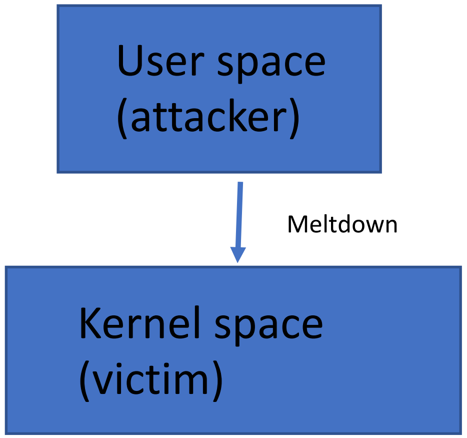
Facebook - Cambridge Analytica data scandal: 87 million user profiles were disclosed

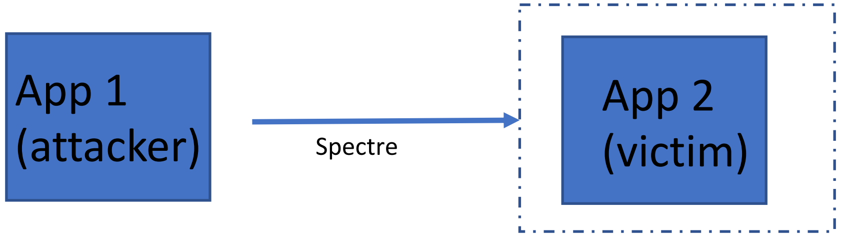
- Various political organizations used information from Cambridge Analytica to attempt to influence public opinion:
  - 2015 and 2016 campaigns of United States politicians Donald Trump and Ted Cruz
  - 2016 Brexit (British exit from the European Union) vote
  - 2018 Mexican general election, 2018 for 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
- Pepple: 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

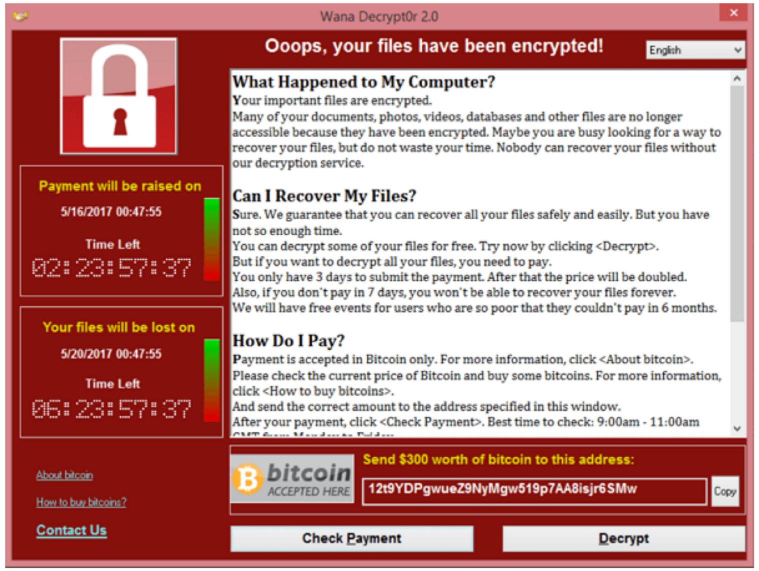
2017 Data Breach and Hacks (cont.)

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



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

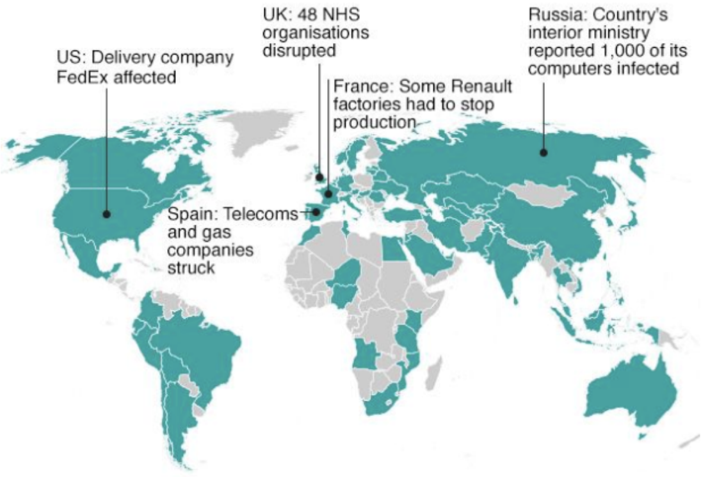
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Countries hit in initial hours of cyber-attack



US: Delivery company FedEx affected
UK: 48 NHS organisations disrupted
France: Some Renault factories had to stop production
Russia: Country's interior ministry reported 1,000 of its computers infected
Spain: Telecoms and gas companies struck

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

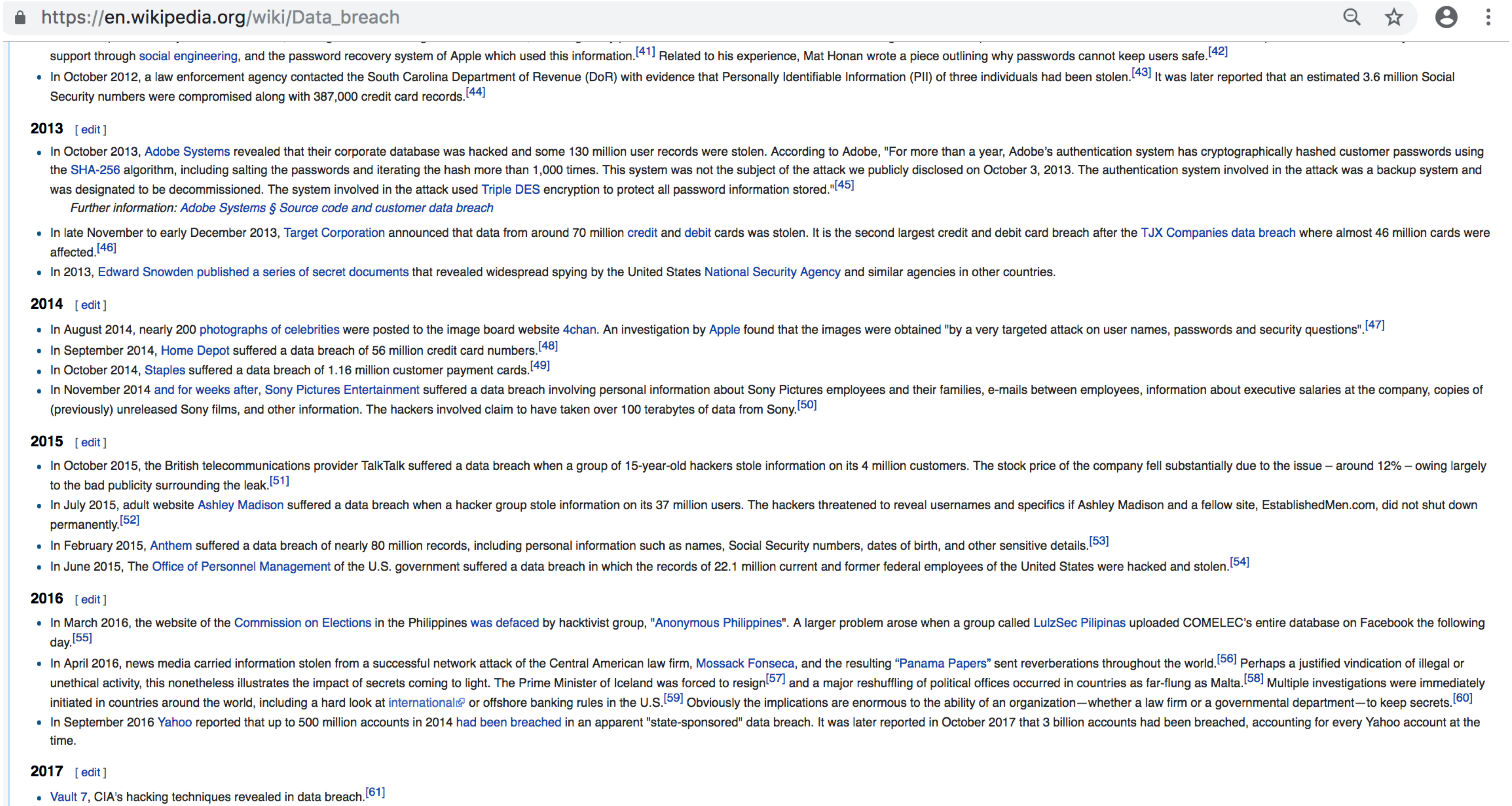
Source: Kaspersky Lab's Global Research & Analysis Team

BBC

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



https://en.wikipedia.org/wiki/Data_breach

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]

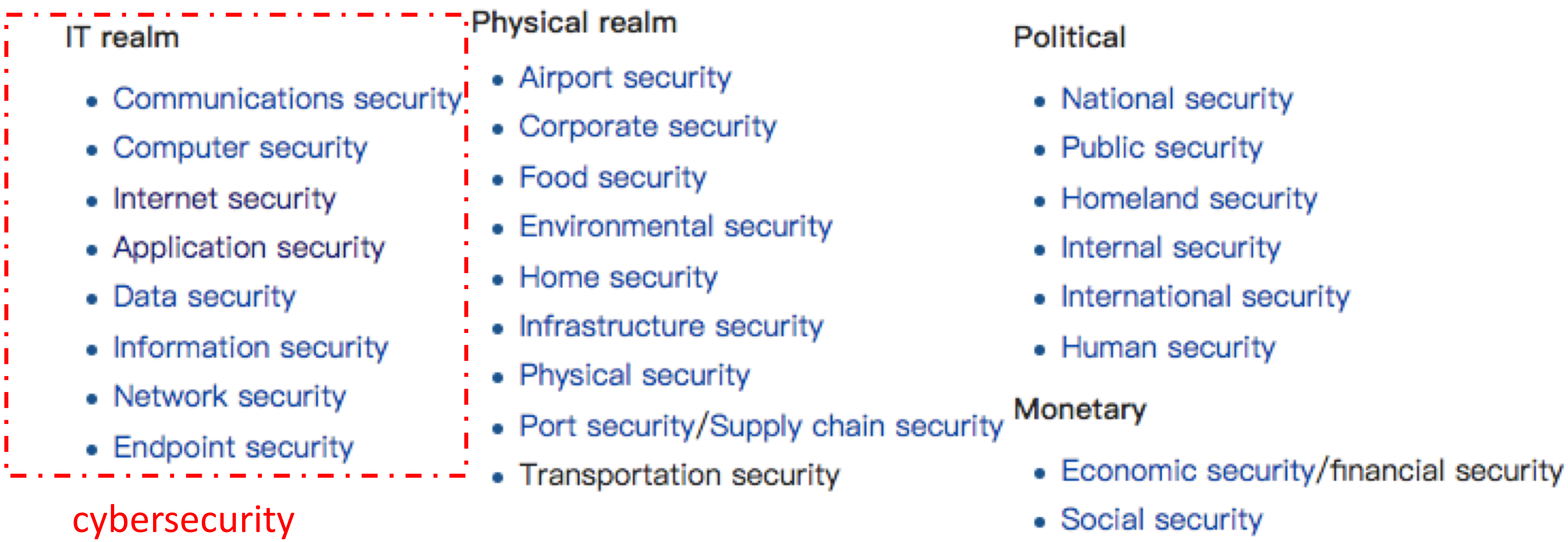
- Vault 7, CIA's hacking techniques revealed in data breach.[61]

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



IT realm

- Communications security
- Computer security
- Internet security
- Application security
- Data security
- Information security
- Network security
- Endpoint security

cybersecurity

Physical realm

- Airport security
- Corporate security
- Food security
- Environmental security
- Home security
- Infrastructure security
- Physical security
- Port security/Supply chain security
- Transportation security

Political

- National security
- Public security
- Homeland security
- Internal security
- International security
- Human security

Monetary

- Economic security/financial security
- Social security

Cybersecurity Objectives: CIA

Main security objectives:

- **C**onfidentiality: unauthorized users cannot read information
- **I**ntegrity: unauthorized users cannot alter information
- **A**vailability: authorized users can always access information

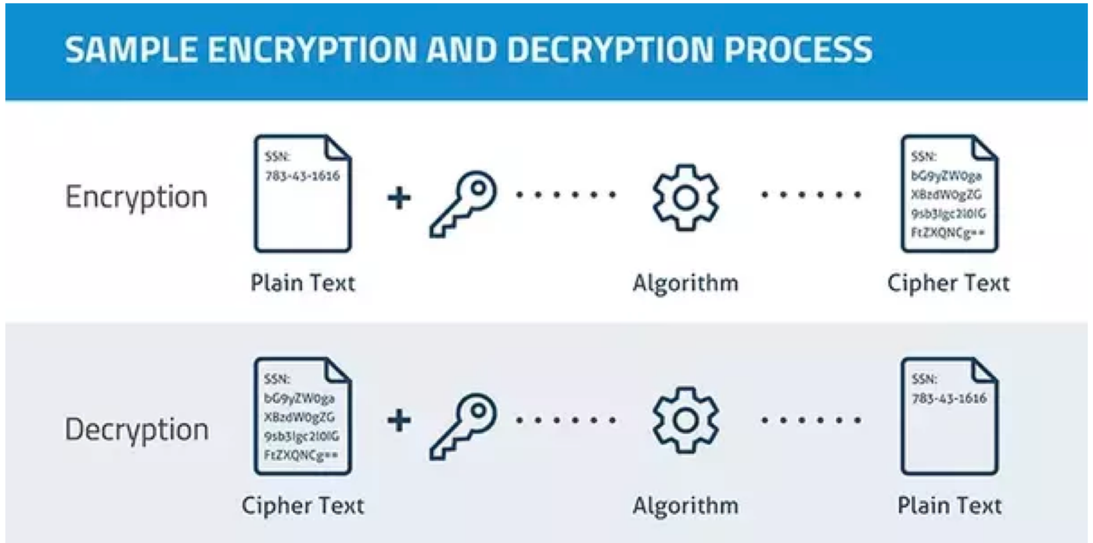
Other security objectives:

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

Confidentiality

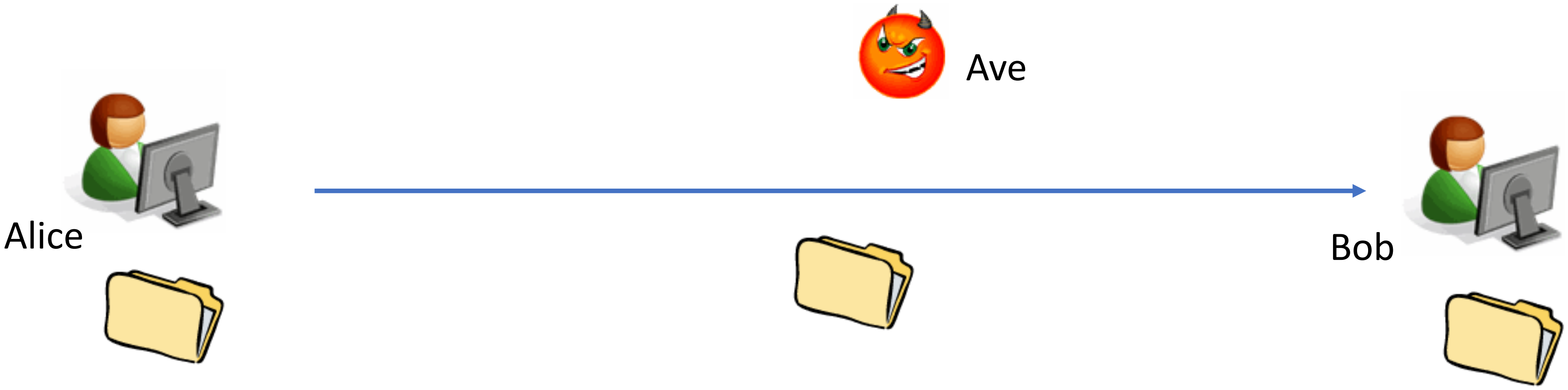
- *The concealment of information or resources*
  - Information is not made available or disclosed to unauthorized individuals, entities, or processes
  - E.g., your bank accounts, private photos, etc

- 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



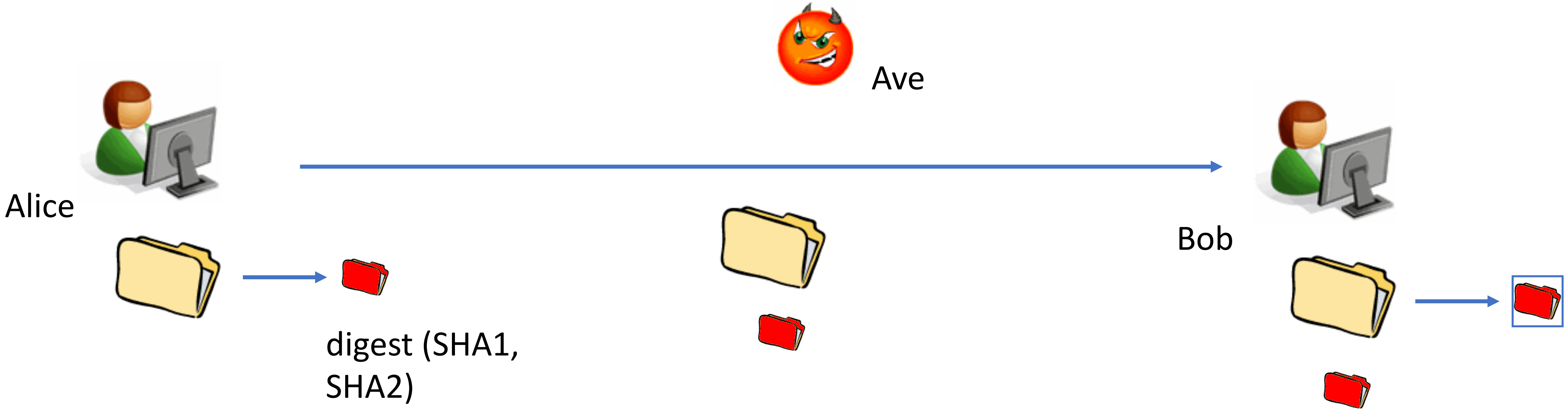
Integrity

- 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

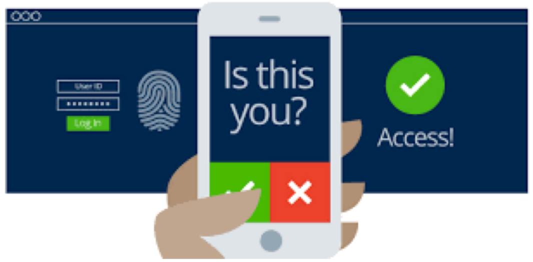
- For any information system to serve its purpose, the service/ information must be available when it is needed
    - This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning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

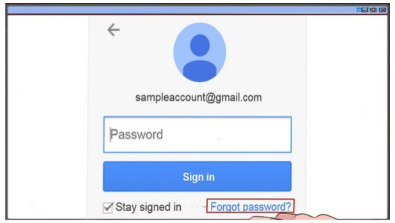
- Authentication in physical world: are you really who you claim?
  - Confirm the identity of a person by validating his/her identity document (e.g., driver license, passport, student ID card)

- 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



sampleaccount@gmail.com

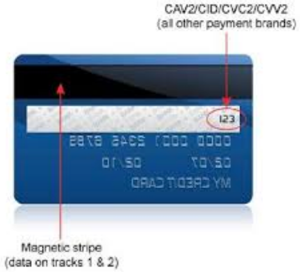
Password

Sign in

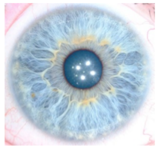
☑ Stay signed in

Forgot password?

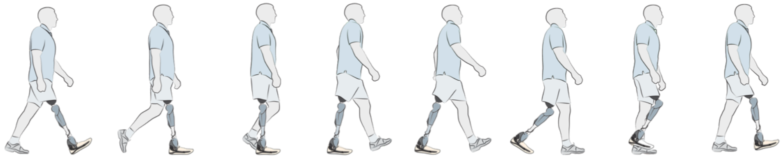
  - Something the individual possesses, a *token*
    - Memory card, smart card



  - 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

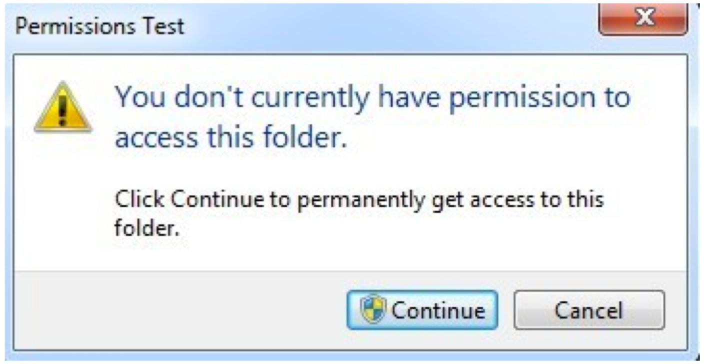
- Access control in physical world: the selective restriction of access to a place. It is a matter of who, where, and when.
  - Historically, this was partially accomplished through mechanical keys and locks

- 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

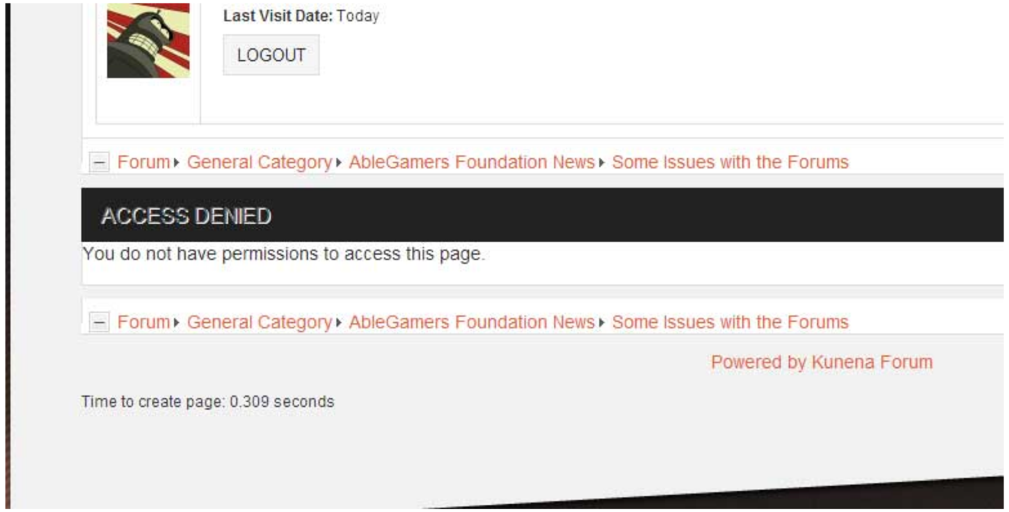
- The access control is enforced by systems (operating systems, database management systems, etc.) following permissions



Permissions Test

You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.



Last Visit Date: Today

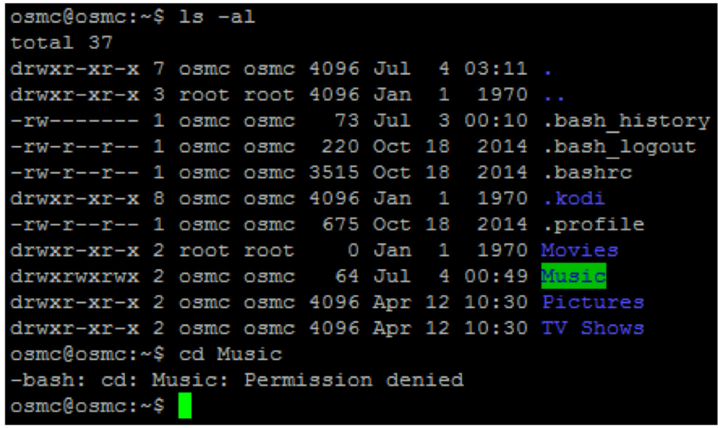
LOGOUT
Forum ▸ General Category ▸ AbleGamers Foundation News ▸ Some Issues with the Forums

ACCESS DENIED

You do not have permissions to access this page.

Forum ▸ General Category ▸ AbleGamers Foundation News ▸ Some Issues with the Forums
Powered by Kunena Forum

Time to create page: 0.309 seconds

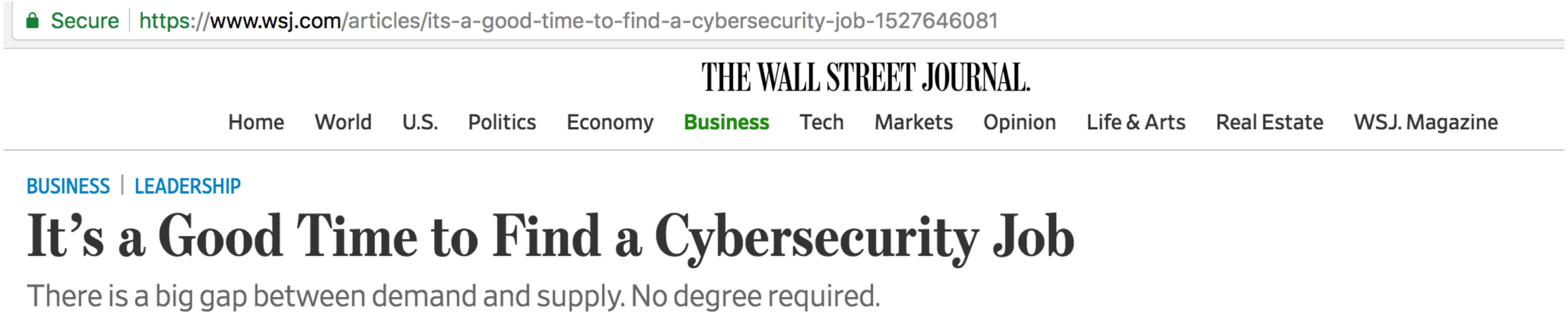


```
osmc@osmc:~$ ls -al
total 37
drwxr-xr-x 7 osmc osmc 4096 Jul  4 03:11 .
drwxr-xr-x 3 root root 4096 Jan  1  1970 ..
-rw------- 1 osmc osmc   73 Jul  3 00:10 .bash_history
-rw-r--r-- 1 osmc osmc  220 Oct 18  2014 .bash_logout
-rw-r--r-- 1 osmc osmc 3515 Oct 18  2014 .bashrc
drwxr-xr-x 8 osmc osmc 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



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

THE WALL STREET JOURNAL.

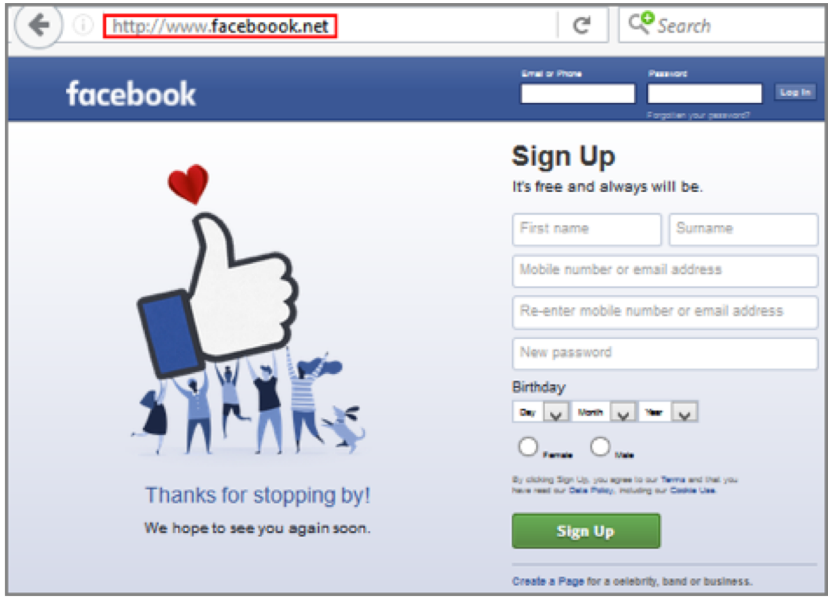
BUSINESS | LEADERSHIP

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



Sign Up

It's free and always will be.

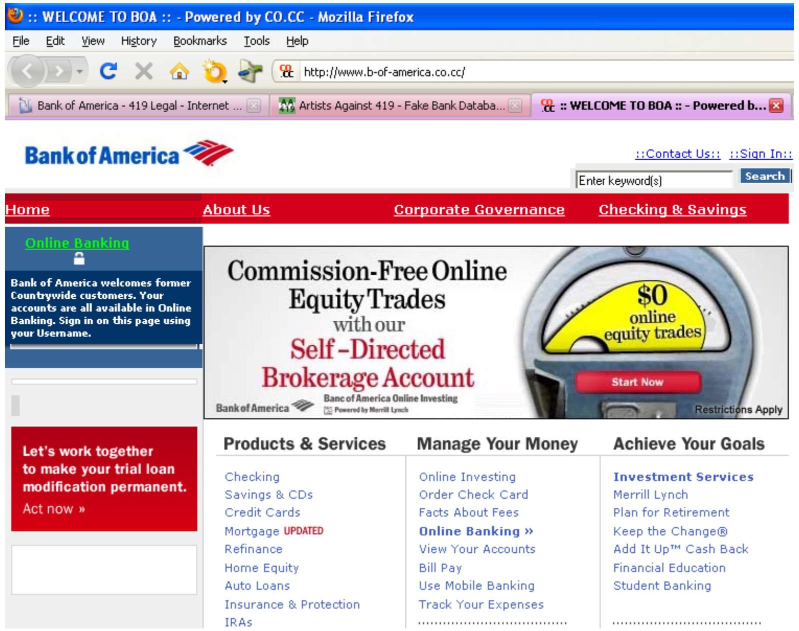
Birthday

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.

Thanks for stopping by!

We hope to see you again soon.



:: WELCOME TO BOA :: - Powered by CO.CC - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.b-of-america.co.cc/
Bank of America - 419 Legal - Internet ...
Artists Against 419 - Fake Bank Databa...
:: WELCOME TO BOA :: - Powered b...
Bank of America
::Contact Us:: ::Sign In::
Enter keyword(s)
Search
Home
About Us
Corporate Governance
Checking & Savings
Online Banking
$0 online equity trades
Start Now
Restrictions Apply
Bank of America
Banc of America Online Investing
Powered by Merrill Lynch

Bank of America welcomes former Countrywide customers. Your accounts are all available in Online Banking. Sign in on this page using your Username.

Commission-Free Online Equity Trades with our Self-Directed Brokerage Account

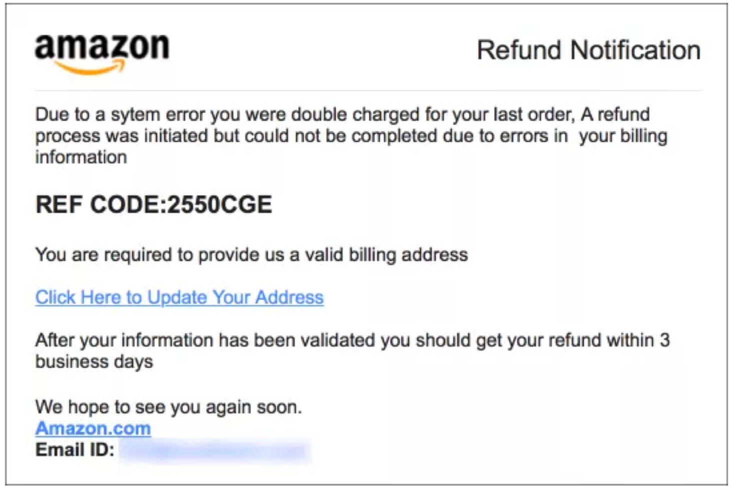
Let's work together to make your trial loan modification permanent.

Act now »

Products & Services	Manage Your Money	Achieve Your Goals
Checking	Online Investing	Investment Services
Savings & CDs	Order Check Card	Merrill Lynch
Credit Cards	Facts About Fees	Plan for Retirement
Mortgage UPDATED	Online Banking »	Keep the Change®
Refinance	View Your Accounts	Add It Up™ Cash Back
Home Equity	Bill Pay	Financial Education
Auto Loans	Use Mobile Banking	Student Banking
Insurance & Protection	Track Your Expenses	
IRAs		

Protect Your Own Asset (cont.)

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



amazon Refund Notification

Due to a sytem 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

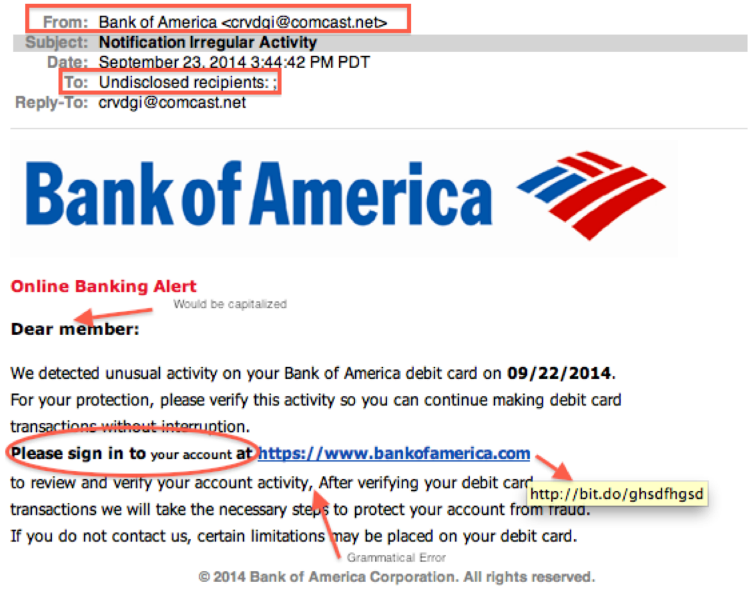
REF CODE:2550CGE

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]



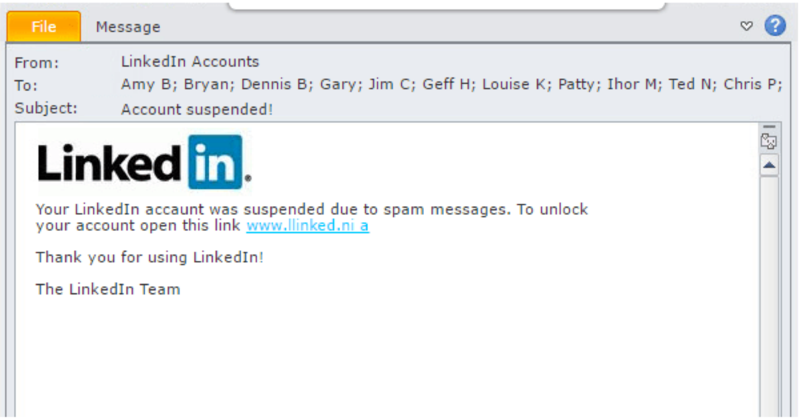
From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

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.



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!

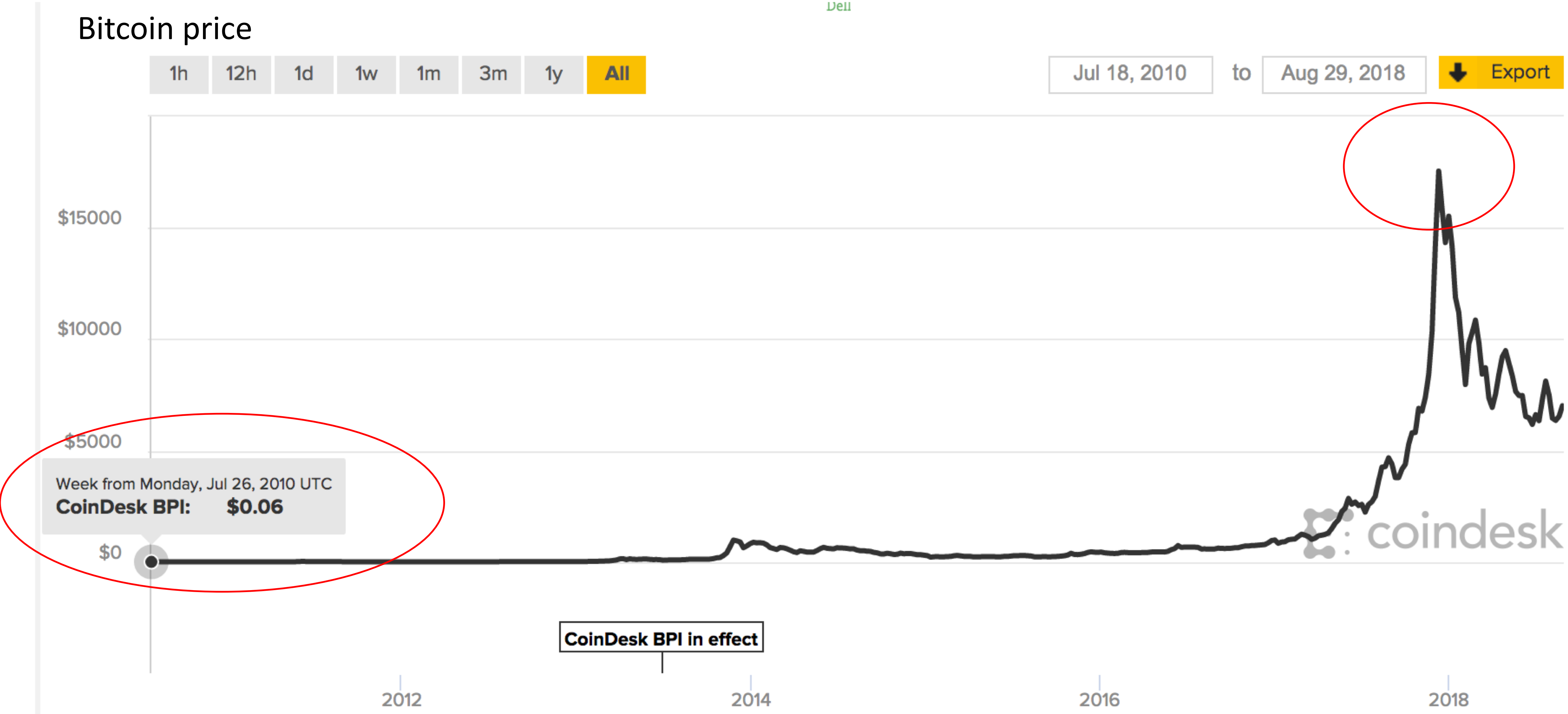
Your LinkedIn accaunt was suspended due to spam messages. To unlock your account open this link www.llinked.ni a

Thank you for using LinkedIn!

The LinkedIn Team

Security Technology Is Money Sometimes

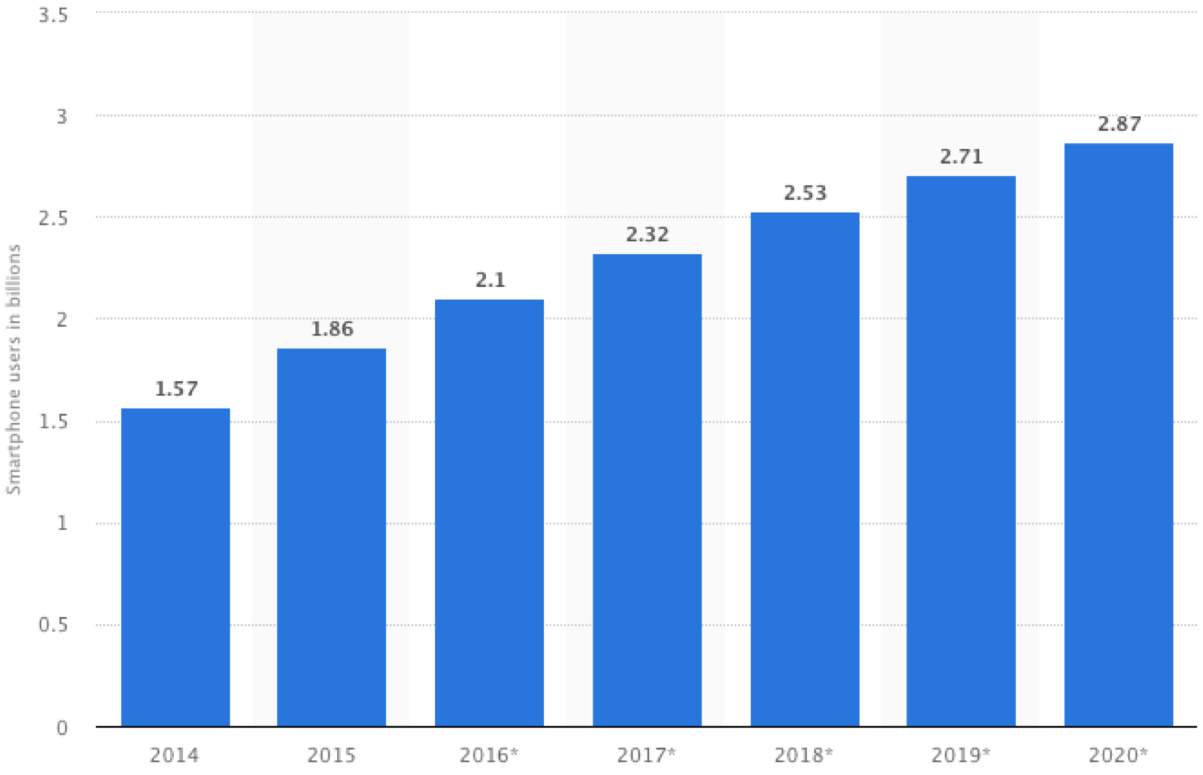
Bitcoin price



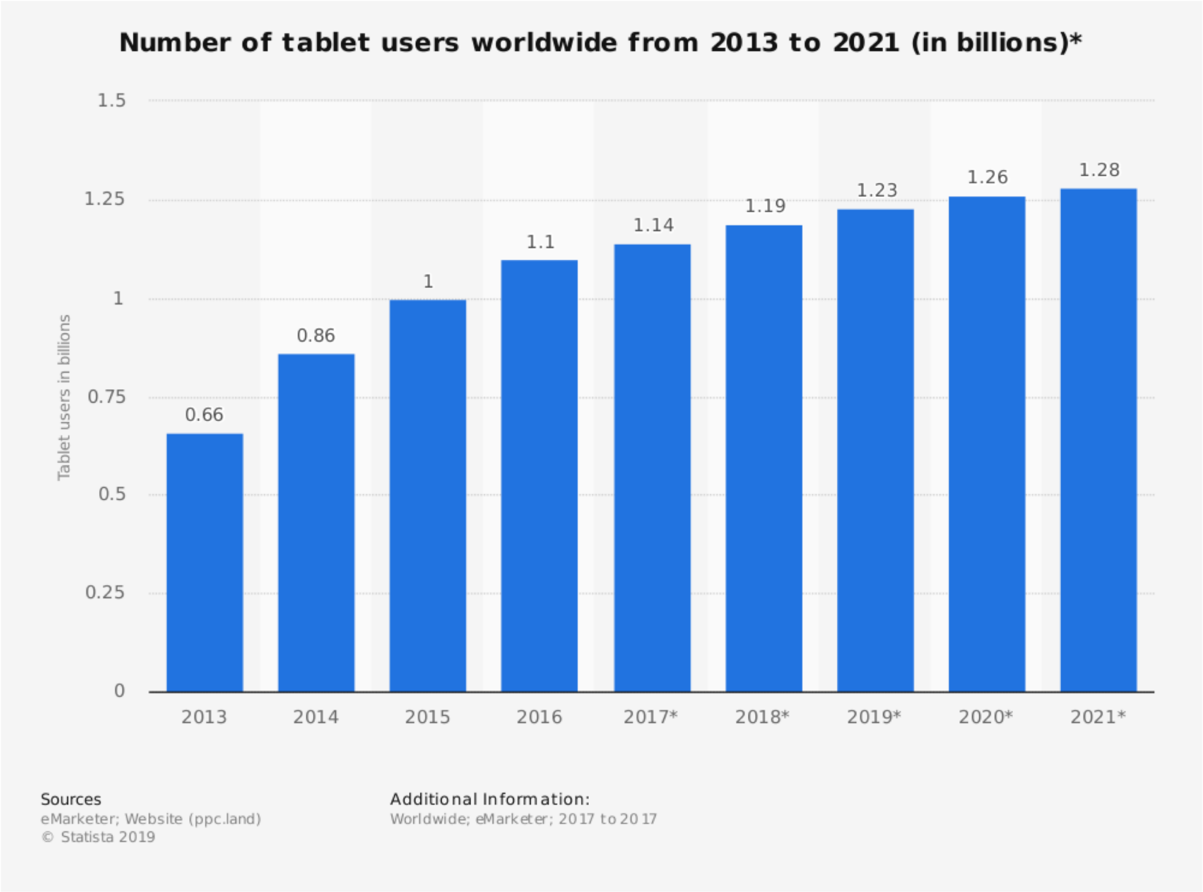
Week from Monday, Jul 26, 2010 UTC
CoinDesk BPI: $0.06

Mobile Devices and Flash Memory

Mobile Devices are Turning to Mainstream Computing Devices



Number of smartphone users worldwide from 2014 to 2020 (in billions)



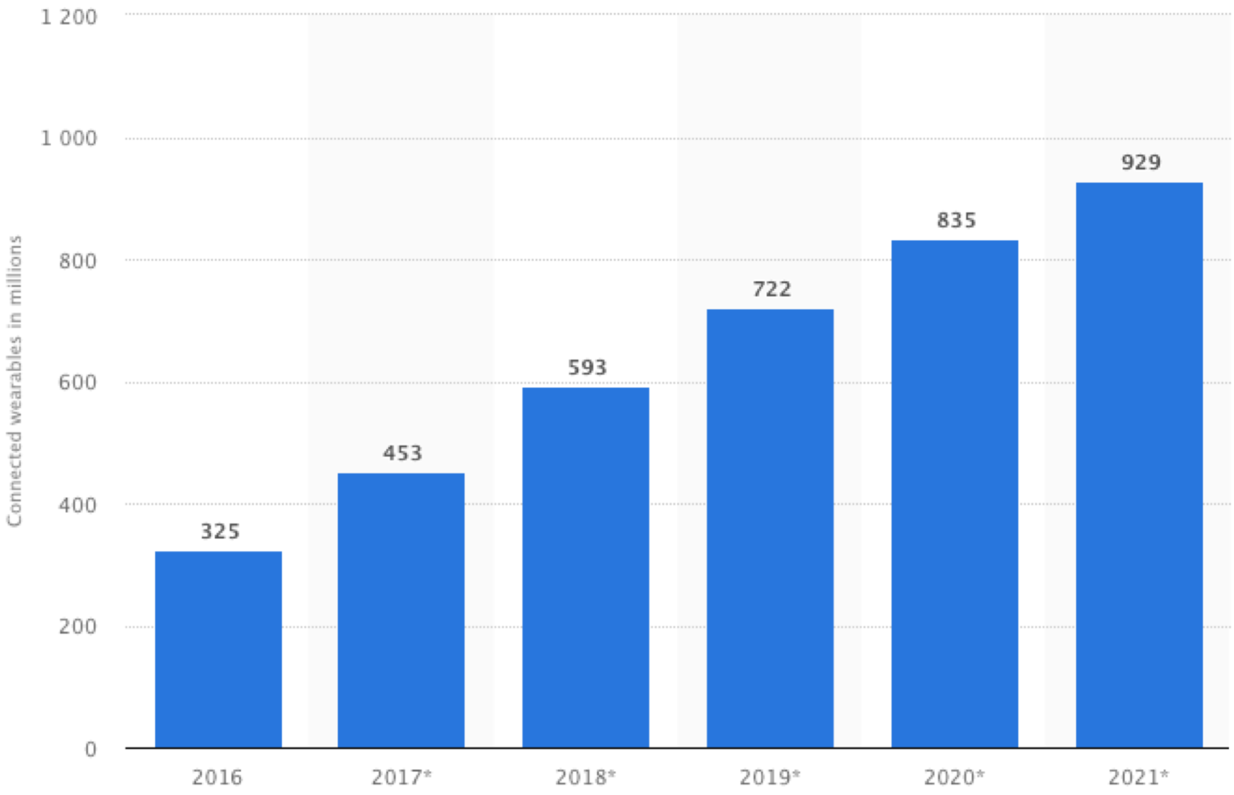
Number of tablet users worldwide from 2013 to 2021 (in billions)*

Sources
eMarketer; Website (ppc.land)
© Statista 2019

Additional Information:
Worldwide; eMarketer; 2017 to 2017

Number of tablet users worldwide from 2013 to 2021 (in billions)

Mobile Devices are Turning to Mainstream Computing Devices (cont.)



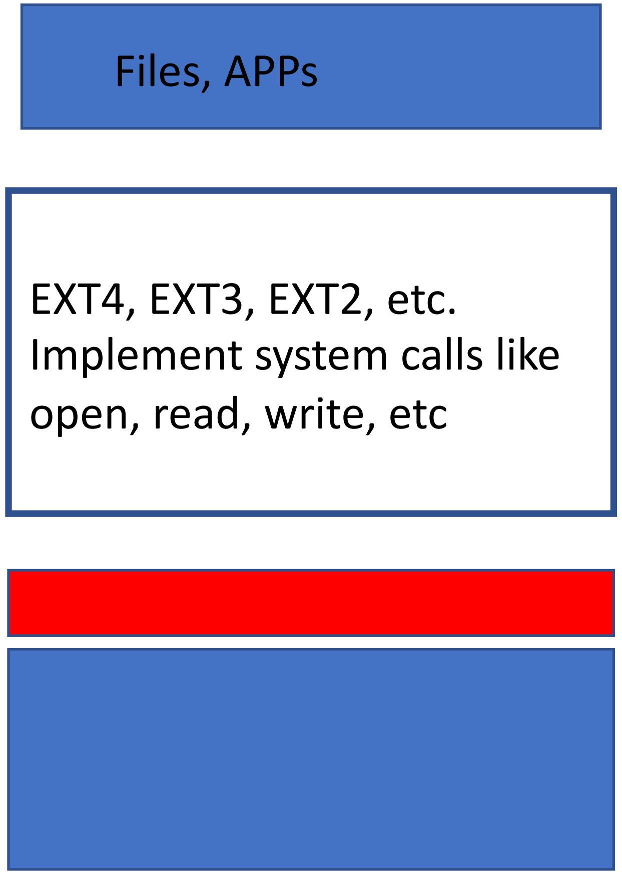
Number of connected wearable devices worldwide from 2016 to 2021 (in millions)

Mobile Devices are Used for Critical Applications

- Mobile devices are increasingly used to handle sensitive data
  - Online banking
  - Ecommerce
  - Cryptocurrency/stock trading
  - Naked photos
  - A human rights worker collects evidence of atrocities in a region of oppression
  - Etc.

- Security issues in mobile computing devices
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
  - …

A Common Storage System of a Mobile Device



Applications layer

Files, APPs

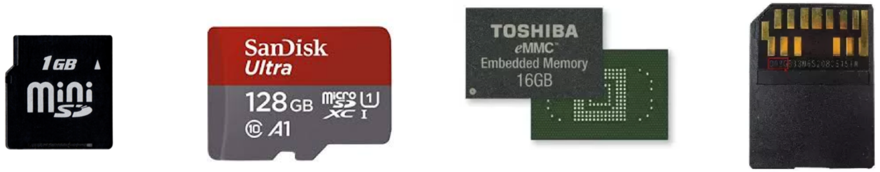
Mobile file system layer

EXT4, EXT3, EXT2, etc.
Implement system calls like open, read, write, etc

Manage the mappings between the applications' view and the block device's view

Block device layer

Flash memory layer



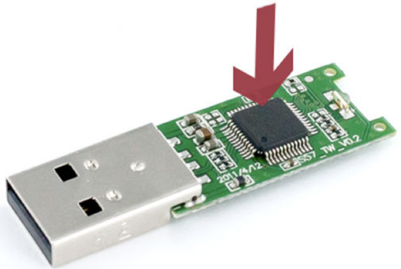
eMMC Chip

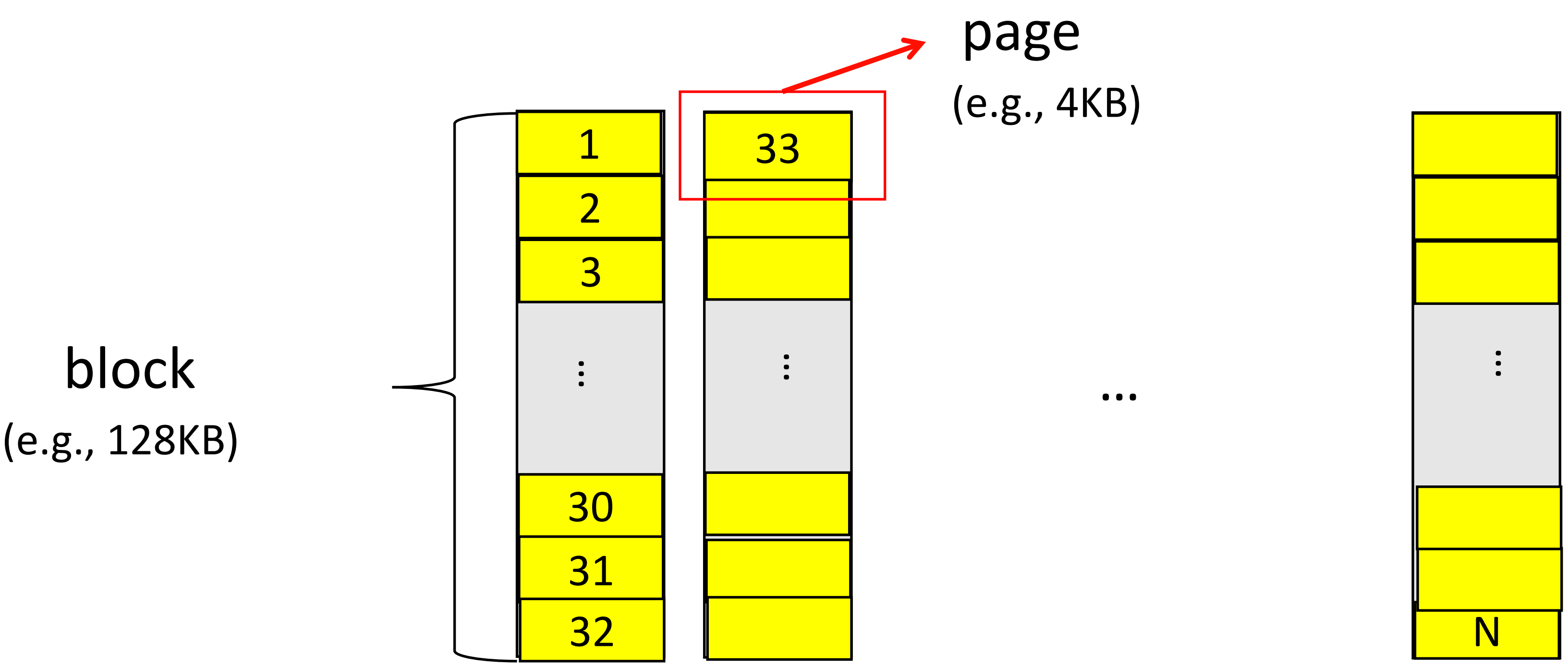
MMC Card

Flash Memory Security Research

NAND Flash is Usually Used as Storage Media

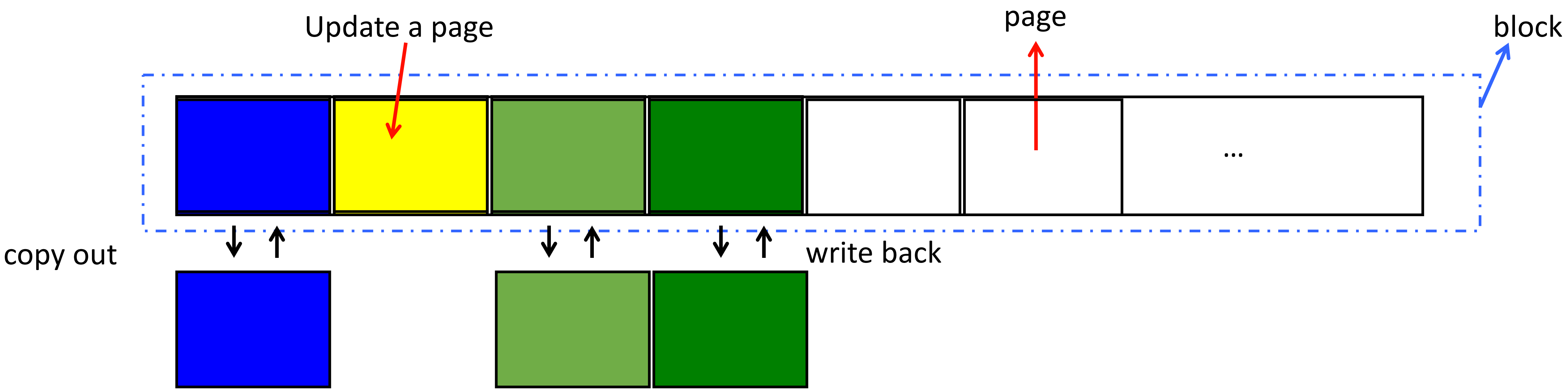
- NAND flash
  - USB sticks
  - Solid state drives (SSD)
  - SD/miniSD/microSD/eMMC





Special Characteristics of NAND Flash

- Update unfriendly
  - Over-writing a page requires first erasing the entire block
  - Write is performed in pages (e.g., 4KB), but erase is performed in blocks (e.g., 128KB)



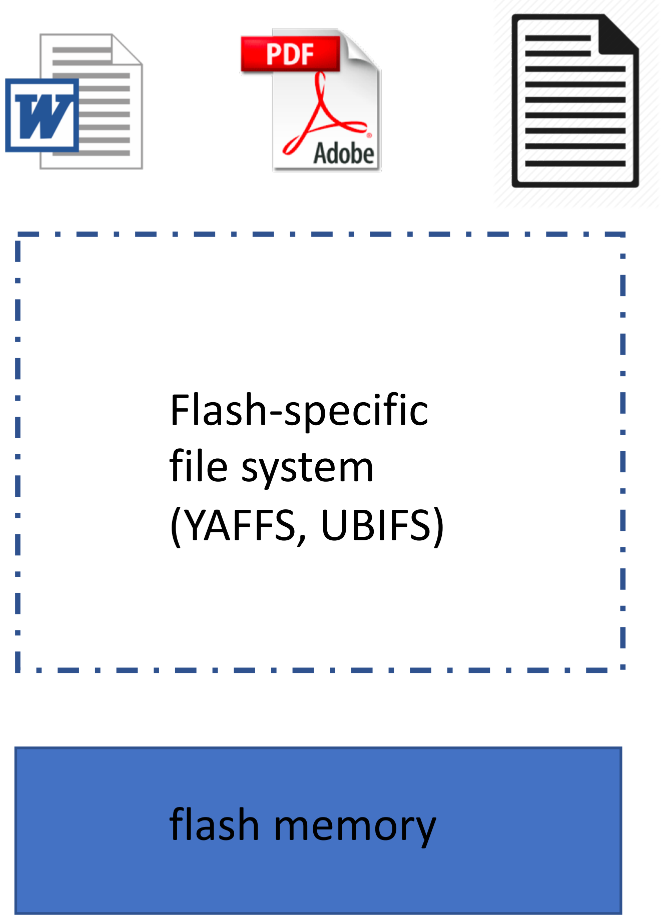
  - Over-write may cause significant write amplification

Special Characteristics of NAND Flash (cont.)

- Support a finite number of program-erase (P/E) cycles
  - Each flash block can only be programmed/erased for a limited number of times (e.g., 10K)
  - Data should be placed evenly across flash (wear leveling)

How to Manage NAND Flash

- Flash-specific file systems, which can handle the special characteristics of NDND flash
  - YAFFS/YAFFS2, UBIFS, F2FS, JFFS/JFFS2
  - Less popular

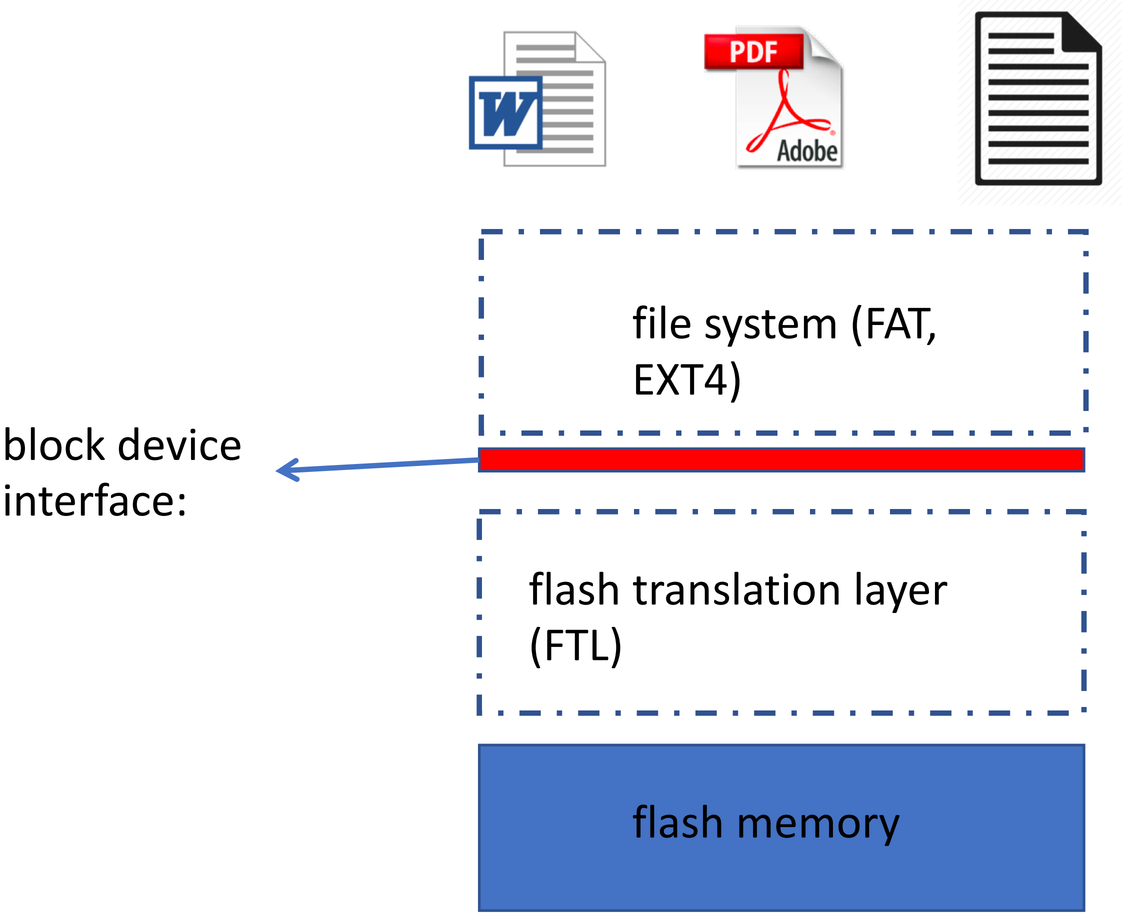


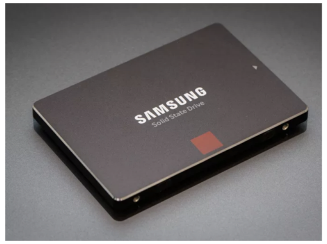
Flash-specific file system (YAFFS, UBIFS)

flash memory

How to Manage NAND Flash (cont.)

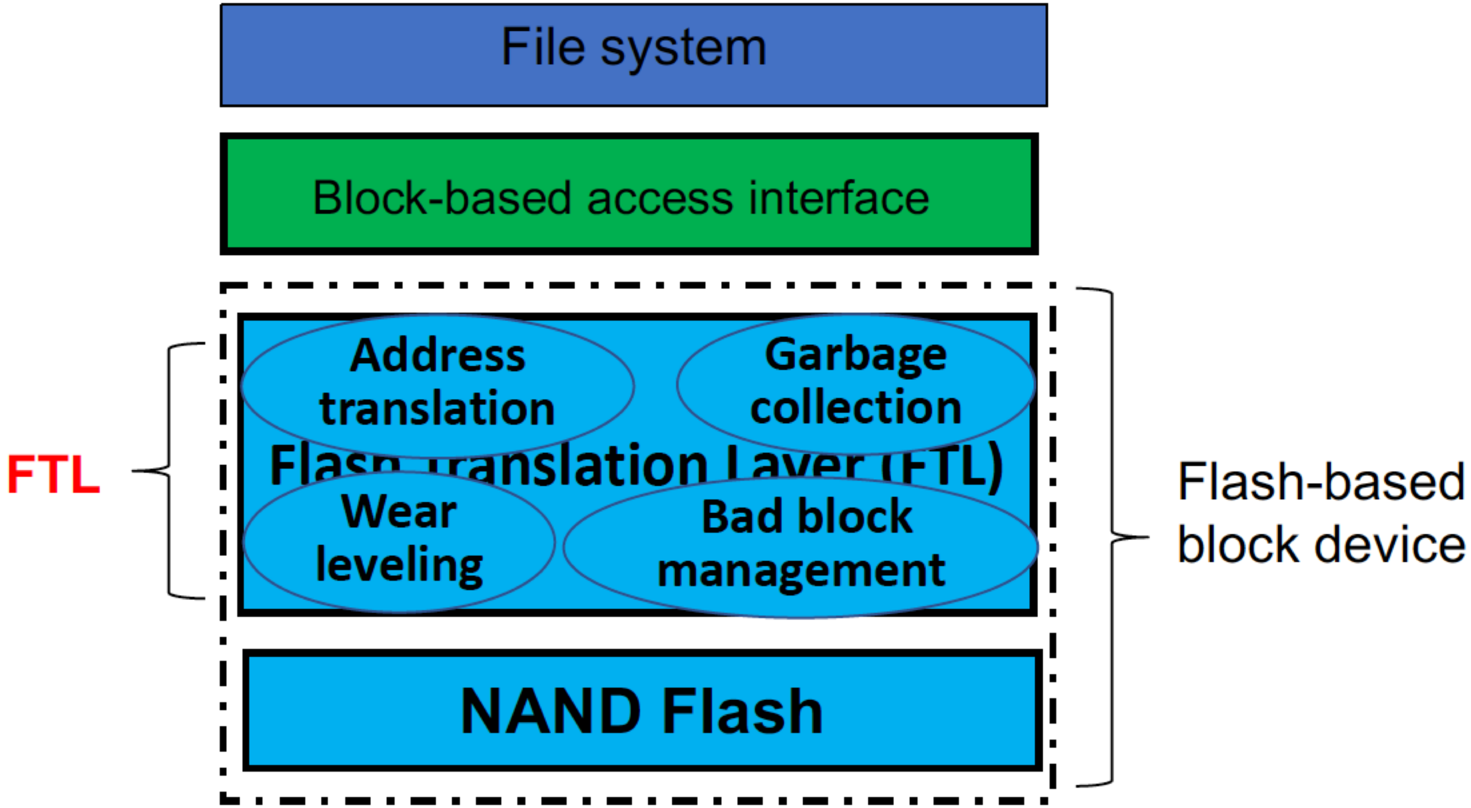
- Flash translation layer (FTL) – a piece of flash firmware embedded into the flash storage device, which can handle the special characteristics of NAND flash and emulate the flash storage as a regular block device (most popular)
    - SSD
    - USB
    - SD





Flash Translation Layer (FTL)

- FTL usually provides the following functionality:
  - Address translation
  - Garbage collection
  - Wear leveling
  - Bad block management

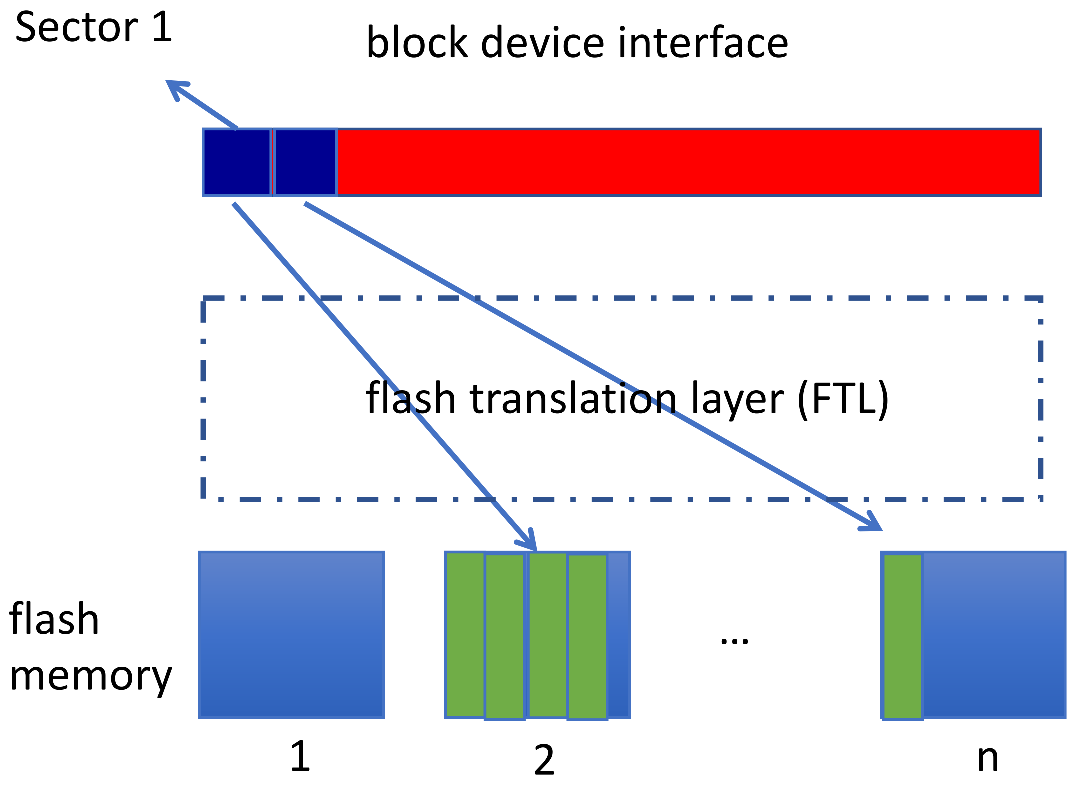


Flash Translation Layer (cont.)

- Address translation
  - Translate address between block addresses and flash memory addresses
  - Need to keep track of mappings between Logical Block Address (LBA) and Physical Block Address (PBA)

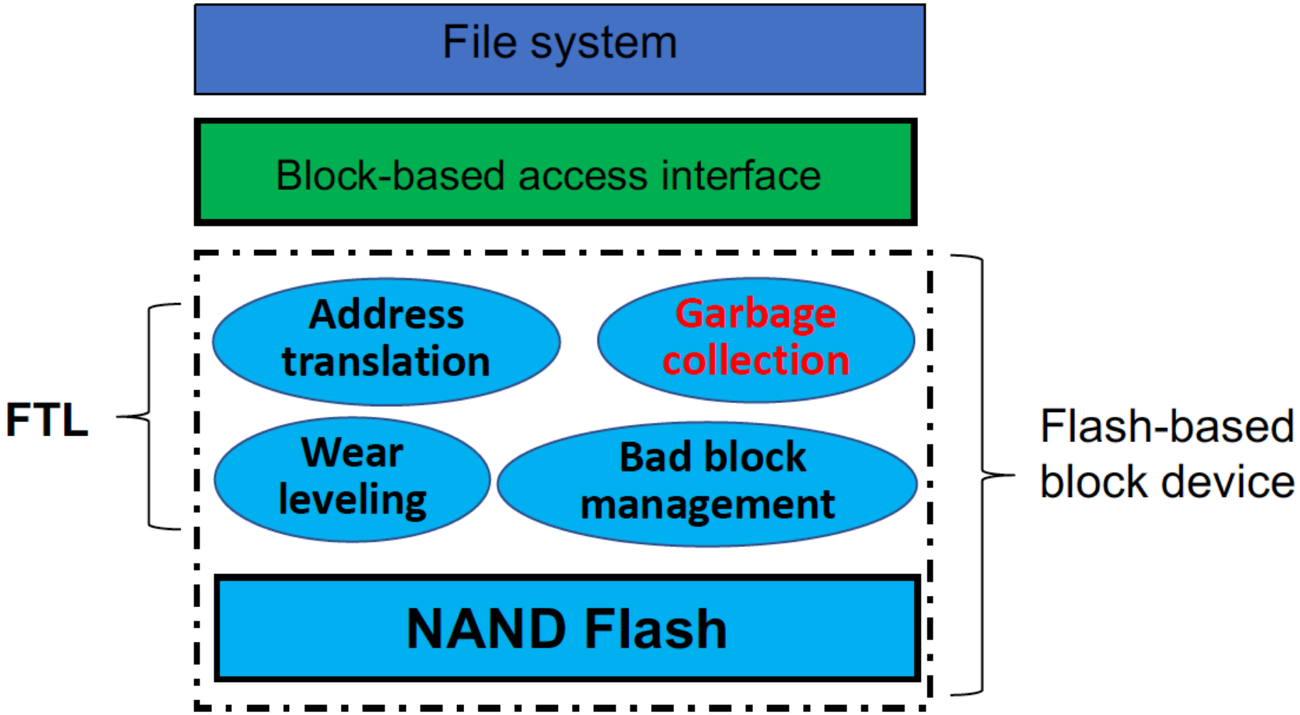
FTL should maintain a mapping table

Block device location	Flash location
Sector 1	(2,3)
Sector 2	(n,1)



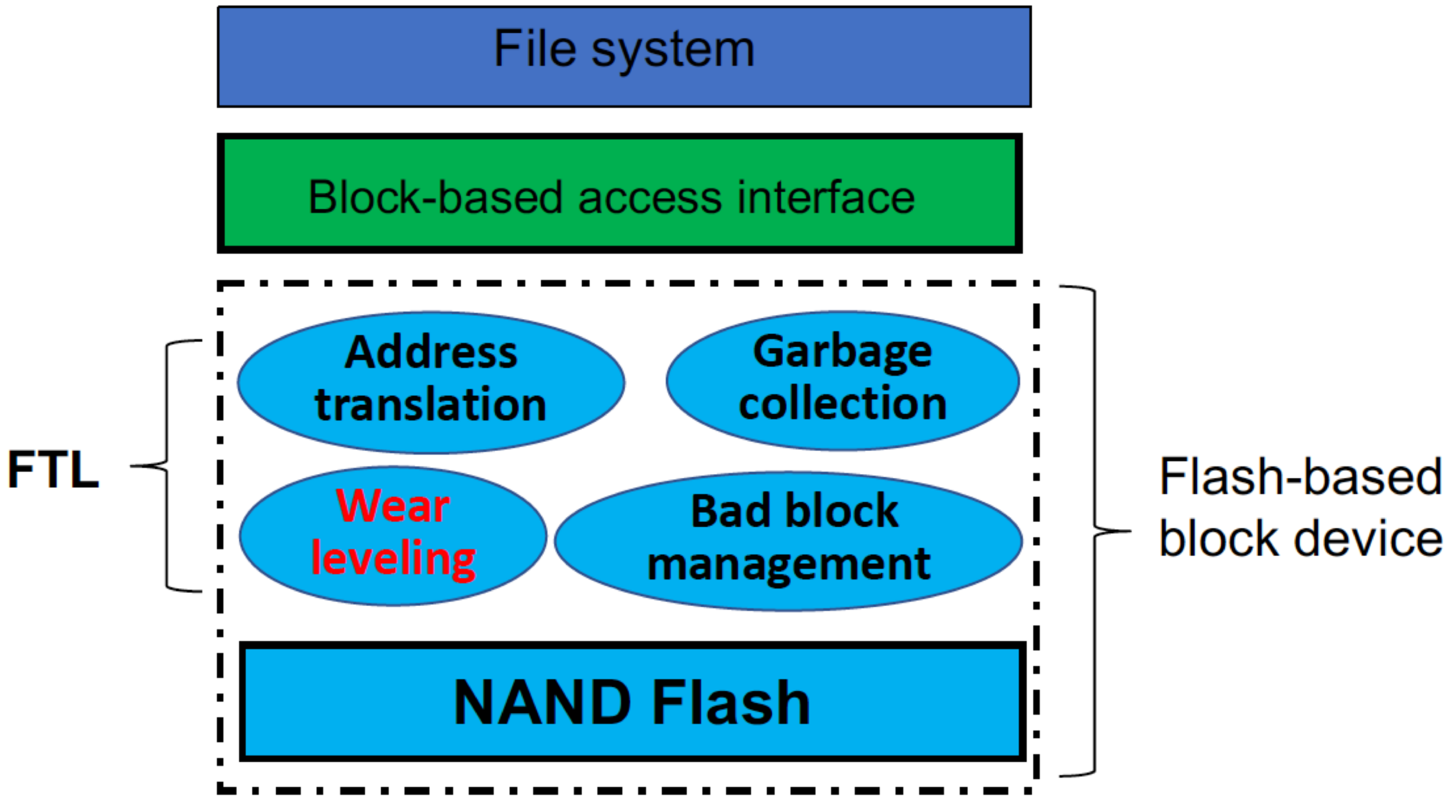
Flash Translation Layer (cont.)

- Garbage collection
  - Flash memory is update unfriendly
  - Not prefer in-place update, but prefer out-of-place update
  - The blocks storing obsolete data should be reclaimed periodically by garbage collection



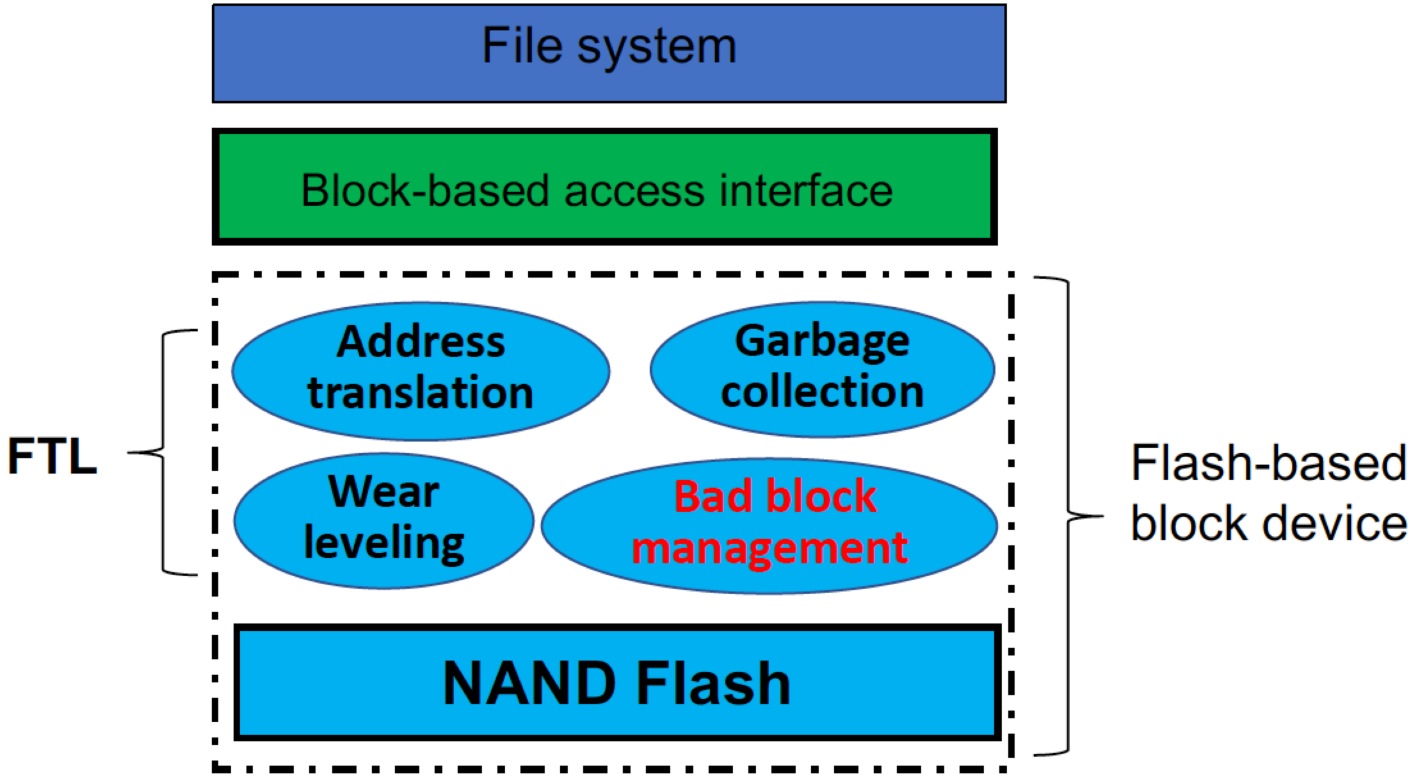
Flash Translation Layer (cont.)

- Wear leveling
  - Each flash block can be programmed/erased for a limited number of times
  - Distribute writes evenly across the flash to prolong its lifetime



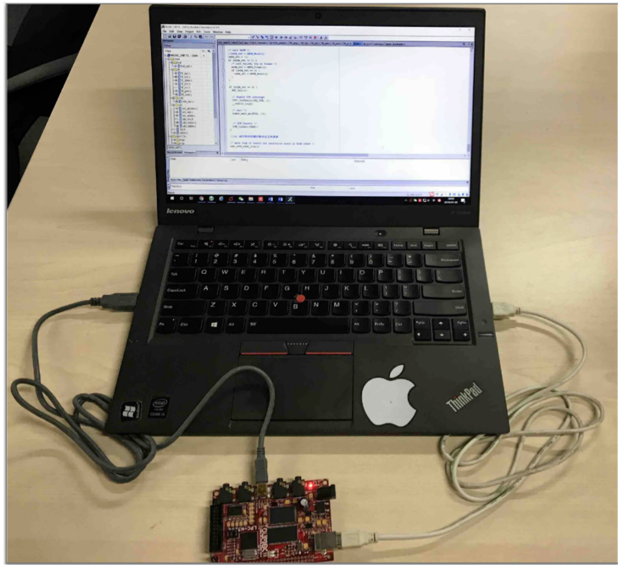
Flash Translation Layer (cont.)

- Bad block management
  - Regardless how good is the wear leveling, some flash blocks will eventually turn “bad” and cannot reliably store data
  - Bad block management is to manage these bad blocks



A Testbed for Flash Memory Security Research

- We have a flash memory testbed in MTU Security and Privacy (SnP) Lab. The lab is located in Rekhi 318

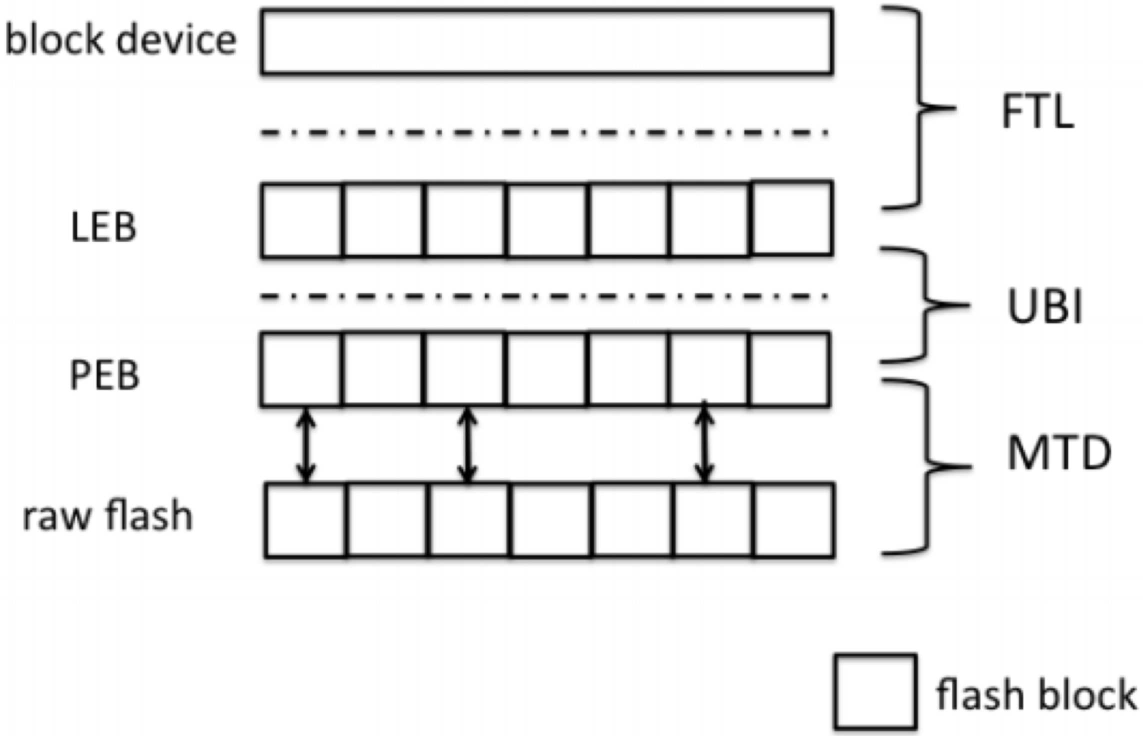


- The testbed includes:
  - Open-source flash firmware: OpenNFM
    - Implement flash translation layer (FTL) which is used to manage raw NAND flash, and provide a block access interface to upper layer
  - Embedded development environment: IAR Embedded Workbench
  - Electronic board: LPC-H3131

A Demo of Flash Memory Testbed

- A demo by Niusen
  - Cross-compile opensource flash firmware OpenNFM using : IAR Embedded Workbench
  - Flash the binary to the electronic board LPC-H3131
  - Use the electronic board as a USB device (YOU CAN MAKE YOUR OWN USB DEVICE NOW)
  - Test throughput using benchmark tool **fio**

Opensource Flash Firmware OpenNFM



OpenNFM - MTD

- MTD: built on top of raw flash, and mainly provides three uniform APIs to allow the UBI to read, write and erase raw flash
  - MTD_Read(PEB index, offset, &data): read data from a PEB page identified by PEB index and offset
  - MTD_Write(PEB index, offset, data): write data to a PEB page identified by PEB index and offset
  - MTD_Erase(PEB index): erase the PEB identified by PEB index

OpenNFM - UBI

- UBI: built on top of MTD, and uses the APIs provided by MTD to read/write PEB pages or erase PEB blocks. Implement wear leveling, garbage collection, bad block management
  - UBI_Read(LEB index, offset, &data): read data from an LEB page identified by LEB index and offset
  - UBI_Write(LEB index, offset, data): write data to an LEB page identified by LEB index and offset
  - UBI_Erase(LEB index): erase an LEB identified by LEB index, which will cause an erasure over the corresponding PEB

OpenNFM - FTL

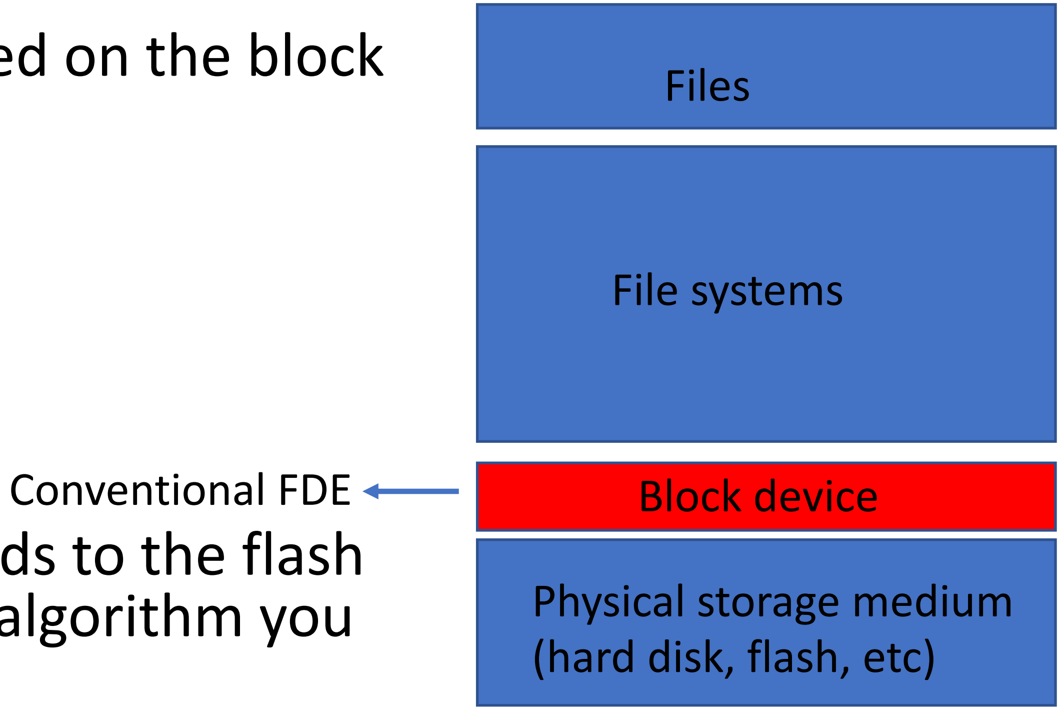
- FTL: build on top of UBI, and use the APIs provided by UBI to read/write LEB pages or erase LEBs. Implement address translation
    - FTL_Read(block_address, &data)
    - FTL_Write(block_address, data)

Our Tasks

- Get familiar with the embedded development environment
- Play with the source code of flash firmware OpenNFM
- Pick a task in the following to gain some hands-on experience on programming flash memory
  - Task 1: data confidentiality in flash memory
  - Task 2: data integrity in flash memory

Task 1 - Data Confidentiality in Flash Memory

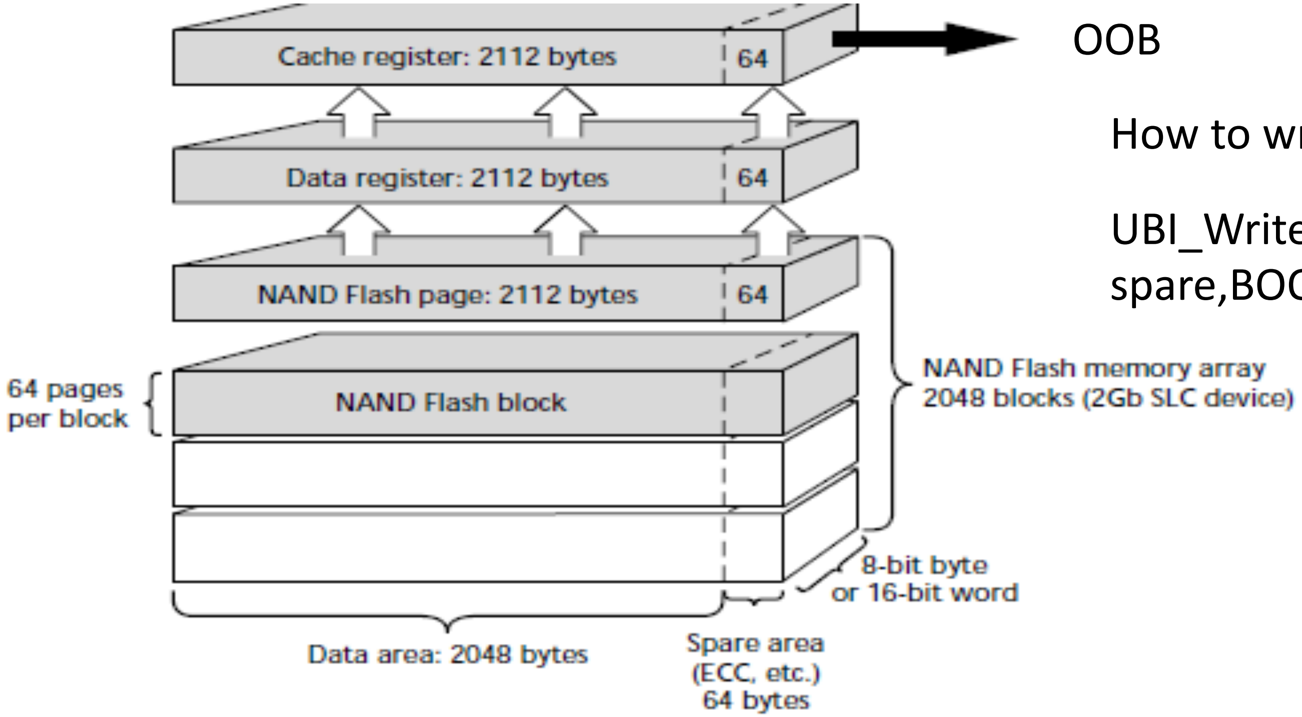
- Conventional full disk encryption (FDE) is incorporated on the block layer to transparently ensure data confidentiality
  - BitLocker (Windows)
  - FileVault (MAC OS X)
  - Android FDE
  - TrueCrypt/VeraCrypt



- We will move the FDE from the block layer downwards to the flash memory layer (implement an symmetric encryption algorithm you like)
  - Write a flash page, encrypt it
  - Read a flash page, decrypt it using the same key
  - Encryption/Decryption is completely transparent to users
  - Test the throughput using benchmark tool fio, compare the throughput with original OpenNFM firmware
- (Optional) How can the system protect the encryption key?

Task 2 - Data Integrity in Flash Memory

- Every flash page (e.g., 2KB) has an out-of-band (OOB) area (e.g., 64 bytes). Therefore, you can create an integrity verification tag for the data of each flash page, and store the tag code to the OOB. Each time when you read a flash page, you can also read the corresponding tag, and check whether the data have been corrupted or not


Cache register: 2112 bytes
64
Data register: 2112 bytes
64
NAND Flash page: 2112 bytes
64
64 pages per block
NAND Flash block
NAND Flash memory array 2048 blocks (2Gb SLC device)
8-bit byte or 16-bit word
Data area: 2048 bytes
Spare area (ECC, etc.) 64 bytes

OOB

How to write OOB area in OpenNFM?

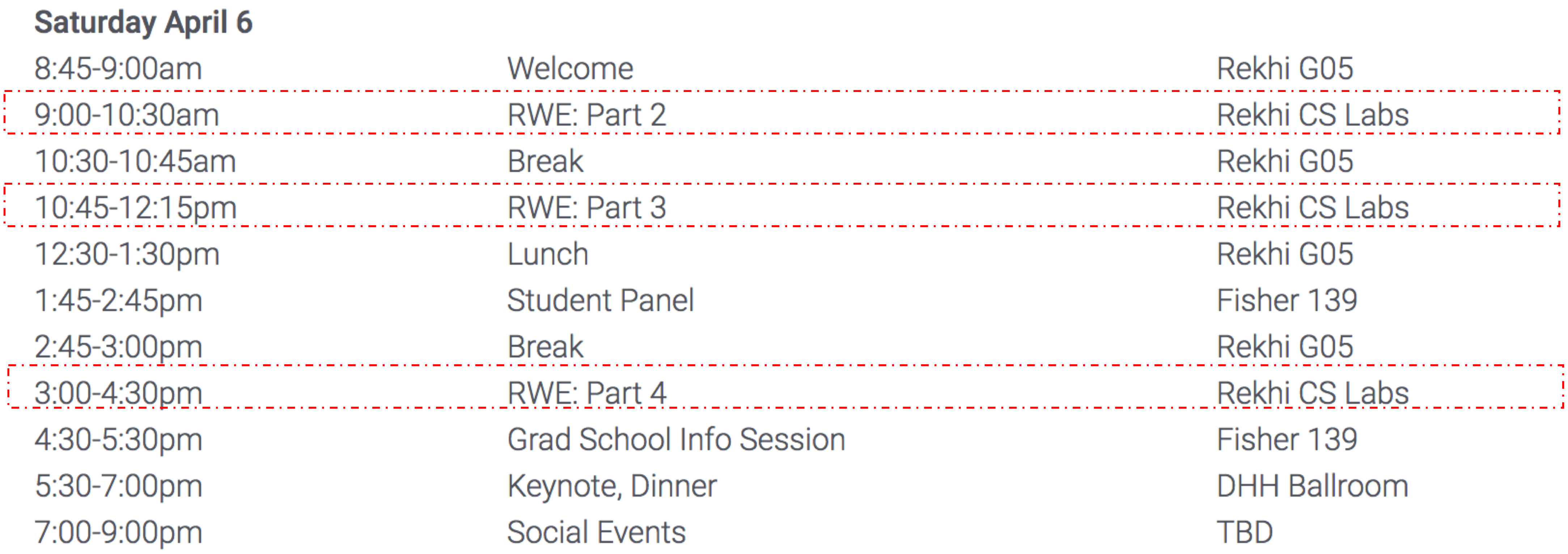
UBI_Write(LOG_BLOCK block, PAGE_OFF page, void* buffer, SPARE spare,BOOL async)

Task 2 - Data Integrity in Flash Memory (cont.)

- Use the following algorithm to detect data corruptions in flash memory (design and implement our own tag generation algorithm)
  - When writing a flash page, generate an integrity verification tag, and store it to the OOB area
  - When reading a flash page, read both the data and the tag, and recompute a new tag for the data, and compare it with the stored tag
  - Test the throughput using benchmark tool fio, and compare the throughput with original OpenNFM firmware
- (optional) Make the project a little more interesting
  - What if I need to recover the corrupted data? You may try error correcting code

Next …

- Location: **Rekhi 318**

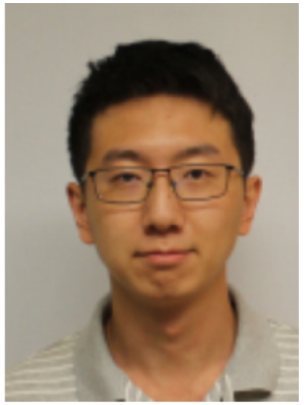


Saturday April 6

8:45-9:00am	Welcome	Rekhi G05
9:00-10:30am	RWE: Part 2	Rekhi CS Labs
10:30-10:45am	Break	Rekhi G05
10:45-12:15pm	RWE: Part 3	Rekhi CS Labs
12:30-1:30pm	Lunch	Rekhi G05
1:45-2:45pm	Student Panel	Fisher 139
2:45-3:00pm	Break	Rekhi G05
3:00-4:30pm	RWE: Part 4	Rekhi CS Labs
4:30-5:30pm	Grad School Info Session	Fisher 139
5:30-7:00pm	Keynote, Dinner	DHH Ballroom
7:00-9:00pm	Social Events	TBD

Next …

- Two graduate students from Security and Privay (SnP) Lab will be there for help



- You need to talk about your project on Sunday (April 7)

- Therefore, you may start to summarize your project and prepare a few slides for presentation in the afternoon of April 6 (in a group)
  - Confidentiality group
  - Integrity group

Enjoy Your Short Journey in Flash Memory Security Research!!!