CyberSecurity Topics of Today!

Debasis Bhattacharya, JD, DBA
University of Hawaii Maui College
debasisb@Hawaii.edu
@uhmcabit
maui.hawaii.edu/cybersecurity
Open Source Intelligence and Research Association (OSIRA) Code of Ethics

1. Responsibility
   • Take responsibility for your actions.

2. Professionalism
   • Always continue to learn and strive for moral high ground.

3. Credibility
   • Be objective and verify the credibility of sources/accuracy of information.

4. Personal Example
   • Be a role model to others by displaying honesty, integrity, and selflessness.

5. Sense of Mission
   • Advance OSIRA and uphold professionalism.

6. Comradeship
   • Help out other OSINT researchers.
Ethical Issues

- Disinformation
- Accuracy
- Credibility
- Reliability
- Abuse of Power
  - Integrity
- Exploitation
- Privacy
- Aggregation
  - Confidential and Classified Data/Info

Cambridge Analytica whistleblower: Data could have come from more than 87 million users, be stored in Russia

By Caroline Kelly
Updated 4:43 PM ET, Sun April 8, 2018
Privacy and Social Media

• Privacy Arguments
  • Pro:
    • “I have nothing to hide.”
  • Con:
    • Those stories we don’t want our bosses knowing about...
Why is social media a prime OSINT tools?

- Contain FREELY given personal information about ANY target that has social media
- Not violating any privacy laws (so no jail time!)
- One of the best resources for gathering intelligence about target
- Easily enables us to build a profile on a target
Brandy Vela

- On November 29, 2016, Brandy committed suicide after online bullying through social media accounts escalated.

- Individuals would create fake profiles and write her cruel messages. In addition, individuals would post her phone number online with solicitations for "free sex."

https://www.youtube.com/watch?v=TAfjxPEnDVM
The Quest for Approval...
Social Media Platforms

• Facebook
• Twitter
• LinkedIn
• Snapchat
• Instagram
• Dating Sites
• Periscope
• Pinterest
• Youtube
• Reddit
Facebook

• Connects millions of people...which can help us build a persons network

• Information is often a little more secure thanks to FB new privacy settings

• However...we can still get a lot of information (and we can always get the information they have private)
Data Policy

• What kinds of information does Facebook collect?
  • Things you do and the info you provide.
  • Things others do and the info they provide.
  • Your networks and connections.
  • Information about payments.
  • Device Information
  • Information from websites and apps that use FB.
  • Information from 3rd party partners
  • Facebook companies.

• How is this information shared?
  • People you share and communicate with.
  • People that see content others share about you.
  • Apps, websites, and 3rd party integrations on or using FB.
  • Sharing within Facebook Companies.
  • New Owner.
  • Advertising, Measurement, and Analytics Services (Non PII only)
  • Vendors, service providers, and other partners.
Facebook Services

• Information
  • No, we don't sell any of your information to anyone and we never will.

• Fake Accounts
  • A fake account is an account where someone is not representing their authentic self. Fake accounts can include accounts for fake or made up people, pets, celebrities, or organizations.

• Friending
  • You can add a friend by searching for them and sending them a friend request. If they accept, you automatically follow that person, and they automatically follow you — which means that you may see each other's posts in News Feed. If you'd like to see updates from people you find interesting but don't know personally, like a journalist or celebrity, try following them instead.
How do I find people on Facebook?

- Facebook friend finder
- Typing the person's name directly into the search bar
- Using URL: https://www.facebook.com/search/top/?q=Firstname%20Lastname
- Example: https://www.facebook.com/search/top/?q=Debasis%20Bhattacharya
Information Gathering: Facebook

- Birthday
- Age
- Gender
- Work Background
- Location
- Family Members
- Relationship Status
- Interests/ Likes
- Education
- Photos
- Geolocation Information
- User Network
- Details about user
- Life Events
- Phone Numbers
- Email
Employment and Employees Search using Facebook URLs

- Current/Past Employees
Location Search Using Facebook URLs

- https://www.facebook.com/search/str/hawaii/pages-named/residents/present
- https://www.facebook.com/search/people/?q=bhattacharya%20hawaii
- https://www.facebook.com/search/people/?q=bhattacharya%20hawaii%20faculty
Age Search based on Facebook URLs

- People called “Bhattacharya” between ages 30 and 60
  - https://www.facebook.com/search/str/bhattacharya/users-named/str/30/60/users-age-2/intersect

- People called “Bhattacharya” between 30 and 60 and who live in Hawaii

- People who are 22 years old named "John Smith"

- People named "Tim Smith" who were born between 1990 and 1999
Likes Search using Facebook URLs

- https://www.facebook.com/search/people/?q=vegas%20hawaii%20kimo
Places Visited, Language, and Gender: Merrie Monarch FB

- Places Visited - https://www.facebook.com/Merrie-Monarch-Festival-185599409199/

- Language

- Gender
Types of Searches that we conducted

• People Named
• People who work/worked at ___
• People who like ___
• People who live in _____
• People who visited___
• School attended___

• People named ____ and like ___
• People who live in ___ and like ___

• Etc...
Searching for an email and telephone numbers on Facebook

- We can also use Facebook to find and confirm emails and telephone numbers.
- Type in the targets name into forgot password.
- Then find the targets profile.
- It will tell you the email service as well as the first and last letter of the email.
- In many cases, we can reverse engineer or guess the email.
- Can also tell us the last 2 digits of the phone number. Some sites, like people finder, will give us 7 and if we have the last 2, that means we are only missing 1 number.
Finding a users Facebook ID....

- **Number of ways**
  - Go to profile, go to *About* tab
  - Look in Facebook URL for the contents between `%3APROFILE_ID%3A`
  - https://www.facebook.com/debasisb/about?lst=1068624025%3A1068624025%3A1523237261
- https://www.facebook.com/search/profileID/places-visited
- https://www.facebook.com/search/profileID/places-liked
- https://www.facebook.com/search/profileID/pages-liked
- https://www.facebook.com/search/profileID/photos-by
- https://www.facebook.com/search/profileID/photos-of
- https://www.facebook.com/search/profileID/photos-commented
- https://www.facebook.com/search/profileID/videos
- https://www.facebook.com/search/profileID/videos-of
- https://www.facebook.com/search/profileID/videos-liked
- https://www.facebook.com/search/profileID/videos-commented
- https://www.facebook.com/search/profileID/apps-used
- https://www.facebook.com/search/profileID/friends
- https://www.facebook.com/search/profileID/events
- https://www.facebook.com/search/profileID/events-joined
- https://www.facebook.com/search/profileID/stories-by
- https://www.facebook.com/search/profileID/stories-commented
- https://www.facebook.com/search/profileID/stories-tagged
- https://www.facebook.com/search/profileID/groups
- https://www.facebook.com/search/profileID/relatives
Common Results

How I’ve used Twitter...

• Twitter can be a great place to find additional information about our target.

• However, it should be noted that often times, twitter users can be a little bit more complex to find because users are allowed to change his/her twitter handle.

• There are additional trips and tricks to searching twitter, such as using twitter’s advanced search options.

• You can even type in the target’s full name on google and a location +twitter and you might be able to get a match.

• In addition, we can also find targets sometimes through the analysis of hashtags.
Prophet

- Monitors the social networks that are associated with an individual
- Individual must use that social networking site in conjunction with multiple sites
- Can see social profiles associated with account, as well as websites and lists...
- Works well with twitter, facebook, linkedin, and google+
How I’ve used Instagram...

• Find targets Instagram
• Find all prior names on Instagram with Google
• Helped me find connections to a secondary hidden Facebook account
• Helped me find more information on targets location and interests.
How I’ve used LinkedIn....

• Great for finding past employment
• Also great for finding professional connections
• Can get a lot of information from LinkedIn
  • Educational History
  • Work History
  • Volunteer work
  • Publications
  • Likes/Dislikes
  • Certifications, etc.
  • Emails/Contact Information...
A word on protecting your privacy...

- Always use the strictest privacy settings
- Never...EVER...geotag (and if possible, don’t let anyone else geotag you)
- Keeps likes/interests to yourself
- Do not make connections public
- Limit photographs made public
- Know that when you post on public pages...those can be seen by others
- Know that old posts are archived and can be viewed again...especially if they were public
Spotting a fictitious profile...

- Account was made recently 2015, 2016, 2017.
- Account has no history published for earlier years, but Facebook says they have been a member since 2009, etc.
- Most fake accounts have 1 image or no real profile photo of the person. Some may only have a select few photos over a long span of time. A well seasoned user would have more photos posted over a long period of time. A fake account may have 7-10 photos posted on the same day.
- User has very few friends in common and or friends in general.
- There is little to no interaction on their page with friends, no comments, likes or responses over their long time line.
- Profile picture seems to good to be true, that hot model added you today! They even messaged you and are interested in you!
- When in doubt use reverse image search. Take their image and see if it is a real person or not.
- When in doubt deny, deny, deny.
**Mobile device forensics** is a branch of digital forensics relating to recovery of digital evidence or data from a mobile device under forensically sound conditions.

Information of Interest in Mobile Devices:
- Pictures
- Text Messages
- Files
- Location Information
- Ownership of phone
- Search history from phone browser
- Music
- Videos
- Other information

Mobile Data is stored in the device:
- SIM Card
- Storage Card
- Device Memory

Copies of Mobile Data is also stored in:
- Cell Towers
- Cloud Providers (Google, Apple, Verizon)
- Phone Company Providers (Verizon, AT&T)
Phone Tracking – IMEI or MEID #

1. Dial *#06# to see your device IMEI

www.imei.info

BEST WAY TO GET TO KNOW
YOUR PHONE BETTER

Every mobile phone, GSM modem or device with a built-in phone / modem has a unique 15 digit IMEI number. Based on this number, you can check some information about the device, eg brand or model. Enter the IMEI number below:

358035080253937

CHECK
### Model:
Pixel XL 2

### Brand:
GOOGLE

### IMEI:
TAC: 358035 FAC: 08 SNR: 025393 CD: 7

---

**Tempe PD's 'Stingray' tracking tool raising concerns, police weigh in**

**BY:** Nick Cicetti  
**POSTED:** 10:32 PM, Apr 6, 2018  
**UPDATED:** 3:14 PM, Apr 7, 2018
Thank you for downloading FTK® Imager 3.4.3. If you have any questions or are interested in getting the full version of FTK, please email us at sales@accessdata.com.

**Download FTK Imager 3.4.3**

For instructions on how to use, view the eForensics Magazine "FTK Imager Step by Step" issue for step by step instructions or the FTK User Guide.

After you create an image of the data with FTK Imager, you can use AccessData® Forensic Toolkit® (FTK®) to perform a thorough analysis and create a report of your findings. For information about using FTK® in the world as the standard in computer forensic software, visit https://www.sleuthkit.org/autopsy/
Securing Cell Phones

• Lock your phone with password, fingerprint or pattern
• Encrypt your data
• Setup remote wipe
• Backup your phone data to the cloud
• Install secure third-party apps
• Avoid jailbreaking your phone
• Be wary of social engineering scams, phishing, malicious links etc.
• Public wifi is inherently insecure, avoid banking or sensitive transactions
• Download anti-malware for your phone
Currencies - Online Transactions

- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation

- Fiat Currency – legal tender whose value is backed by a government
  - Note that since 1971, the US$ has no backing with gold!
  - Cryptocurrencies are not fiat currencies!

- Physical currencies can’t be used online directly

  ➢ Electronic credit or debit transactions
    ◆ Bank sees all transactions
    ◆ Merchants can track/profile customers
    ◆ Cryptocurrencies are not associated with any bank or regulatory agency!
Bitcoin

• A distributed, decentralized digital currency system
• Released by Satoshi Nakamoto 2008
• Effectively a bank run by an ad hoc network
  • Digital checks
  • A distributed transaction log
Size of the BitCoin Economy

• Number of BitCoins in circulation ~17 million (April 8, 2018)
• Total number of BitCoins generated cannot exceed 21 million.
  • Around 4 million left to be mined!

• Average price of a Bitcoin:
  • $7,149 in April 8, 2018
  • $18,000 in December, 2017
  • $3,867 on September 25, 2017;
  • $2,350 on June 27, 2017
  □ Price has been very unstable and speculative.

• Currently, 244,157 tx/day or ~170 tx/minute.
  (In contrast, Visa transaction 200,000 per minute!)
<table>
<thead>
<tr>
<th>POPULAR STATS</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Price (USD)</td>
<td>$7,107.74</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average Block Size</td>
<td>0.43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transactions per Day</td>
<td>141,243</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mempool Size</td>
<td>186,246</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Bitcoin block mining reward halves every 210,000 blocks, the coin reward will decrease from 12.5 to 6.25 coins.

| Total Bitcoins in circulation: | 16,968,713 |
| Total Bitcoins to ever be produced: | 21,000,000 |
| Percentage of total Bitcoins mined: | 80.79% |
| Total Bitcoins left to mine: | 4,033,288 |
| Total Bitcoins left to mine until next blockhalf: | 1,406,288 |
| Bitcoin price (USD): | $7,134.80 |
| Market capitalization (USD): | $121,054,100,345.00 |
| Bitcoins generated per day: | 1,800 |
| Bitcoin inflation rate per annum: | 3.95% |
| Bitcoin inflation rate per annum at next block halving event: | 1.80% |
| Bitcoin inflation per day (USD): | $12,842,640 |
| Bitcoin inflation until next blockhalf event based on current price (USD): | $10,047,849,655 |
| Total blocks: | 517,337 |
| Blocks until mining reward is halved: | 112,603 |
| Total number of block reward halvings: | 2 |
| Approximate block generation time: | 10.00 minutes |
| Approximate blocks generated per day: | 144 |
Bitcoins – Average price since April 2017
Bitcoins in circulation

The total number of bitcoins that have already been mined; in other words, the current supply of bitcoins on the network.

Source: blockchain.info
USD Exchange Trade Volume

The total USD value of trading volume on major bitcoin exchanges.

Source: Blockchain.info
Average Number Of Transactions Per Block

The average number of transactions per block.
Source: blockchain.info
BitCoin: Challenges

• Creation of a virtual coin/note
  • How is it created in the first place?
  • How do you prevent inflation? (What prevents anyone from creating lots of coins?)

• Validation
  • Is the coin legit? (proof-of-work)
  • How do you prevent a coin from double-spending?

• Buyer and Seller protection in online transactions
  • Buyer pays, but the seller doesn’t deliver
  • Seller delivers, buyer pays, but the buyer makes a claim.

• Trust on third-parties
  • Rely on “proof of work” instead of trust
  • Verifiable by everyone – blockchain is visible to all
  • No central bank or clearing house
Security in Bitcoin

• Authentication
  • Am I paying the right person? Not some other impersonator?

• Integrity
  • Is the coin double-spent?
  • Can an attacker reverse or change transactions?

• Availability
  • Can I make a transaction anytime I want?

• Confidentiality
  • Are my transactions private? Anonymous?
Security in Bitcoin

• Authentication → Public Key Crypto: Digital Signatures
  • Am I paying the right person? Not some other impersonator?

• Integrity → Digital Signatures and Cryptographic Hash
  • Is the coin double-spent?
  • Can an attacker reverse or change transactions?

• Availability → Broadcast messages to the P2P network
  • Can I make a transaction anytime I want?

• Confidentiality → Pseudonymity
  • Are my transactions private? Anonymous?
Back to BitCoin

• Validation
  • Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  • How do you prevent a coin from double-spending? → Broadcast to all nodes

• Creation of a virtual coin/note
  • How is it created in the first place? → Provide incentives for miners, earn bitcoins after work!
  • How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins. Right now, 12.5 coins to miners
Bitcoin Transactions

Public key 0xc7b2f68...

Signature 0xa87g14632d452cd
Bitcoin Network

• Each P2P node runs the following algorithm:
  • New transactions are broadcast to all nodes.
  • Each node (miners) collects new transactions into a block.
  • Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  • When a node finds a proof-of-work, it broadcasts the block to all nodes.
  • Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  • Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.
Practical Limitation

• At least 10 mins to verify a transaction.
  • Agree to pay
  • Wait for one block (10 mins) for the transaction to go through.
  • But, for a large transaction ($$$) wait longer, around 60 minutes. Because if you wait longer it becomes more secure.
  • For large $$$, you wait for six blocks (1 hour).
BitCoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the “network’s capacity”
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new Bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25
  - Since 2016 N = 12.5, next half is June 2020 for N = 6.25.
  - Halved every 210,000 blocks (every four years)
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)
Privacy Implications

• No anonymity, only pseudonymity
• All transactions remain on the block chain— indefinitely!
• Retroactive data mining
  • Target used data mining on customer purchases to identify pregnant women and target ads at them (NYT 2012), ended up informing a woman’s father that his teenage daughter was pregnant
  • Imagine what credit card companies could do with the data
47,000 Businesses Trust Coinbase To Integrate Bitcoin Payments, Including...
Coinbase Exits as Hawaii Requires Bitcoin Companies to Hold Fiat Reserves
Cryptocurrencies and Blockchains

• Cryptocurrencies and technology are here to stay...
  • http://www.bitcoin.org/ - Started Satoshi Nakamoto, 10/08
  • www.ZeroCoin.org - Extend Bitcoin to make it private
  • www.Litecoin.org - Open Source P2P Internet Currency
  • www.Ethereum.org - Smart Contracts (Microsoft)
  • www.Hyperledger.org - Blockchains for Business (IBM)

• Security is an issue just like anything else
  • Consumers: Social Engineering, Malware, Phishing etc.
  • Exchanges: Hacks, Botnets, Malware, Phishing, APT etc.
Acknowledgements

Some of the slides, content, or pictures are borrowed from the following resources, and some pictures are obtained through Google search without being referenced below:

- Most of the OSINT content in this presentation is from - Online Class on Open Source Intelligence (OSINT) 2016 class at Cyber Watch West (CWW) by Anastacia Webster, Adjunct Instructor at California State University, San Bernardino, CA
- Michael Bazzell- Open Source Intelligence Techniques; Hiding from The Internet; Privacy and Security; Personal Digital Security
- Johnny Long- No Tech Hacking : Google Hacking
- L24-BitCoin and Security, many of the slides borrowed from this presentation with modifications.