DSci529: Security and Privacy In Informatics

Crypto-Currencies
Privacy Preserving Technologies

Prof. Clifford Neuman

Lecture 13
16 April 2021
Online

Course Outline

- Overview of Security and Privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- Reasonable expectation of privacy
- Big Data – Technology and Privacy
- AI and Bias
- The Internet of Things and Security and Privacy
- Social Networks and the use of our Data
- Access to Data by Governments - Privacy in a Pandemic
- Privacy Regulation - GDPR, CCPA, CPRA
- Influence of Social Media – Free Speech – Disinformation
- **CryptoCurrency - TOR - Privacy Preserving Technologies**

Upcoming Presentations
Other Security Topics – April 23rd

- Yo-Shuan Liu – User experience and Multi-Factor Authentication
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India

Today's Agenda

12:00 – 12:05 Introduction and Announcements

12:05 – 12:45 Student Presentations – Payments

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – Cryptocurrency - History and Technology
- Saurabh Jain – Privacy of Payment Information
- Yifeng Shi - Financial value of personal Data

12:45 – 13:15 Class Discussion – Payments - Dr. Neuman

13:15 – 13:25 Break

13:25 – 14:15 Student Presentations – Privacy Preserving Technology

- Haipeng Yu - Comparison of privacy preserving technologies
- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

14:15 – 14:50 Class Discussion – Privacy Preserving Tech

14:50 – 15:20 Current Event Discussions

Security & Privacy in the Financial Sector

By Jonathan De Leon

What is the financial sector?

- Payments
- Insurance
- Banking
- Investments

#1 most attacked

Financial services including banking and insurance

$18.5 million

Average annual cost of cybercrime per financial company

70%

Experienced a cyber security incident in the past 12 months

1.
Data Collection

What is being processed?

- Bank balances
- Account numbers
- SSN
- Biometrics
- Other non-financial PII

How is it being used?

- ”Free” services (tax returns)
- Credit score
- Financial advertising
- Boost customer satisfaction
- Monitor fraudulent activity
- Predicting market

2. Security & Privacy Concerns

Security Concerns

- Unencrypted data
- Manipulated data
- Malware
- Non-secure third-party services

Privacy Concerns

- Identity theft
- Data sharing
- Big Data as talked about in class
- Consent

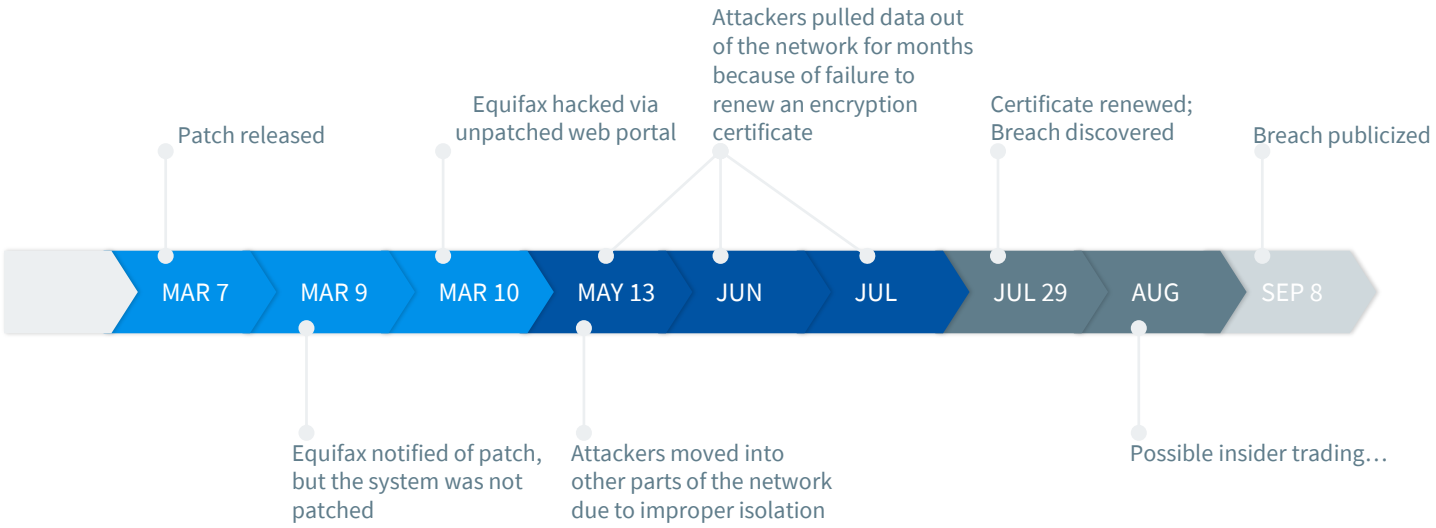
There are only two types of companies: those that have been hacked and those that will be

- Robert Mueller

Case Study

Equifax

Timeline


Patch released
Equifax hacked via unpatched web portal
Attackers pulled data out of the network for months because of failure to renew an encryption certificate
Certificate renewed; Breach discovered
Breach publicized
MAR 7
MAR 9
MAR 10
MAY 13
JUN
JUL
JUL 29
AUG
SEP 8
Equifax notified of patch, but the system was not patched
Attackers moved into other parts of the network due to improper isolation
Possible insider trading…

Case Study: Equifax

By the numbers

Affected 143 million people (40% US population) – names, address, DOB, SSN, drivers' licenses numbers. Smaller subset included credit card numbers.

0 reported fraud cases

What can we learn

- No network is invulnerable
- Proper network isolation
- Security is about effective policy, risk analysis, and risk management
- Containment architecture

3.
Regulation

Regulation

GDPR/CCPA

Framework for the processing/sharing of personal data. Gives more rights and control over personal information. Limited by region (EU or CA).

GLBA

Gramm-Leach-Biley Act (1999) allowed banks to offer financial services (investments and related). They must explain their data-sharing practices allowing “opt-out”. It requires limited privacy protections.

PCI-DSS

Standards to protect cardholder data.

Conclusion

Be aware of “free” services and how institutions process the data they collect. Financial institutions need a robust, forward-looking framework. Greater transparency beyond regulation compliance is called for.

References

https://www.ibm.com/security/data-breach/threat-intelligence

https://www.stealthlabs.com/blog/cybersecurity-in-financial-sector-8-important-facts-and-statistics/

https://www.clearswift.com/blog/2019/08/28/cyber-security-and-finance-sector-need-stronger-data-protection-capabilities

https://www.ngdata.com/data-privacy-guide-for-banks-and-financial-institutions/

https://www.imperva.com/blog/top-security-and-data-privacy-regulations-for-financial-services/

https://www.washingtonpost.com/technology/2019/03/07/when-tax-prep-is-free-you-may-be-paying-with-your-privacy/?noredirect=on

https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

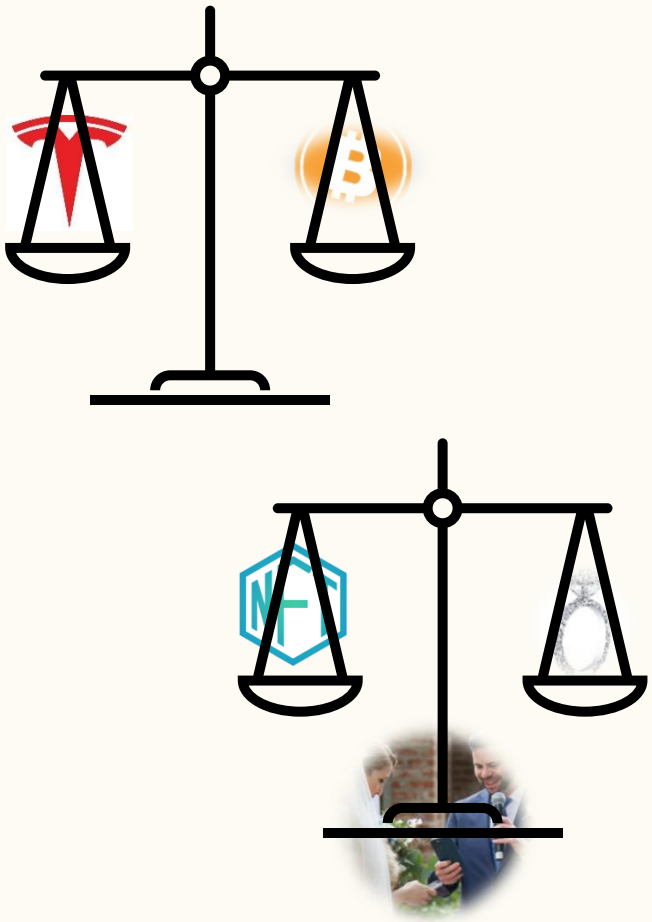
HISTORY AND TECHNOLOGIES FOR CRYPTOCURRENCY

Sidong Wang

April 16, 2021

Overview

- History of cryptocurrency and its evolution
- How cryptocurrency works
- Technologies behind cryptocurrency
- Privacy and security issues
- Regulation



Current events

- Elon Musk bought $1.5 billion worth of bitcoin in February 2021 and recently in March, Tesla already accepted bitcoin as a way of payment.
- Coinbase, the largest crypto platform in the U.S. just went public on Wednesday from a starting reference price of $250 and close at $328.28.
- Two Coinbase employees exchanged NFT rings with their wedding vows as part of the ceremony.

General statistics

- As of April 2020, there are over **5,300** alternative cryptocurrencies being traded with a total market capitalization of **$201bn**
- Bitcoin alone accounts for **$6 billion** of daily online transactions in comparison with Visa **$30.3bn** MasterCard **$16.2bn**.
- With the aid of malware, **$1.1 billion** worth of cryptocurrency was stolen within the first half of 2018.
- Over **18.3 million** Bitcoins have been mined and are in existence as of Q1 2020. **2.7 million** Bitcoins are left to be mined, and it will take over **a hundred years** before the last Bitcoin is mined.

Development History

- American cryptographer David Chaum
  - Conceived an anonymous cryptographic electronic money called ecash. (1983)
  - Implemented ecash through Digicash. (1995)
- Computer engineer Wei Dai
  - Developed the Crypto++ cryptographic library.
  - Created the b-money cryptocurrency system. (1998)
- Presumably pseudonymous developer Satoshi Nakamoto
  - Created the first decentralized cryptocurrency, bitcoin (2009)
- Other notable cryptocurrency
  - Namecoin: forming a decentralized DNS
  - Litecoin: use script instead of SHA-256
  - Peercoin: use a proof-of-work/proof-of-stake hybrid

How it works (Bitcoin as example)

FOR GENERAL USER

- A mobile app or computer program that provides a personal wallet and allows a user to send and receive bitcoins with it.

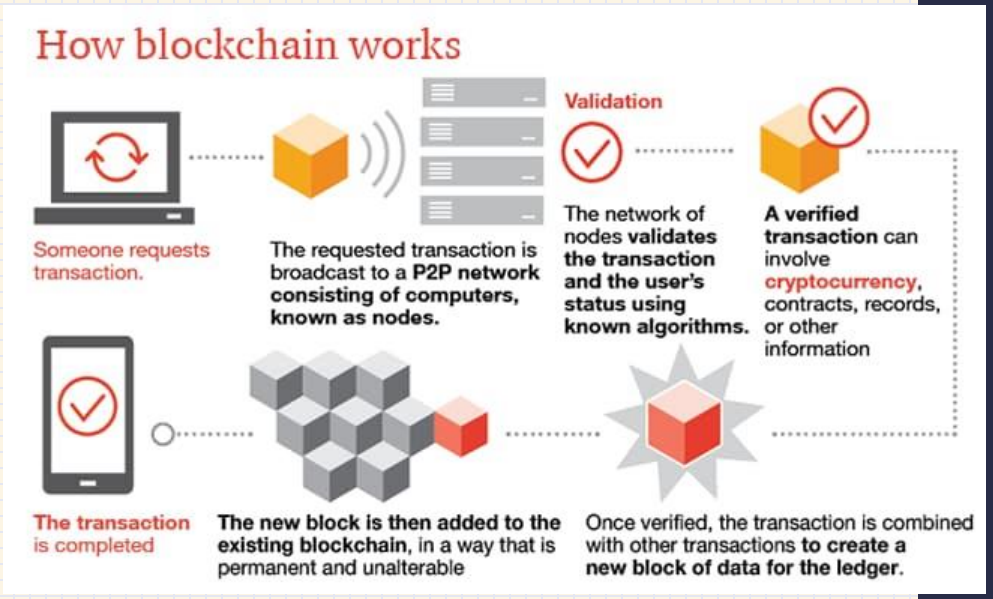
BEHIND THE SCENE

- A public ledger called the "blockchain" containing every transaction ever processed.
- Wallets keep a private key used to sign transactions, providing a mathematical proof that they have come from the owner of the wallet.
- Anyone can process transactions to confirm it using the computing power of specialized hardware and earn a reward in bitcoins for this service.

VALUE AND PRICE

- Bitcoin's value comes only and directly from people willing to accept them as payment, providing trust and adoption for it to hold value.
- The price of a bitcoin is determined by supply and demand.
- Bitcoin is still a relatively small market; it doesn't take significant amounts of money to move the market price up or down

Technology behind

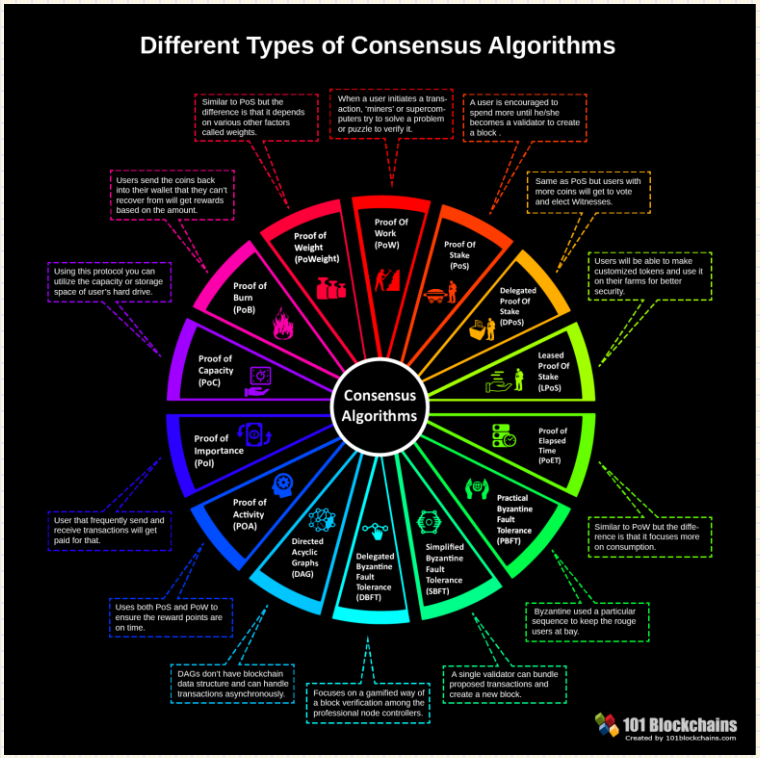


Blockchain technology

A blockchain is a growing list of records, called blocks, that are linked using cryptography.

- Immutability
  - Every existing nodes need to check the validity of the new adding transaction.
- Decentralized
  - No governing authorities, maintain over nodes.
- Consensus
  - Use consensus algorithm

Technology behind



Consensus algorithm

Consensus algorithms are a decision-making process for a group, where individuals of the group construct and support the decision that works best for the rest of them.

- Prove of Work System
  - Offer DDoS protection and lower the overall stake mining
  - Greater Energy Consumption (77.78 TWh of electricity per year)
  - The miners get less bitcoins overtime. Smaller incentives ensure less chance of 51% attack

- Prove of Stake System
  - Need to deposit a certain amount of coin before being a miner
  - Far less power consumption
  - Full decentralization is not possible
  - The 51% attack is ridiculously expensive

Technology behind

```
Function scrypt
   Inputs: This algorithm includes the following parameters:
      Passphrase:                Bytes    string of characters to be hashed
      Salt:                      Bytes    string of random characters that modifies the hash to protect against Rainbow table attacks
      CostFactor (N):            Integer  CPU/memory cost parameter – Must be a power of 2 (e.g. 1024)
      BlockSizeFactor (r):       Integer  blocksize parameter, which fine-tunes sequential memory read size and performance. (8 is commonly used)
      ParallelizationFactor (p): Integer  Parallelization parameter. (1 .. 2^32-1 * hLen/MFlen)
      DesiredKeyLen (dkLen):     Integer  Desired key length in bytes (Intended output length in octets of the derived key; a positive integer satisfying dkLen ≤ (2^32 - 1) * hLen.)
      hLen:                      Integer  The length in octets of the hash function (32 for SHA256).
      MFlen:                     Integer  The length in octets of the output of the mixing function (SMix below). Defined as r * 128 in RFC7914.
   Output:
      DerivedKey:                Bytes    array of bytes, DesiredKeyLen long

   Step 1. Generate expensive salt
   blockSize ← 128*BlockSizeFactor   // Length (in bytes) of the SMix mixing function output (e.g. 128*8 = 1024 bytes)

   Use PBKDF2 to generate initial 128*BlockSizeFactor*p bytes of data (e.g. 128*8*3 = 3072 bytes)
   Treat the result as an array of p elements, each entry being Blocksize bytes (e.g. 3 elements, each 1024 bytes)
   [B0...Bp−1] ← PBKDF2HMAC-SHA256(Passphrase, Salt, 1, blockSize*ParallelizationFactor)

   Mix each block in B Costfactor times using ROMix function (each block can be mixed in parallel)
   for i ← 0 to p-1 do
      Bi ← ROMix(Bi, CostFactor)

   All the elements of B is our new "expensive" salt
   expensiveSalt ← B0 // B1 // B2 // ... // Bp−1   // where // is concatenation

   Step 2. Use PBKDF2 to generate the desired number of bytes, but using the expensive salt we just generated
   return PBKDF2HMAC-SHA256(Passphrase, expensiveSalt, 1, DesiredKeyLen);
```

Crypto algorithm

- SHA-256
  - Implemented in some widely used security applications and protocols
  - Practical attack can break 28/64 rounds of SHA-256 while theoretic one can break 52/64
- Script
  - Generate a large vector of pseudorandom bit strings
  - Costly to perform large-scale custom hardware attacks by requiring large amounts of memory.

Privacy and Security

- Bitcoin is not anonymous and cannot offer the same level of privacy as cash. The use of Bitcoin leaves extensive public records.
- Stefan Thomas, a German-born programmer living in San Francisco, has two guesses left to figure out a password that is worth, as of this week, about $220 million.
- In November 2020, the United States government seized more than $1 billion worth of bitcoin connected to Silk Road, stolen by an anonymous hacker.
- The ISIS propagandist who called himself Azym Abdullah reportedly turned to cryptocurrency in 2014, asking for donation and using bitcoin paying for severs.

Regulation

- Bitcoin has not been made illegal by legislation in most jurisdictions. However, some jurisdictions (such as Argentina and Russia) severely restrict or ban foreign currencies. Other jurisdictions (such as Thailand) may limit the licensing of certain entities such as Bitcoin exchanges.
- Most common actions taken are government-issued notices about the pitfalls and added risk of investing in the cryptocurrency markets.
- In March 2021, Congress introduced legislation to create a working group with the U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) to evaluate the current legal and regulatory framework around digital assets in the U.S.

Governance – 51% percent attack

- A potential attack on blockchain giving the attacker a possible control of majority (more than half) users and taking over most of the mining power enough to control everything in the cryptocurrency network.
- Allow attackers to:
  - Prevent some or all transactions from being confirmed
  - Prevent some or all other miners from mining
- Attackers would not be able to:
  - Reverse transactions or to prevent transactions from being created and broadcasted to the network.
  - Change the block's reward, create or steal coins
- The bigger the network, the stronger the protection against attacks and data corruption.
- Smaller cryptocurrencies with lower computational power are much more vulnerable to 51% attack.

Reference

- https://www.cnbc.com/2021/03/24/elon-musk-says-people-can-now-buy-a-tesla-with-bitcoin.html
- https://www.cnet.com/personal-finance/coinbase-stock-what-you-should-know-about-the-crypto-exchange-that-just-went-public/
- https://www.theverge.com/tldr/2021/4/2/22364647/coinbase-employees-nft-wedding-exchange-romance
- https://techjury.net/blog/cryptocurrency-statistics/#gref
- https://www.daviescoin.io/blog/a-short-history-of-cryptocurrencies
- https://bitcoin.org/en/faq#can-i-make-money-with-bitcoin
- https://101blockchains.com/introduction-to-blockchain-features/
- https://101blockchains.com/consensus-algorithms-blockchain/#6
- http://www.tarsnap.com/scrypt.html
- https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html
- https://www.wired.com/story/feds-seize-billion-stolen-silk-road-bitcoin/
- https://www.buzzfeednews.com/article/johntemplon/bitcoin-cryptocurrency-terrorist-financing-janet-yellen
- https://academy.binance.com/en/articles/what-is-a-51-percent-attack
- https://www.loc.gov/law/help/cryptocurrency/world-survey.php
- https://www.coindesk.com/lawmakers-digital-asset-regulation

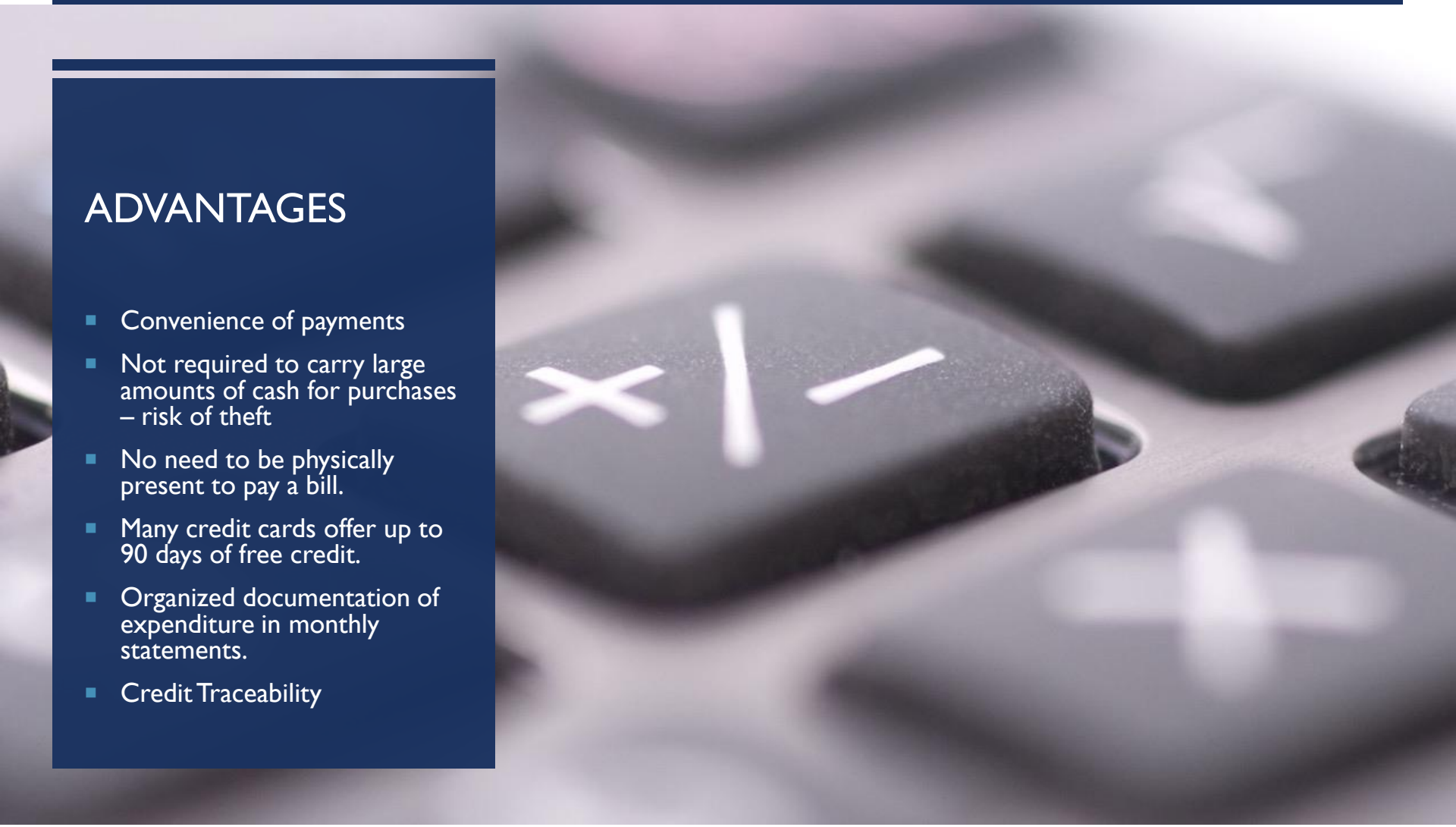
PRIVACY OF CREDIT CARD/PAYMENT CARD INFORMATION

SAURABH JAIN

04/16/2021

ADVANTAGES

- Convenience of payments
- Not required to carry large amounts of cash for purchases – risk of theft
- No need to be physically present to pay a bill.
- Many credit cards offer up to 90 days of free credit.
- Organized documentation of expenditure in monthly statements.
- Credit Traceability



DISADVANTAGES

- Ubiquitous records imperil privacy
- Issues arise with the collection of private information
- Authorized use by authorized parties does not necessarily mean that privacy is protected
- Protection methods such as encryption software are compromised by market forces
- Legislation changes so far are not seen to be sufficient to protect privacy

YOUNG, A. M. "PRIVACY ISSUES OF USING CASHLESS MEDIUMS OF EXCHANGE OVER THE INTERNET." *THE INTERNET SOCIETY II: ADVANCES IN EDUCATION, COMMERCE & GOVERNANCE*, 2006. *CROSSREF*, DOI:10.2495/IS060421.

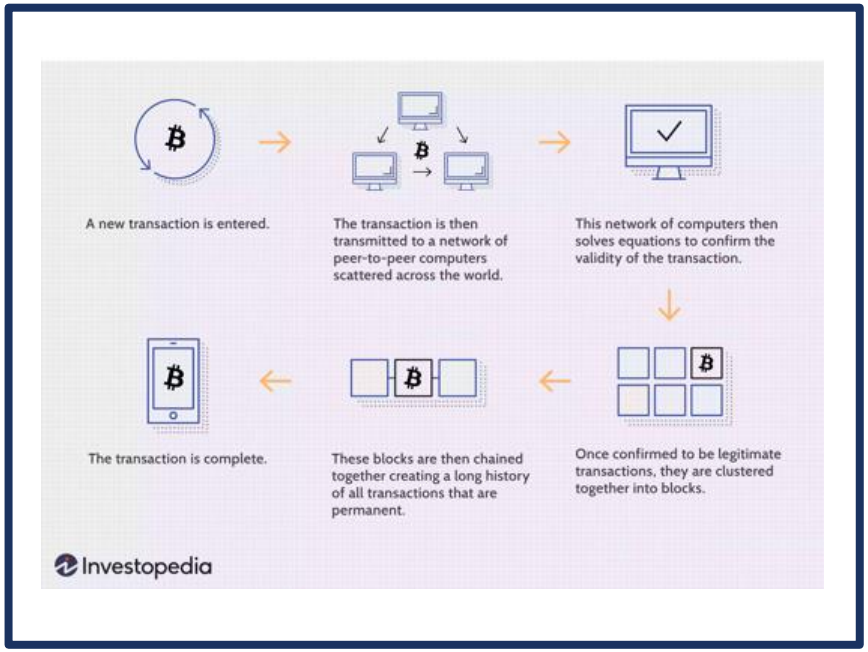
PRIVACY RISKS WITH CREDIT/DEBIT CARDS

- Cash protects privacy outside those involved in an exchange.
- The mere consolidated visibility affects a person's privacy whether that information is specifically used or not.
- Access can be gained to private information by authorized parties such as the financial institution
- Authorized uses, by authorized parties does not always constitute what many would consider ethical or even legal.
- Introduction of a middleman
  - Visa has around 60% of the credit/debit card market, MasterCard - 25%, American Express - 13%, and Discover - 2%
  - Mobile apps such as Apple Pay, Venmo, and Square are also gaining a foothold.
- Unauthorized uses by unauthorized people are also a very real threat to privacy.
- Tracing perpetrators can also be a difficult task despite the existence of a firewall.

SOME SECURITY RISKS WITH CREDIT/DEBIT CARDS IN THE US.

- Credit Card Fraud
  - If someone steals your card or memorizes your number, he can use it to make unauthorized purchases in your name.
  - Your balance will increase, and if you can't remove the charges from your account, the credit card company may hold you responsible for the unpaid amount.
- Identity Theft
  - Credit cards are connected to sensitive information such as your Social Security number and birth date.
  - Using this information, thieves can steal your identity to open fraudulent accounts, obtain medical care in your name or fund criminal activity.
- Unauthorized Charges
  - These may appear because of an error, such as a double billing, or they may be intentionally imposed by a shady company.
  - Depending on how quickly you discover the fraudulent activity, it may be difficult to remove unauthorized charges from your account.

STANLEY, JAY. "WHY DON'T WE HAVE MORE PRIVACY WHEN WE USE A CREDIT CARD?" *AMERICAN CIVIL LIBERTIES UNION*, 14 AUG. 2019, WWW.ACLU.ORG/BLOG/PRIVACY-TECHNOLOGY/CONSUMER-PRIVACY/WHY-DONT-WE-HAVE-MORE-PRIVACY-WHEN-WE-USE-CREDIT-CARD.



Venmo's privacy policy states that it shares user data "for everyday business purposes, for marketing purposes, for joint marketing with other companies." Venmo also shares "information about your transactions and experiences" with its affiliates.

BANK

Bank account information is stored on the bank's private servers and held by the client. Bank account privacy is limited to how secure the bank's servers are and how well the individual user secures their own information. If the bank's servers were to be compromised, then the individual's account would be as well.

BITCOINS

Bitcoin can be as private as the user wishes. All Bitcoin is traceable, but it is impossible to establish who has ownership of Bitcoin if it was purchased anonymously. If Bitcoin is purchased on a KYC exchange, then the Bitcoin is directly tied to the holder of the KYC exchange account.

Target breach shows need to create more secure payment systems.

Posted on: January 4, 2014 **Posted in:** Compliance & Regulations, Cybercrime **Posted by:** Trend Micro

An attack on the point-of-sale systems at retail giant Target over the holidays may have exposed sensitive data, including PINs, from tens of millions of payment cards. The breach coincided with Black Friday, the traditional kickoff to the holiday shopping season, and may have extended to mid December. Ultimately, this incident may rank as one of the largest and most costly in retail history, with banks already taking decisive action to protect cardholders from fraud.

The Target breach was confined to POS terminals at the retailer's locations in the U.S. and Canada and did not affect its website. Malware distributed throughout these brick-and-mortar stores may have facilitated the mass skimming of card data, and this line of attack may demonstrate the blurring line between physical security and cybersecurity.

More specifically, organizations must be equally attentive to on-site vulnerabilities and remotely orchestrated campaigns, as the Target breach was the result of many individual POS systems being compromised by one carefully engineered attack. To this end, antimalware solutions will need to be paired with upgraded payment systems. Ideally, the shift from magnetic stripe to microchip technology in debit and credit cards will shore up POS security, but retailers will also need to be diligent about handling customer data and working with PCI and cybersecurity experts.

- **Target breach shows needs for new payment card technology**
- An attack on the point-of-sale systems at retail giant Target over the holidays may have exposed sensitive data, including PINs, from tens of millions of payment cards.
- The Target attackers took advantage of the ongoing reliance on magnetic stripe cards in the U.S., but in other countries, this technology has already been superseded by the Europay, Mastercard and Visa (EMV) standard.

MICRO, TREND. "TARGET BREACH SHOWS NEED TO CREATE MORE SECURE PAYMENT SYSTEMS." *TREND MICRO, INC.*, 14 JAN. 2014, HYPERLINK.

FEB 16, 2012 @ 11:02 AM 3,122,087 VIEWS The Little Black Book of Billionair

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill, FORBES STAFF
Welcome to The Not So Private Parts where technology & privacy collide FULL BIO

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +0.21%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant -- and loyal -- buyers of all things pastel, plastic, and miniature. He talked to Target

Find the right solution
to meet your
unique networking nee

TARGET

- There are some brief periods in a person's life when old routines fall apart and buying habits are suddenly in flux.
- If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail they send you or you visit their Web site, they will record it and link it to your Guest ID - that keeps tabs on everything they buy.

DUHIGG, CHARLES. "HOW COMPANIES LEARN YOUR SECRETS." *THE NEW YORK TIMES*, 22 FEB. 2012, WWW.NYTIMES.COM/2012/02/19/MAGAZINE/SHOPPING-HABITS.HTML?PAGEWANTED=1&_R=2&HP&.

GRAMM-LEACH-BLILEY ACT

- The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
- Although it has often been described as a "financial privacy law," Gramm-Leach created nothing more than a weak "fig leaf" privacy standard.
- Consumers have no privacy under federal regulations unless they affirmatively take steps to "opt out" of this sharing.

"GRAMM-LEACH-BLILEY ACT." *FEDERAL TRADE COMMISSION*, 1999, WWW.FTC.GOV/TIPS-ADVICE/BUSINESS-CENTER/PRIVACY-AND-SECURITY/GRAMM-LEACH-BLILEY-ACT.

STANLEY, JAY. "WHY DON'T WE HAVE MORE PRIVACY WHEN WE USE A CREDIT CARD?" *AMERICAN CIVIL LIBERTIES UNION*, 14 AUG. 2019, WWW.ACLU.ORG/BLOG/PRIVACY-TECHNOLOGY/CONSUMER-PRIVACY/WHY-DONT-WE-HAVE-MORE-PRIVACY-WHEN-WE-USE-CREDIT-CARD.

CASHLESS SOCIETY AND THE COVID-19 PANDEMIC

- Cash is still the second-most-used form of payment in America today after debit cards.
- But many advocates for "going cashless" believe that the paper dollar's time is nearly up.
- As the coronavirus pandemic ravages communities around the globe, the use of cash is raising concerns around cleanliness and viral transmission

"WHY AMERICA WON'T BE GOING CASHLESS ANYTIME SOON." *FORTUNE*, 25 JUNE 2020, WWW.FORTUNE.COM/2020/06/25/CASHLESS-SOCIETY-CORONAVIRUS-CASH-AMERICA-FINTECH-UNBANKED-PRIVACY.

CONCLUSION

- With the compromise of technical protection and admissions of shortfalls in the existing privacy legislation, privacy over the internet related to cashless payments remains a concern.
- Moving towards a cashless society, without reflecting on how this could be used to surveil a populace and ostracize those who don't have cash alternatives will only accelerate the degradation of individual privacy, one of many shifts this year.

THANK YOU!

Questions and comments?

Financial value of data gathered through free services

Yifeng Shi

DSCI 529 Presentation
April 16th

We are living in a world of social media

Advertisement: important factors

- “If the product is free, then you are the product”
- The numbers of users is the key to this way of making financial benefits
- More importantly, how much users will stick to their computers or smartphones is also an important factor in this section
- Influencers will act as catalysts for viewers-growth for the advertising, increasing the revenue of the social media
- User-targeting is also important in this section
- Not surprisingly, social media platforms will utilize your personal data when you signed up for advertising purpose

Advertisement: users sticking to the platforms

- The platforms will design their apps to be habit-forming, making sure users will check updates on the app every day. They uses daily update-push ups and personalized stories feed to help the users to form habits
- Social media will allow users to like, dislike, star mark, or direct messages, which keep users interacting with their friends or subscribers, increasing the amount of time they spent on the social platforms

CCPA: business pricing vs personal data

Even though CCPA prohibits business from any discriminations of the pricing, services, or products

But it's worth discussion that the law doesn't provide quantitative and detailed standards on the pricing based on the users' data value, and there has some room left by the business owners to vary prices as long it's based on the users' personal data.

A good question here will be what do you think about the standard for the business owner to price items whose price difference is based on the customer's data value?

Advertisement: how social media targets you?

- Some social media will percept users' preferences by asking users personalized questions
- Social media will collect your updated posts, what posts you've read, whose stories you liked or disliked and analyze those data to form targeted advertising to you
- Social media will base on your browsing history/cookies to do the advertising recommendations

Other ways of revenue: subscriptions/monthly plan

- This is usually hard to obtain large amounts of revenue for new startup social media → users would not like to pay the subscriptions at the first place.
- Some creative products like Facebook Gift or Wechat red packet during New Lunar Year Festival
- Venture Capital is another way: investors will see the potential in the apps

Thank You!

Yifeng Shi

DSCI 529 Presentation
April 16th

Reference

- https://www.investopedia.com/stock-analysis/032114/how-facebook-twitter-social-media-make-money-you-twtr-lnkd-fb-goog.aspx
- https://themanifest.com/mobile-apps/what-makes-social-media-apps-successful
- https://www.redalkemi.com/blog/post/traditional-marketing-vs-social-media-marketing
- https://www.bigcommerce.com/blog/social-media-advertising/#the-6-best-social-networks-for-ecommerce-advertising
- https://www.loyola.edu/academics/emerging-media/blog/2017/3-ways-that-social-media-knows-you-better-than-your-friends-and-family-do
- https://shanebarker.com/blog/pros-and-cons-of-influencer-marketing/
- https://www.jdsupra.com/legalnews/ccpa-what-is-the-value-of-your-personal-16202/

Today's Agenda

12:00 – 12:05 Introduction and Announcements

12:05 – 12:45 Student Presentations – Payments

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – Cryptocurrency - History and Technology
- Saurabh Jain – Privacy of Payment Information
- Yifeng Shi - Financial value of personal Data

12:45 – 13:15 Class Discussion – Payments - Dr. Neuman

13:15 – 13:25 Break

13:25 – 14:15 Student Presentations – Privacy Preserving Technology

- Haipeng Yu - Comparison of privacy preserving technologies
- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

14:15 – 14:50 Class Discussion – Privacy Preserving Tech

14:50 – 15:20 Current Event Discussions

Some Readings: Bitcoin

We start with a late-night television sketch discussing BitCoin. This is very funny, and most of what is said is accurate, although intentionally over the heard of many viewers.

- Late Night with Seth Meyers skit on BitCoin

We should really have started with the original technical paper describing bitcoin, so I am assigning this as an additional reading now. The original bitcoin paper is here. It is written under the pseudonym Satoshi Nakamoto, and no one really knows who that is.

- Bitcoin: A Peer-to-Peer Electronic Cash System

CryptoCurrency

One concern with cryptocurrencies is their regulation. The next link provides a survey of how cryptocurrencies are regulated (or not) in different jurisdictions throughout the world.

- https://www.loc.gov/law/help/cryptocurrency/world-survey.php

So, is Bitcoin really anonymous? Here is a discussion on US National Public Radio.

- https://www.npr.org/2017/11/09/563050434/once-an-underground-currency-bitcoin-emerges-as-a-new-way-to-track-information

There are many different cryptocurrencies, not just BitCoin. Here is a survey of some of them:

- https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future

CryptoCurrency

Next we read a BBC article about China's Digital Currency Electronic Payment (DCEP), and another story discussing the status of BitCoin in China.

- https://www.bbc.com/news/business-54261382
- https://www.newsbtc.com/news/bitcoin/china-state-outlet-xinhua-exposes-bitcoin/

Blockchain

- Blockchain
  - A technology for preserving and documenting integrity of a chain of transactions.
  - Useful for many purposes beyond currency.
    - Supply chain, food, electronics, pharmaceuticals, software, real estate transactions
    - Integrity of audit records
  - Often overhyped
    - Claims that it can be used for other security services, such as confidentiality.
      - Can contributed to solutions, but these other services end up primarily provided by other mechanisms.
- https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

Some Issues

- Bitcoin
  - Democratization – who controls
  - Trust – 51% problem – Security
  - Use in developing (or waning) countries and economic impact.
  - Use as a substitute for established currencies.
    - Avoiding hyperinflation
  - Use to avoid regulation/taxation.
  - Use in illegal activities.
  - Issues of privacy and anonymity (end of lecture)

Engineering 499
Privacy, Security, and Policy in the Age of the Internet

Understanding Traceability Of Crypto-Currency

Prof. Clifford Neuman
Center for Computer Systems Security
Information Sciences Institute
University of Southern California
bcn@isi.edu

Originally
ECTF 2019 Spring Meeting
USC UPC Campus
17 May 2019

What is Bitcoin

- Bitcoin is a distributed internet Crypto-currency that allows transfers of value between individuals and businesses without relying on an central authority.
  - There is no entity that “backs” the currency, its value is based solely on willingness of others to accept it as payment, and its value fluctuates greatly.
  - Balances are managed on a “distributed” blockchain whose authenticity is managed by consensus of the participants.
  - Balances are associated with “numbered” accounts that can be created simply by choosing a “random account number”, and generating a corresponding “password”. The account comes into existence as soon as funds are transferred to it and the transaction is recorded in the blockchain.
  - Technically, the random account number is a public key, and password is the corresponding private key.

Anonymity is a common misconception

- Bitcoin and its brethren are the currency of choice for cyber-criminals.
  - Including online purveyors of illegal goods.
  - These “numbered” accounts provide some level of anonymity, … but
  - For many cryptocurrencies, the movement of funds from one account to another is recorded in a PUBLIC ledger making it much easier to *follow the money*.
  - Consider findings in the Mueller report… more on this later.

Bitcoin is just on of many cryptocurrencies

- Most modern cryptocurrencies are based on the same principal, that transactions are recorded in a public blockchain.
  - Some claim to be backed by balances elsewhere.
  - Some use more advanced principals such as zero-knowledge-proofs to protect certain information on the public blockchain.
  - Level of anonymity varies greatly

Some Popular Cryptocurrencies

Name	Symbol	Privacy	Comment
Bitcoin	BTC	"Numbered accounts"	Source, destination, and amounts of payments visible in public ledger.
Etherium	ETH	Similar to BTC	More efficient and commonly used by developers and smart-contract applications.
Monero	XMR	Stronger Anonymity	More difficult to follow transactions since ledger does not disclose source, destination, and amount. Built in tumbling.
Zcash	ZEC	Significant privacy of transactions.	Zero-knowledge-proofs are used to ensure critical properties of the money supply without divulging details (source, destination, amount) of transactions.
Bitcoin Cash	BCH	Similar to BTC	Branch of original Bitcoin ledger.

What is an Initial Coin Offering (ICO)

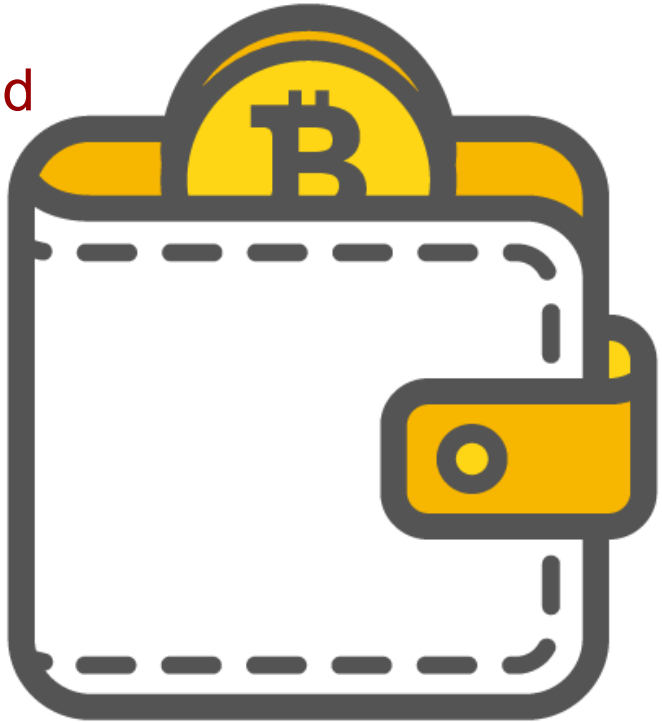
- A speculative offering of early coins in a new cryptocurrency in exchange for funds that might be used to support development and or backing of the cryptocurrency.
  - Very low bar to creating a new cryptocurrency.
  - “investors” hope the new currency will gain traction.
  - This can be helped if there is a differentiating factor in the management of or technology used by the new currency.
    - E.g. privacy supported by zero knowledge proofs
    - Acceptability of the currency in certain markets
    - In some cases, ICO funds used to back (or partially back) the currency.

So, can we seize cryptocurrency?

- What about asset forfeiture?
- Let's consider how the assets are "stored"
  - The value of ones crypto-currency is recorded in a distributed ledger called a blockchain.
  - Changes to the balances of accounts occur when a transaction is recorded in the blockchain.
  - This occurs when the transaction is signed by the private key (password) associated with the originating bitcoin address.
  - Transactions are validated and entered into the blockchain based on consensus (with proof of work) by the majority of the entities maintaining the blockchain.
  - So, the quick answer is NO, not unless you control a majority of the entities managing the blockchain.

What is a Bitcoin wallet

- A bitcoin wallet is memory (and associated management software) that stores the bitcoin private key and “signs” authorized transactions.
  - Which funds from an account.
- Can it be seized?
  - Yes, in the same way that most criminals steal bitcoin, i.e. you gain access to a physical device through physical entry or a cyberattack.
- Special considerations in seizing a bitcoin wallet.
  - Subject may have a backup copy.
  - Counter to the usual rules of forensics, you must move funds out of the account.
  - Might require a password or phrase.
  - You will want to keep moving funds to the new address whenever payments are made to the seized bitcoin account.



What is an exchange

- Most bitcoin users obtain their initial currency by purchasing funds at an exchange.
  - Making payment by credit card or bank transfer
  - Or exchanging a different cryptocurrency.

- Cryptocurrency Exchanges facilitate these purchases
  - Some store their customers wallets, in which case users transact bitcoin by instructing their exchange to sign the requested transaction using their managed wallet.
  - These exchanges may keep information about account holders that can be used to identify the owner of a bitcoin address. These exchanges may be subject to know-your-customer rules.
  - Wallets might be seizable on exchanges if located in the appropriate jurisdiction.
    - It might require a password to transact with wallet (e.g. shift funds to a new address).

What is a tumbler?

- A Cryptocurrency Mixing Service
  - Used to scramble the flow of funds across multiple transactions by unrelated parties to obfuscate the flow of funds making it harder to follow the money.
  - Tumblers collect a fee for providing this service.
  - The service improves privacy, but is commonly used for money laundering.
  - One can still track the flow probabilistically, i.e funds moved to one of X destinations, and iterative tumbling decreases ability to follow the money.

- Monero (XMR) effectively builds in tumbling to its transactions, no separate tumbling required.

How to follow the money

- Identify the identifiable endpoints
  - Bitcoin addresses at where funds enter the system.
    - Wallets created at exchanges where know-your-customer rules provide some degree of identification.
    - Possibly identify credit cards or bank accounts used to purchase the cryptocurrencies.
    - Photos at Bitcoin ATM's.
  - Identify destination bitcoin addresses.
    - Address to receive payments on darkweb marketplaces.
    - Payment bitcoin addresses in "classified" ads.
    - Ransom drop addresses for ransomware.
    - Well know sites for legitimate commercial enterprises accepting bitcoin.
    - Then can tell you the "shipping" addresses for orders paid for with bitcoin.
  - For basic cryptocurrencies, follow the flow of funds through the system.

The Mueller Report

The GRU began planning the releases at least as early as April 19, 2016, when Unit 26165 registered the domain dcleaks.com through a service that anonymized the registrant.[137] Unit 26165 paid for the registration using a pool of bitcoin that it had mined.[138] The dcleaks.com landing page pointed to different tranches of stolen documents, arranged by victim or subject matter. Other

[113] Bitcoin mining consists of unlocking new bitcoins by solving computational problems. IT [redacted] kept its newly mined coins in an account on the bitcoin exchange platform CEX.io. To make purchases, the GRU routed funds into other accounts through transactions designed to obscure the source of funds. *Netyksho* Indictment ¶ 62.

Investigators determined that the coins added to the CEX.io account (e.g. a wallet) were newly mined (originating without an external point of contact). Some of the currency from this wallet might have been previously tracked to destinations used in other operations for which the GRU was suspected to be involved.

Tools to Follow the Money

- Several companies scour the ledger and use data science to identify clusters of addresses linked to users or organizations, as well as to identify patterns indicative of illegal activity.
  - E.g. Chainalysis & CipherTrace
- There are websites (and local tools) that allow visualization flow of funds.
  - E.g. https://www.blockchain.com/btc/tree/59587897

Freezing vs. Seizing Funds

- If we can't seize funds can we freeze them.
  - Technically, no. But, there have been proposals for "redlisting" funds that originate from flagged addresses (such as those that received stolen bitcoin, ransom, or illicit activity).
  - As expected, there has been negative reaction within the cryptocurrency community.
- Most cryptocurrencies already allow this kind of analysis through the blockchain.
  - So, what if one were to develop a tool to identify percentage of funds in a wallet that originated with known flagged addresses, after an address was flagged.
- What kinds of disincentives might this provide.
  - What are the jurisdictional issues
  - What are the legal consequences
  - How do you deal with privacy enhanced cryptocurrencies

A hackathon experiment

- In our April 2018 Viterbi Graduate Student Hackathon teams were asked to demonstrate a system to scrape the web to identify known ransomware drops, and then track the flow of funds into and out of those cryptocurrency addresses.
  - One team developed a simple metric (which they called zeta score) based on the distance from a known drop, which could be used as a measure of the trust that might be placed in funds from various sources.
  - The metric was a proof of concept, and insufficient, but the idea could be further refined.

Summary

- Traditional cryptocurrencies are pretty easy to track.
  - The difficulty lies in identifying end points.
  - That requires good old-fashion detective work.
  - Privacy enhanced cryptocurrencies more difficult to track.
- Seizing crypto-wallets requires seizing or subverting physical devices.
  - Access or moving funds may require additional passwords.
  - Funds must be “moved” immediately, counter to usual rules.
- Tools to assess the taint on funds would be useful.

Today's Agenda

12:00 – 12:05 Introduction and Announcements

12:05 – 12:45 Student Presentations – Payments

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – Cryptocurrency - History and Technology
- Saurabh Jain – Privacy of Payment Information
- Yifeng Shi - Financial value of personal Data

12:45 – 13:15 Class Discussion – Payments - Dr. Neuman

13:15 – 13:25 Break

13:25 – 14:15 Student Presentations – Privacy Preserving Technology

- Haipeng Yu - Comparison of privacy preserving technologies
- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

14:15 – 14:50 Class Discussion – Privacy Preserving Tech

14:50 – 15:20 Current Event Discussions

Overview of privacy enhancing technologies (PET)

Haipeng Yu

Outline

- Definition and its importance
- Two ways of classifications
- Some detailed techniques used for privacy preserving computations

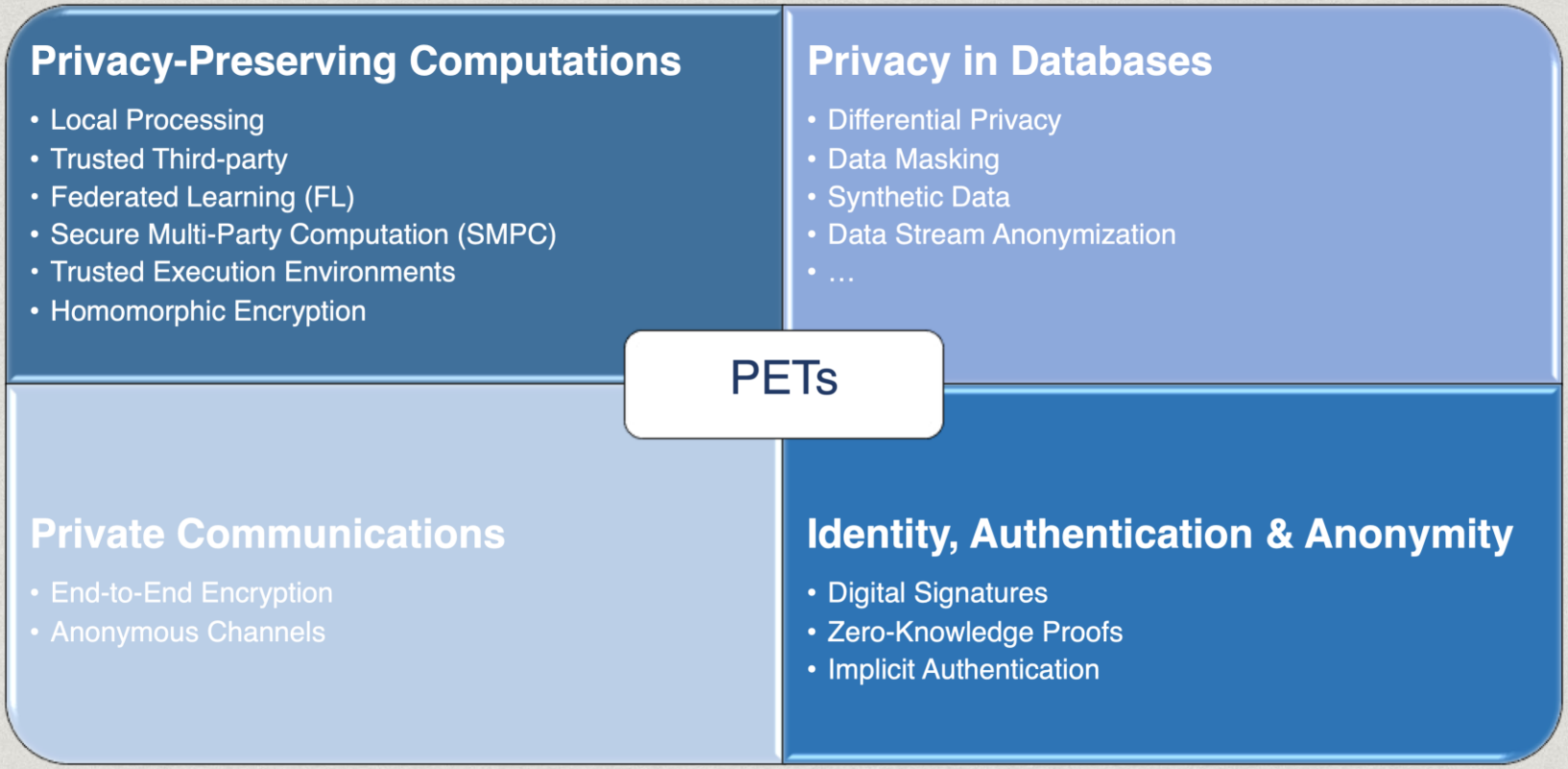
Privacy Enhancing Technologies (PET)

Privacy-enhancing technologies (PETs) are a broad range of technologies that are designed to extract data value in order to unleash its full potential, without risking the **privacy and security** of this information.

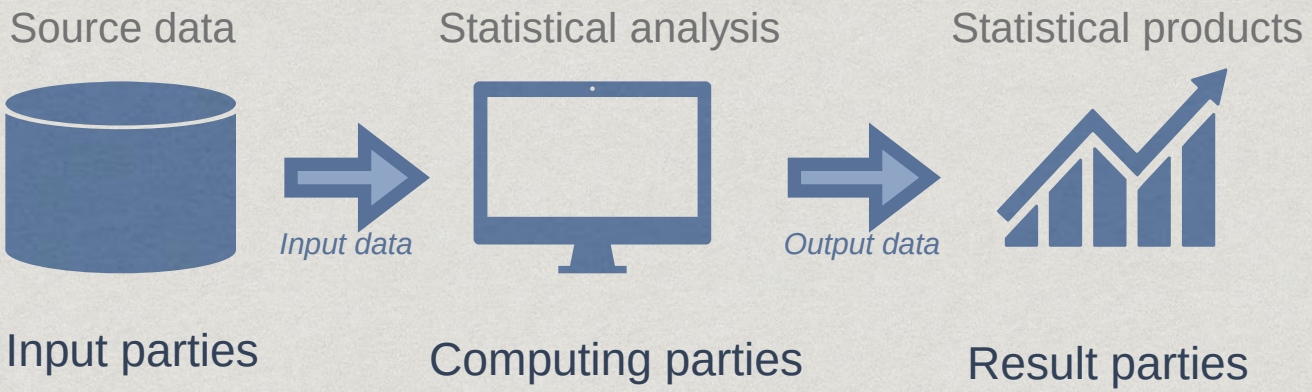
Importance for businesses:

- Compliance to data protection laws such as GDPR and CCPA
- Reputation of brand
- Data may need to be processed by third-party organizations due to the lack of self-sufficiency in analytics.

Classification of PETs

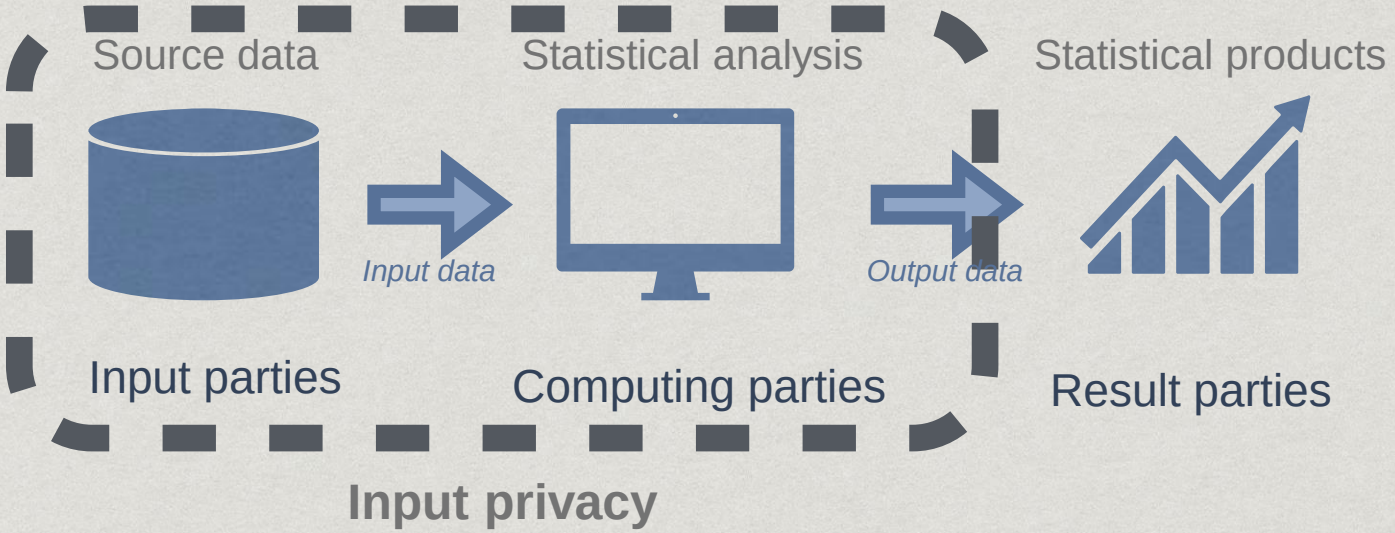


Classification of PETs in data analysis



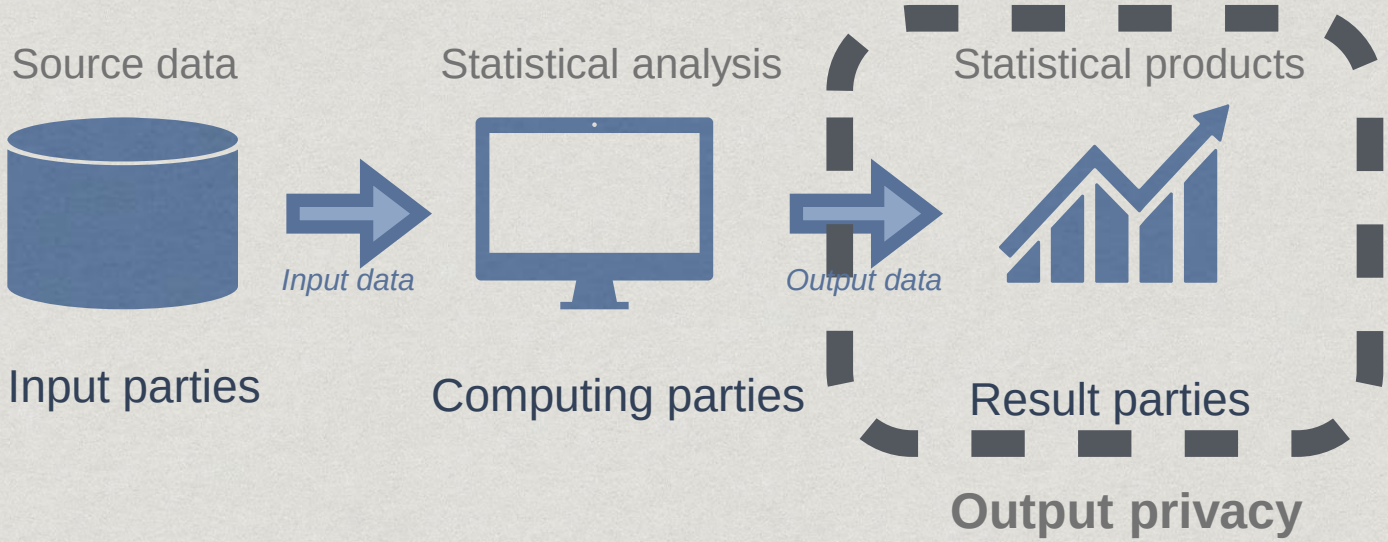
One or more Input Parties provide sensitive data to one or more Computing Parties who statistically analyze it, producing results for one or more Result Parties.

Classification of PETs in data analysis



Computing Party cannot access or derive any input value provided by Input Parties, nor access intermediate values or statistical results during processing of the data.

Classification of PETs in data analysis

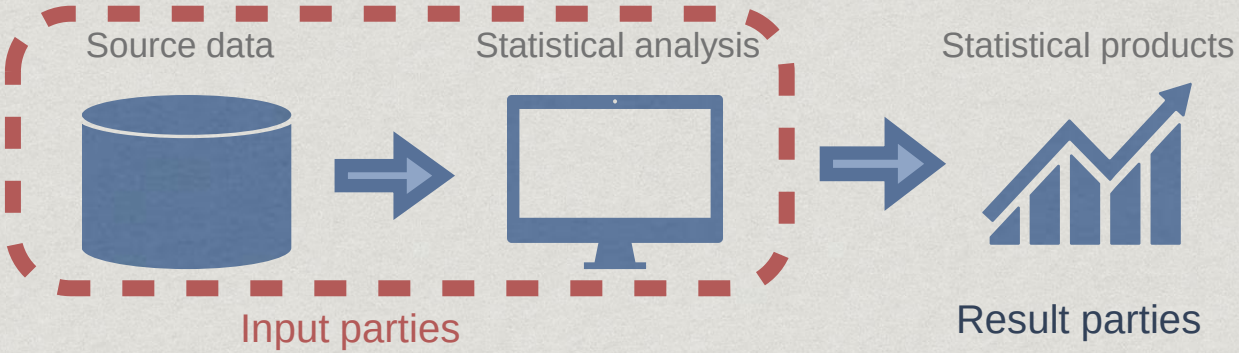


Output results do not contain identifiable input data beyond what is allowable by Input Parties.

Classification of PETs in data analysis

Input privacy preserving	Output privacy preserving
Privacy-Preserving Computation • Local Processing • Trusted Third-party • Federated Learning (FL) • Secure Multi-Party Computation (SMPC) • Trusted Execution Environments • Homomorphic Encryption Zero-Knowledge Proofs	Privacy in Databases • Differential Privacy • Data Masking • Synthetic Data Generation • Data Stream Anonymization • …
Private Communications - End-to-End Encryption - Anonymous Channels	

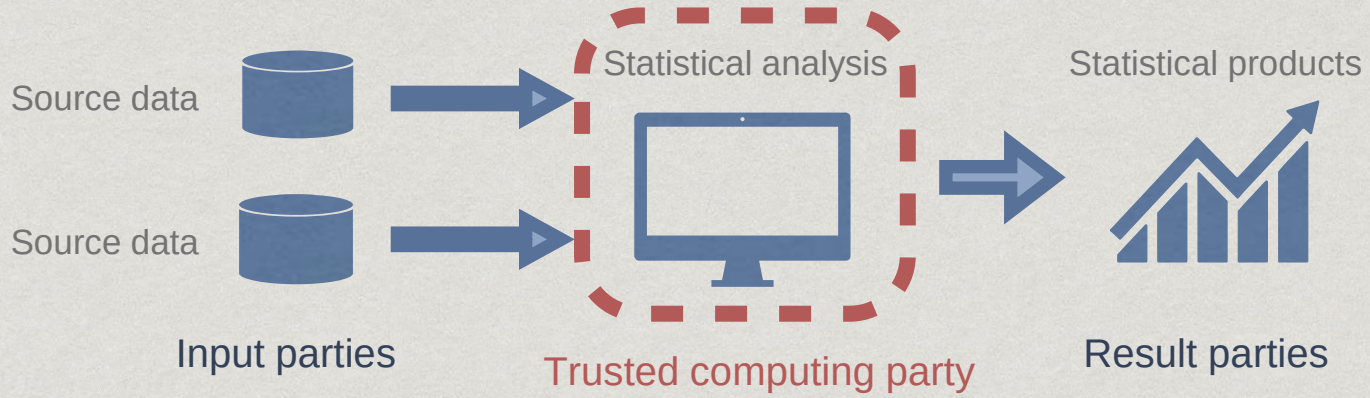
Local Processing



Input parties compute tasks for the output parties on their local infrastructure

- Source data kept in the input party, which has control over processing tasks
- Computing power is required to sit next to the data

Trusted Third-party

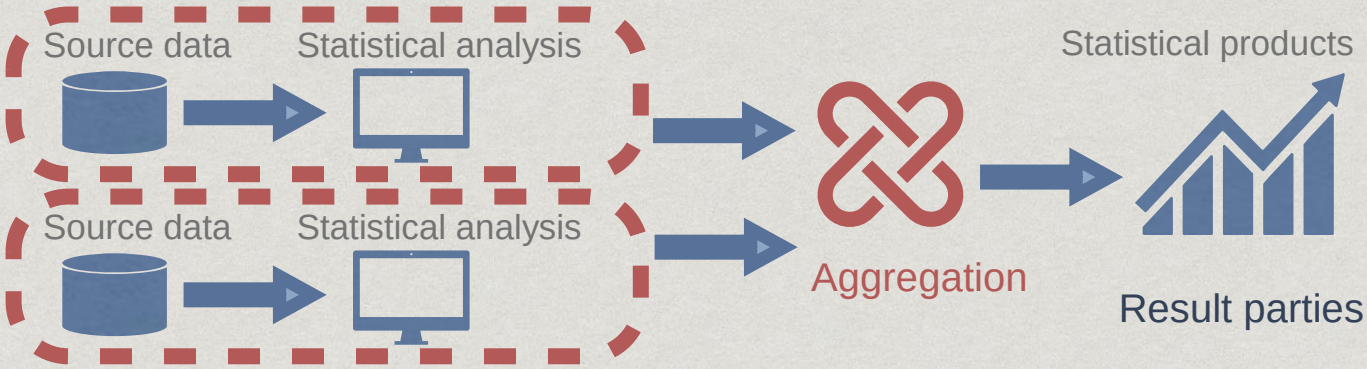


If data is located across several collaborating parties that do not want to share data among themselves, one can use a third-party.

Suitable for combining data from multiple input parties

Surface of attack is extended to the trusted party since data is still copied

Federated Learning (FL)

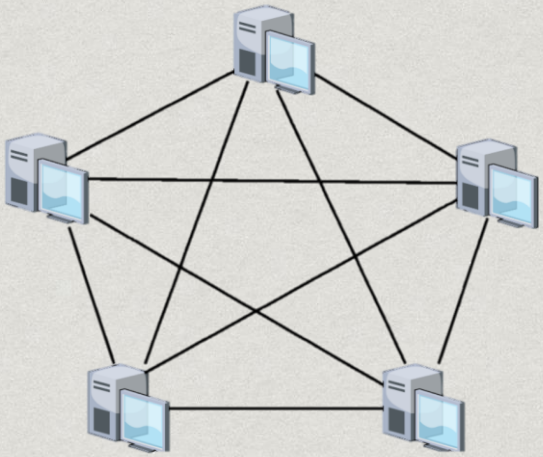


Processing/learning tasks are distributed across all input parties

Eliminate the need of centralized data in the cloud

- Computing power is required to sit next to the data
- Complexity in calculation (model biases, bandwidth, data availability)

Secure Multi-Party Computation (SMPC)

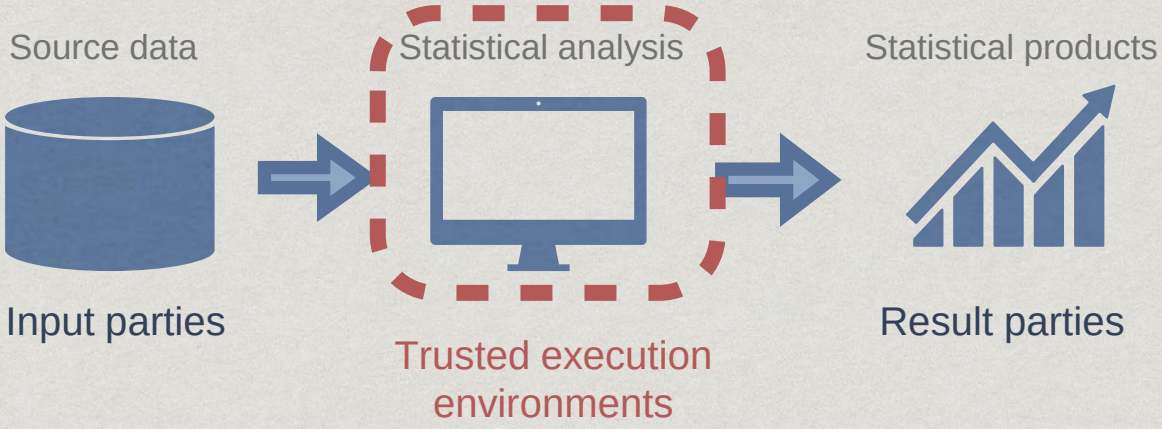


- Computation is spread across all parties with each party get some random pieces of input from other parties
- The parties gain no additional information about each other's inputs
- The computation output from each party is eventually reconstructed to produce the final output

- Same as Federated Learning
- Can gain collective intelligences on inputs from all parties

- Complexity in managing distributed learning tasks as in FL
- Little research done on performing comparison (<, >, ==, !=) within MPC protocols

Trusted execution environments (TEEs)



hardware which protects the data inside from being seen

- Guarantees of integrity and confidentiality
- Require specialized hardware to run

Thank you!

Any question?

Reference

Domingo-Ferrer J., Blanco-Justicia A. (2020) Privacy-Preserving Technologies. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_14

Miller, R. (2019). Emerging privacy preserving technologies are game changing. Medium. https://medium.com/@bertcmiller/emerging-privacy-preserving-technologies-are-game-changing-f32f06ac6aa

M. (2021). The two Families of Privacy-preserving Technologies & How to Choose. Medium. https://medium.com/sarus/the-two-families-of-privacy-preserving-technologies-how-to-choose-60ab34a3969f

Apfelbeck, F. (2020). Evaluation of Privacy-Preserving Technologies for Machine Learning. Medium. https://medium.com/outlier-ventures-io/evaluation-of-privacy-preserving-technologies-for-machine-learning-8d2e3c87828c

Kantarci, A. (2021). *Top 10 Privacy Enhancing Technologies (PETs) in 2021*. AIMultiple. https://research.aimultiple.com/privacy-enhancing-technologies/

UN handbook on Privacy-Preserving Computation Techniques. (2019). UN Global Working Group (GWG) on Big Data. http://publications.officialstatistics.org/handbooks/privacy-preserving-techniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf

How to anonymise your datasets?

Privacy Preserving DatabaseTechnologies

ZIHUAN RAN, APR 2021

Outline

Privacy and Anonymised Data

Statistical Disclosure Control(SDC) Techniques

Level of Anonymisation: Privacy Models

Data Privacy in Data Mining

“To anonymise datasets while preserving the utility.”

To wipe out the connection between an individual’s identity and the individual’s data.

“Statistical Disclosure Control(SDC)”

- Non-perturbative Masking
- Perturbative Masking
- Synthetic Micro-data Generation
- Techniques for Textual Data
- Techniques for Stream Data

Masking: Non-perturbative Masking

Form a dataset X' without perturbing values in X, just by making it more general.

- **Sampling**
  - 10k records -> 1k records, randomly
- **Generalisation**
  - "Los Angeles" -> "CA"/"US"
- **Top/bottom coding**
  - age 27 -> age group "25-40"
- **Local suppression**
  - replace some attributes with missing value -> lower # records sharing such attributes

Masking: Perturbative Masking

Form a dataset X' by changing some values in X in microscope.

- **Noise adding**
  - income 10k -> income 10k$\pm\omega$, with ω being the noise
- **Data swapping**
  - attribute "age" swapped randomly. Distribution of "age" is preserved, but multivariate distribution harmed.
- **Microaggregation**
  - 3 record(age 27, 28, 30) -> 1 record(age 28.33…)

Synthetic Micro-data Generation

Regenerate a new, artificial dataset using the statistical properties of the real, sensitive data.

- **Example**:

Original data(100 records) has attribute “income”, with mean at 50k variance at 1.86, approximately normally distributed.

=> Generate 100 new points on Normal distribution N(50k, 1.86), taking them as the “income” attribute.

- **Pros**: fully eliminate the use of sensitive original data
- **Cons**: possible re-match between respondent and records due to similarity; only chosen stats properties preserved.
- **Improvements**: synthetic sensitive attributes, keep others original.

Textual Data

Sensitive texts in documents: to wipe them, or to generalise them?

- **Redaction**
  - fully wiped out
  - but this blank itself tells something
- **Sanitisation**
  - generalise “AIDS” to “disease”, without being noticed.
- A tool to sanitise: Named Entity Recognition (NER)

Stream Data

Fast, effective privacy-preserving treatment to streaming data.

- **Perturbative masking**
  - add Laplacian noise to each record
- **Non-perturbative masking**
  - aggregate records at receiving
- **Counterfeiting**
  - Hide this real record (“Lisa”, 34, 50k) in a group of artificial records like (“Li”, 23, 28k), (“Lau”, 56, 23k),…

Level of Anonymisation: Privacy Models

Some criterions that tell us how anonymised are datasets after processing.

- **k-Anonymity**

  At least k records with the same attribute tuple.

- **Differential Privacy**

  ε-differentially private algorithm: the output is ε-similar with/without any single record.

- **Permutation Model**

  permutation(d, v) + noise.

Data Privacy in Data Mining

How to achieve privacy-preserving data mining?

- **Perturbation**

  Based on SDC techniques, aiming to provide accurate stats at macro-level while perturbing individual records at micro-level.

- **Secure Multiparty Computation(SMC)**

  Like distributed computing, to separate data into different parties, and use cryptography to ensure computations achieved while data not disclosed.

References:

- Domingo-Ferrer J., Blanco-Justicia A (2020) Privacy-Preserving Technologies. In: Christen M., Gordijn B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_14
- Florian Apfelbeck, (2018) Evaluation of Privacy-Preserving Technologies for Machine Learning. Outlier Ventures. https://medium.com/outlier-ventures-io/evaluation-of-privacy-preserving-technologies-for-machine-learning-8d2e3c87828c
- Privacy Models, ARX-Data Anonymization Tool. https://arx.deidentifier.org/overview/privacy-criteria/
- Soria-Comas, J., Domingo-Ferrer, J. Big Data Privacy: Challenges to Privacy Principles and Models. *Data Sci. Eng.* **1,** 21–28 (2016). https://doi.org/10.1007/s41019-015-0001-x
- Finkel JR, Grenager T, Manning C (2005) Incorporating non-local information into information extraction systems by gibbs sampling. Proceedings of the 43rd annual meeting on association for computational linguistics. Assoc Comput Linguist:363–370
- Kim S, Sung MK, Chung YD (2014) A framework to preserve the privacy of electronic health data streams. J Biomed Inf (Elsevier) 50:95–106

5G AND DATA PRIVACY

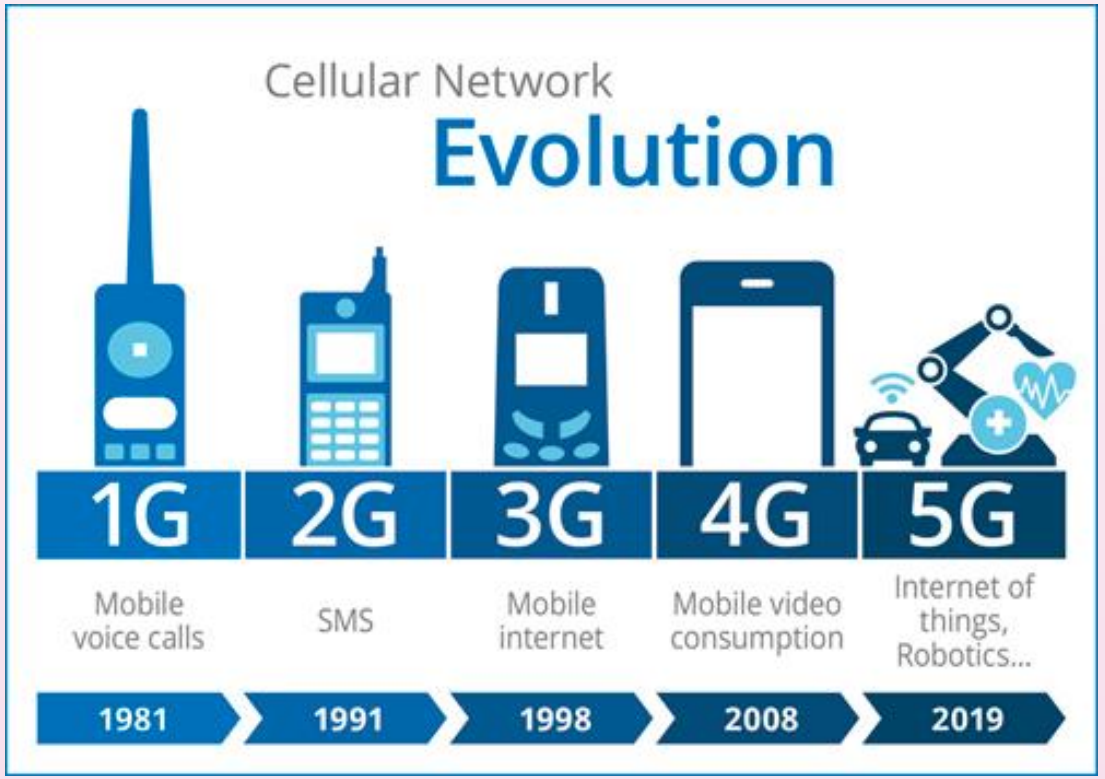
BY AZIZA SAULEBAY

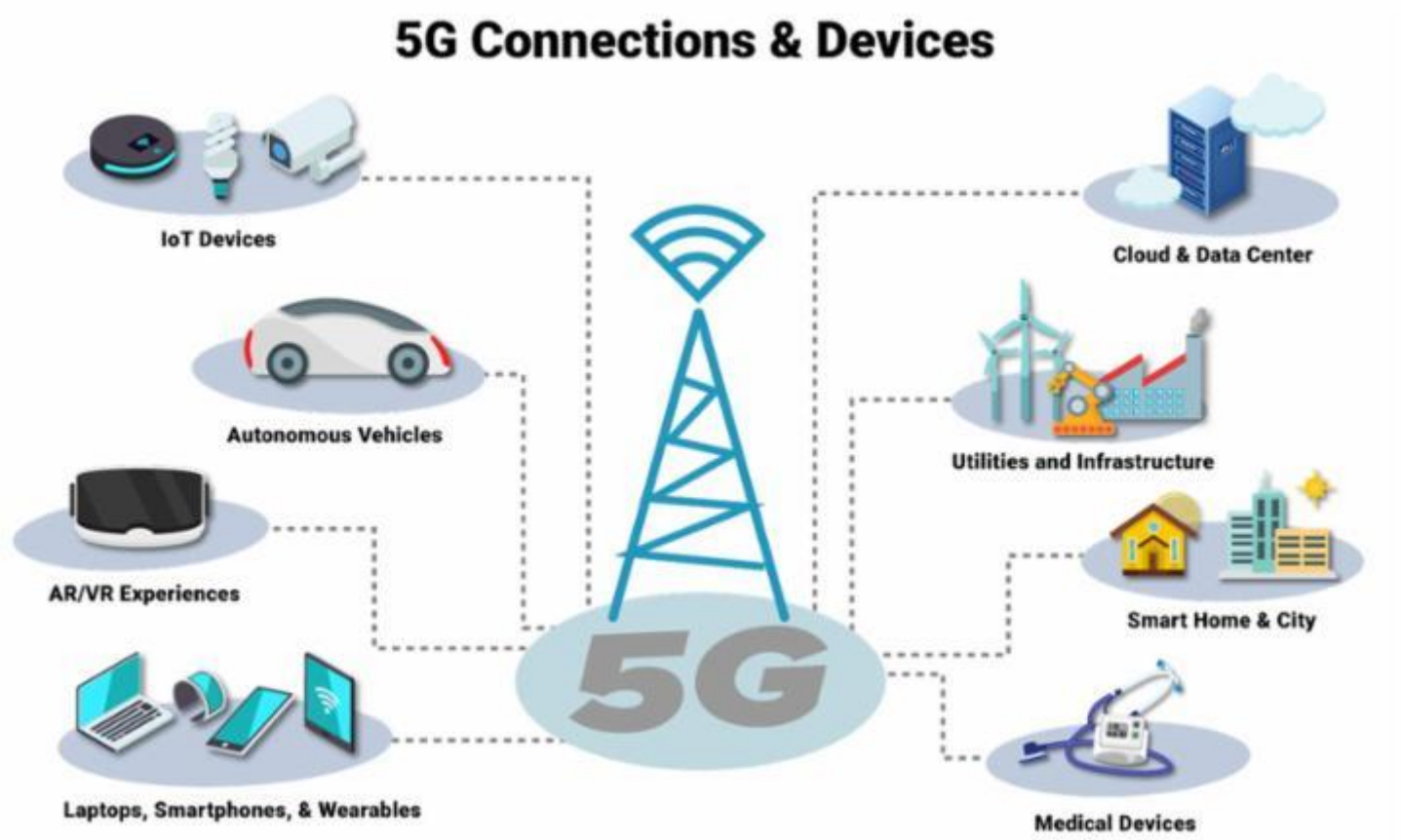
WHAT IS 5G?

5G IS THE 5TH GENERATION MOBILE NETWORK.

IT IS A NEW GLOBAL WIRELESS STANDARD AFTER 1G, 2G, 3G, AND 4G NETWORKS.

5G ENABLES A NEW KIND OF NETWORK THAT IS DESIGNED TO CONNECT VIRTUALLY EVERYONE AND EVERYTHING TOGETHER INCLUDING MACHINES, OBJECTS, AND DEVICES.




5G Connections & Devices
IoT Devices
Autonomous Vehicles
AR/VR Experiences
Laptops, Smartphones, & Wearables
5G
Cloud & Data Center
Utilities and Infrastructure
Smart Home & City
Medical Devices

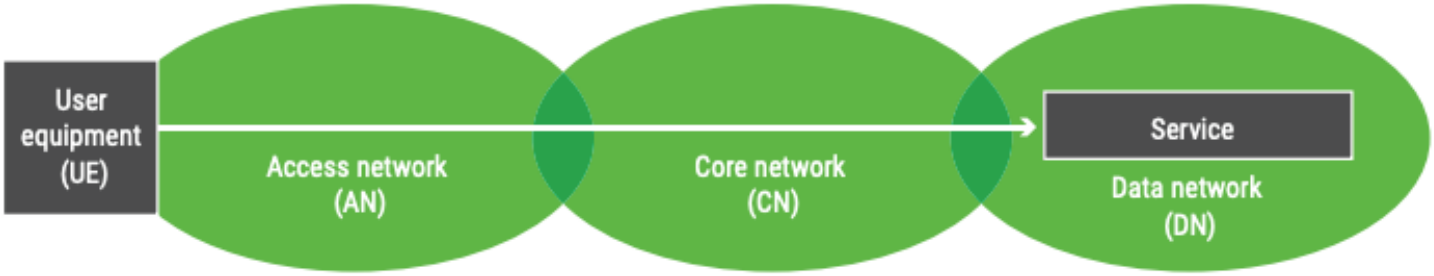
WHY TO USE 5G?

The Main Features of 5G

Speed	Capacity	Latency/ Response time	Connection	Mobility	Battery life
10 to 20 Gbps	10 TB/s/km^2	Ultra-reliable low-latency communication (URLLC): 1 millisecond Enhanced Mobile Broadband (eMBB): 4 millisecond	1,000,000 devices/km^2	500+ km/hour	15+ years
10-100x of 4G	1000x of 4G	1/10 of 4G	100x of 4G	1.5x of 4G	10x of 4G

Source: GSMA, EY

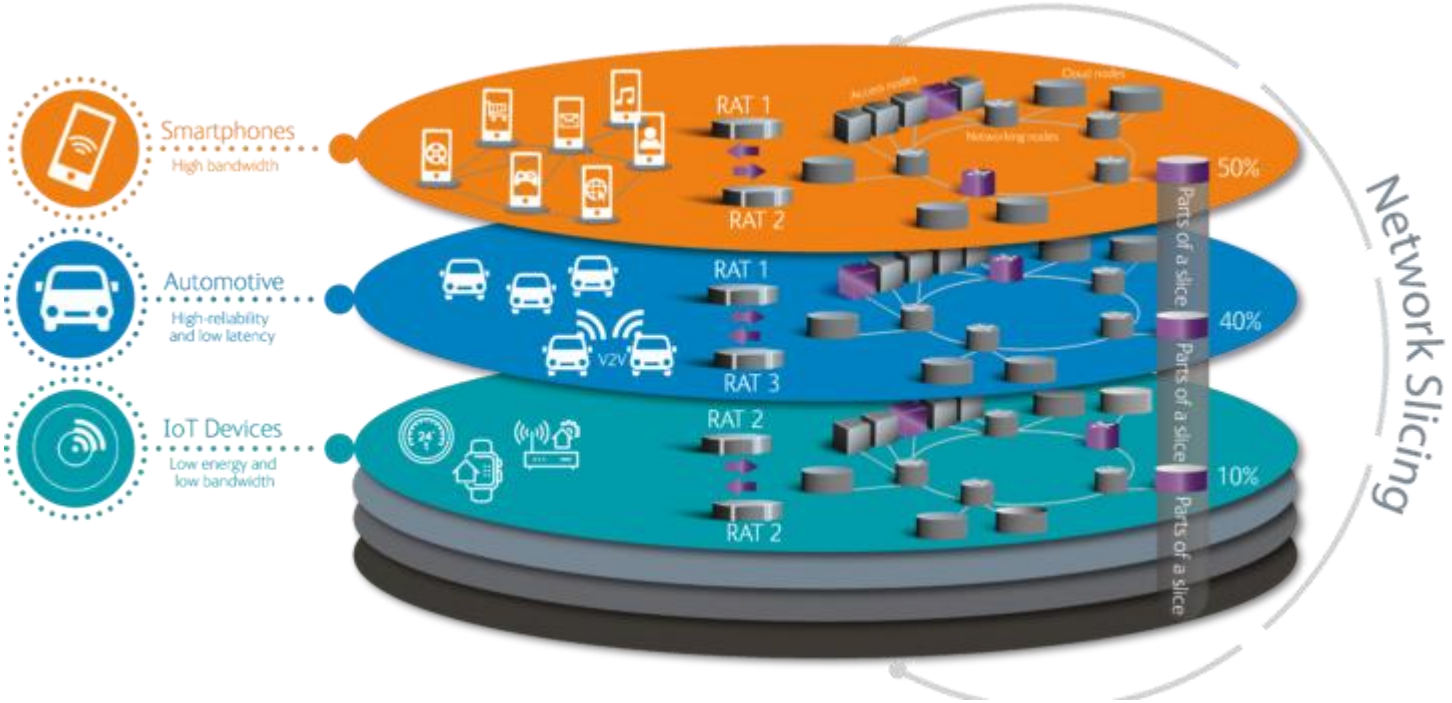
WILL 5G TECHNOLOGY BE SECURE?



- Radio access network (RAN) takes signals from cellphones and other devices and transmits them back to the core, using cellphones, towers or base stations. Elements of RAN include:
- User equipment (UE)
- Radio unit (RU), which is an element that connects user equipment with the network

- The 5G core network uses cloud-aligned, service-based architecture (SBA) that spans all 5G functions and interactions, including:
- Authentication
- Security
- Session management
- Aggregation of traffic from end devices

5G maintains clear separation between RAN and the core network



EACH "SLICE" OR PORTION OF THE NETWORK CAN BE ALLOCATED BASED ON THE SPECIFIC NEEDS OF THE APPLICATION, USE CASE OR CUSTOMER.

5G THREATS AND MITIGATING SECURITY CONTROLS

I. Authentication	
Threats	**5G Security Features (Mitigating Controls)**
• Bidding down attacks	• Subscription authentication • Enhanced subscriber privacy • Network authorizations
• Exploitation of user plane integrity	• User plane integrity protection
• Malicious network connection • Connection to network by rogue user equipment • Pretense of user equipment roaming on networks	• Stronger roaming authentication via 5G Authentication and key agreement (5G-AKA)

III. 5G Core Network	
Threats	**5G Security Features (Mitigating Controls)**
• Abuse of remote access threat and authentication traffic spike due to malicious acts • Abuse of third party-hosted network function threat • Application programming interface (API) exploitation threat	• Security-enhancing network functions (NFs) • Interoperator security

5G THREATS AND MITIGATING SECURITY CONTROLS

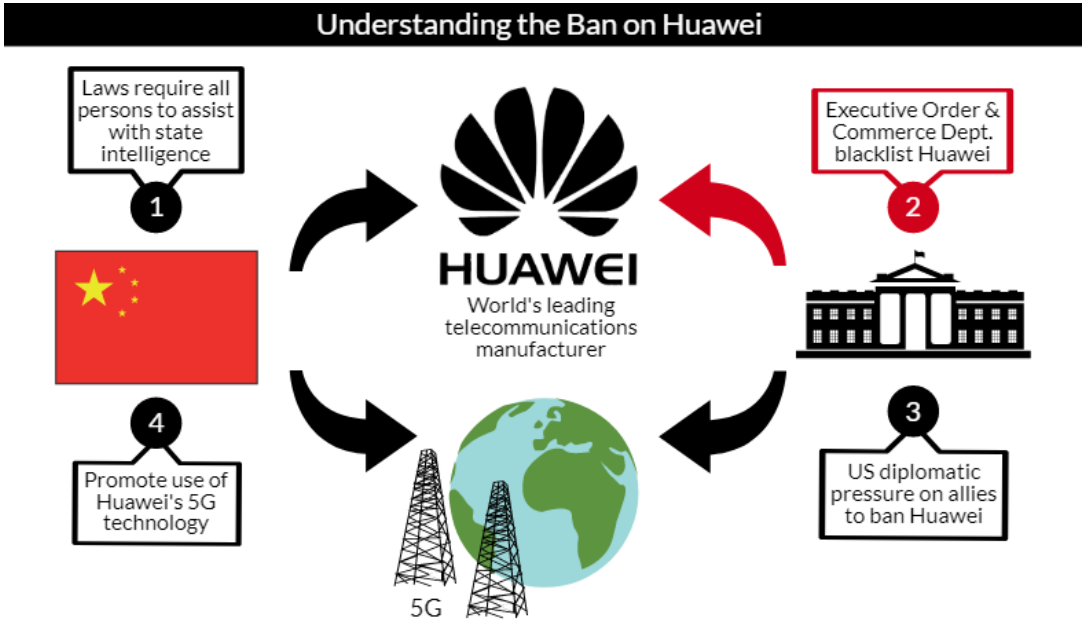
II. 5G Radio Access Network (RAN)	
Threats	**5G Security Features (Mitigating Controls)**

• Sensitive data vulnerability because of physical attacks due to unencrypted or poorly encrypted radio units (RUs)/distributed units (DUs)Higher risk of attackers due to the introduction of new interfaces for core/user plane and 5G core network resulting in:
  • More attackers
  • Network disruptions
  • Fake access network node threat
  • Flooding attack threat via interface flooding
	• Restriction of sensitive data via encryption of user equipment communications
	• RAN interface protection

5G: WHAT ARE THE OTHER ISSUES?

- Many countries are preparing to move from 4G to more advanced 5G mobile networks.
- Huawei, a Chinese company with global ambitions, seems to be on course to become dominant in 5G, establishing new pilots and partnerships worldwide. The current degree of consolidation in the industry exacerbates the risks of market failure.
- With 5G – involving massive machine-to-machine communications – perimeter cyber defense will no longer be effective as it will be impossible to grant access exclusively to authorized devices.
- Potential espionage and transparency concerns are compounded by Huawei's growing importance as the largest provider of 5G equipment globally.

POLITICAL IMPLICATIONS BEHIND



Huawei says it's never been asked to spy and "would categorically refuse to comply". It adds: "We would never compromise or harm any country, organization, or individual, especially when it comes to cyber-security and user privacy protection."

The issue of aggregation of data in one place and "major dependency on a single supplier" was a focal point of the escalating political issues between China, United States and other countries.

The reasons for that:

- Chinese companies have direct political connections to their government, including to the intelligence community due to local law.
- China's internal big data policy – based on massive surveillance and limited privacy
- Huawei's ownership structure – being "effectively state-owned."
- The concern is that state-sponsored hackers could use these devices, which often have weaker security features, as back doors into strategically vital networks.

Countries that restrict access to its 5G network from Chinese companies	Countries that put more stringent rules and procedures	Countries that have already adopted Chinese 5G technology
In May 2019, the US Commerce Department banned US companies from selling any products to Huawei and blacklisted company. But, not yet entered into force due to 90-day extensions that have been renewed four times.	Italy, have not placed a ban on Chinese 5G equipment manufacturers but have already committed to stricter regulations.	Hungary and Spain
The UK government has announced that will ban UK mobile providers from buying new Huawei 5G equipment after the end of this year and they will have to remove all of its 5G kit from their networks by 2027.	Germany Deutsche Telekom has already announced that it will continue working with Chinese 5G providers.	Indonesia and the Philippines

CONCLUSION

THE DISCUSSION ON 5G WILL CONTINUE IN THE MONTHS AND YEARS AHEAD. IT IS IMPORTANT THAT ALL ALLIES BE FLUENT WITH THE DISCUSSION AND UNDERSTAND THE IMPLICATIONS OF THIS TRANSITION: AT THE ECONOMIC, POLITICAL AND MILITARY LEVELS. WITHOUT A SINGLE DOMINANT PLAYER, THIS SOLUTION COULD ALLOW THE ALLIES TO ACHIEVE SECURITY AND PRIVACY WITHOUT COMPROMISING THEIR ECONOMIC EFFICIENCY, TO HAVE ACCESS TO AN EFFECTIVE AND RESILIENT COMMUNICATIONS NETWORK FREE FROM SUPPLY DISRUPTIONS.

Messaging Application Security and Privacy

Carol Varkey

April 16, 2021

DSCI 529

Outline

Background

- Definition: "Software that enables messages to be sent and received…(known as) instant messaging" (1)
- These messaging apps are deployed/used on mobile devices, as an additional service to social media platforms, or on their own online messenger platform
- Prominent Messaging Applications Over the Years: Quantum Link, AOL Instant Messenger (AIM)
- Ex: **WhatsApp, Facebook Messenger, Signal, WeChat, Telegram**
- Introduction of Smartphones and Monetization (Text/Email → Messaging Apps)

What Data is Collected by the Platform

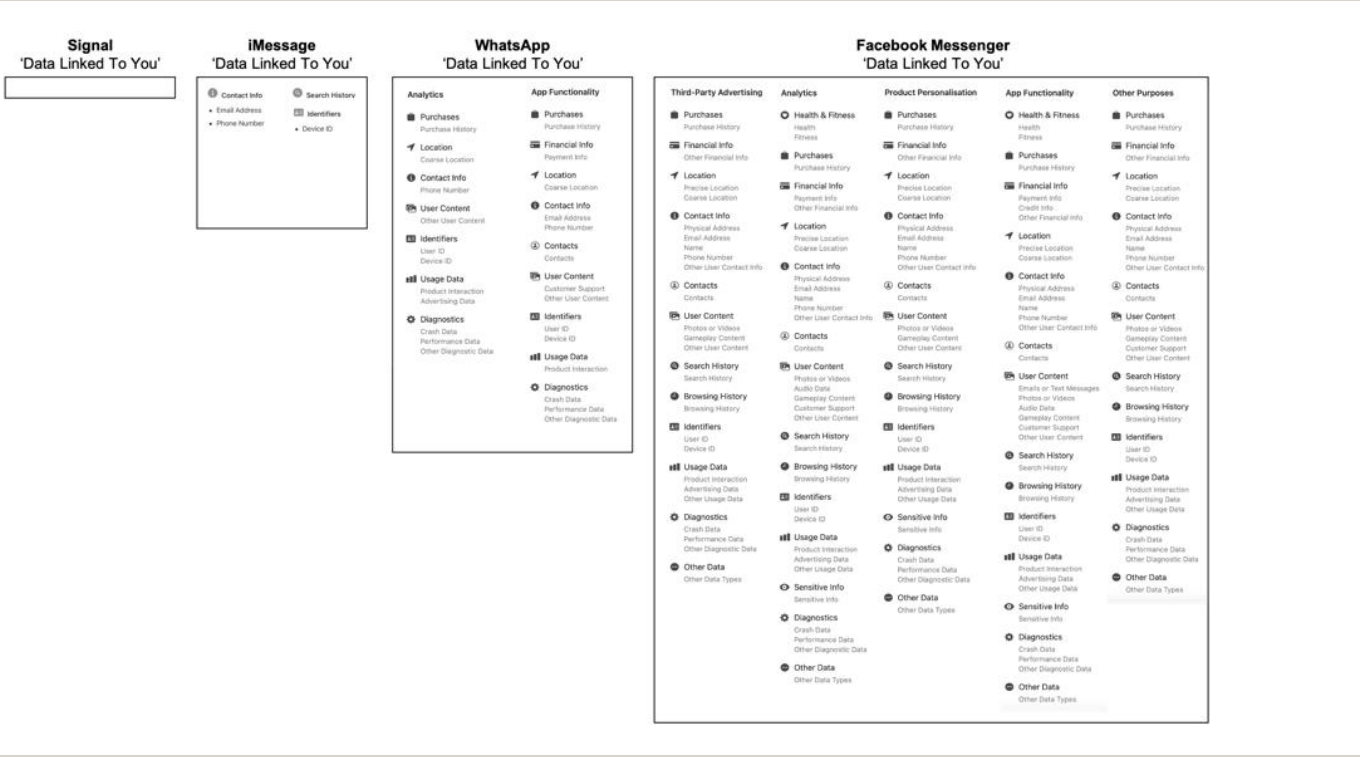
Dependent on the given Messaging App

- Registration Information (Phone Number, Email etc.)
- Metadata: Including sender/receiver IDs, time of message delivery, login times, IP addresses, device types, call duration
- Address Book
- Message Contents/File's Shared

Apple privacy nutrition label for select apps

Messaging apps	Number of data types collected		
	Data linked to you	Data used to track you	Data not linked to you
Messenger	14	0	0
WeChat	11	1	0
WhatsApp	9	0	0
Telegram	3	0	0
Messages	3	0	3
Signal	0	0	1

What Data is Collected by the Platform



Security and Privacy Concerns

Security Vulnerabilities

- Authentication and Account Hijacking: Based on weaknesses in authentication mechanisms that can lead to hijacking/impersonation
- Data Breaches: Unauthorized access to platform's data servers/cloud resources
- Backups on the Cloud
- Sender ID Spoofing/Message Manipulation: Forging of sender information or messages during transfer; less common

Privacy Issues

- Surveillance
- Eavesdropping
- User Profiling via Address Book Matching
- Spam

Security/Privacy Measures

- **Encryption**: Messaging app uses some form of encryption (not all forms equally secure)
  - End-To-End Encryption (most secure)
    - Can be implemented but may not used by default ("Secret Chat", "Private Conversation")
    - Private key on the local device only → there are concerns on the platforms access to this private key, and key management
  - Encryption In Transit
    - Stored in clear-text → enables access from the platform, third parties etc.

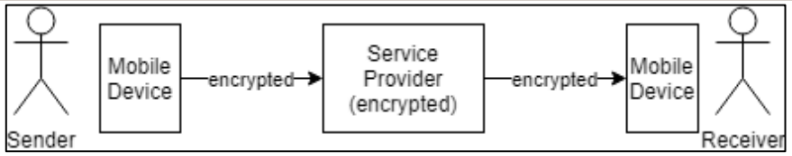


Figure 1. End-to-end Encryption

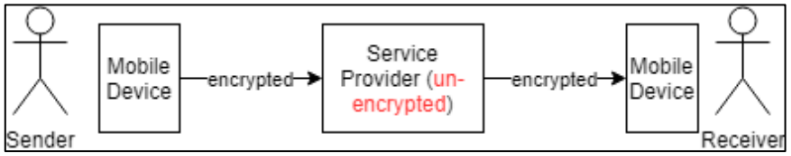


Figure 2. Encryption in Transit

Security/Privacy Measures

- Message Deletion
  - From the Message Apps Servers
  - For sender's message
    - Self-Deleting messages after a set time
- Authentication Mechanisms → For Registration and proceeding Logins
  - Password Locks
  - Multi-Factor Authentication
- Remote Logout
- Source Code Review/Transparency

Messaging App	End-to-end encryption	Encryption in Transit	Private key not accessible by provider	Deleted from Server	Self-Destruct Messages	Open-Source	Password lock	Verification SMS/Email	Screenshot detection	Two-step Verification	Remote logout	Remotely Wipe Messages	Account self-destruct	Free
Confide	✓							✓						
CoverMe	✓				✓							✓		
Dust	✓			✓	✓				✓					✓
Hangouts		✓												✓
iMessage	✓		✓	✓	✓									✓
Line	✓							✓						✓
Messenger	✓(optional)	✓			✓									✓
Signal	✓				✓	✓	✓							✓
Skype	✓(optional)	✓												✓
Slack		✓												✓
Snapchat	✓													✓
Telegram	✓(optional)	✓	✓		✓	✓	✓			✓	✓		✓	✓
Threema	✓													
Viber	✓		✓	✓	✓		✓							✓
WeChat														✓
WhatsApp	✓		✓				✓	✓				✓		✓
Wickr Me	✓								✓					

WhatsApp Case Study

- WhatsApp's Privacy Policy Update highlights privacy concerns on their data sharing practices
  - Sharing of data for chats with Business Account
  - Sharing of data with Facebook
- Compromising Privacy From Functionality

> To give you enough time to review changes at your own pace and convenience, we've extended the effective date to May 15th. If you haven't accepted by then, WhatsApp will not delete your account. However, you won't have full functionality of WhatsApp until you accept. For a short time, you'll be able to receive calls and notifications, but won't be able to read or send messages from the app.

- WhatsApp has a separate privacy policy for Europe, as a result of GDPR
- "**WhatsApp's new 'privacy' policy is a gift to other messaging apps**" [15]
- Users shift to more secure messaging app platforms
  - **Signal, Telegram**

References

(1) "Definition of Messaging App." *PCMag*, www.pcmag.com/encyclopedia/term/messaging-app.

(2) Dickson, Ben. "How Secure Is Your Messaging App?" *PCMag*, 26 Dec. 2018, www.pcmag.com/news/how-secure-is-your-messaging-app.

(3) Barot, Trushar, and Eytan Oren. "A Brief History of Chat Apps." *A Brief History of Chat Apps · Guide to Chat Apps*, Nov. 2015, towcenter.gitbooks.io/guide-to-chat-apps/content/introductionthe_dawn_of/a_brief_history.html.

(4) Botha, J., et al. "A Comparison of Chat Applications in Terms of Security and Privacy." *ResearchGate*, Conference: A Comparison of Chat Applications in Terms of Security and Privacy, www.researchgate.net/publication/334537058_A_Comparison_of_Chat_Applications_in_Terms_of_Security_and_Privacy.

(5) Mueller, Robin, et al. "Security and Privacy of Smartphone Messaging Applications." *International Journal of Pervasive Computing and Communications*, vol. 11, no. 2, June 2015, pp. 132–150., doi:10.1108/ijpcc-04-2015-0020.

(6) Noé, Guillaume. "Privacy Dilemmas of (In)Secure Messaging Apps." *CPO Magazine*, CPO Magazine, 17 Aug. 2018, www.cpomagazine.com/data-privacy/privacy-dilemmas-of-insecure-messaging-apps/.

(7) Cheng, Yao, et al. "Bind Your Phone Number with Caution: Automated User Profiling through Address Book Matching on Smartphone." *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security - ASIA CCS '13*, May 2013, pp. 335–340., doi:10.1145/2484313.2484356.

(8) Gupta, R.. "Common Vulnerabilities and Risk Analysis in Messaging Applications in Social Media with special reference to Whatsapp." (2016).

(9) Schrittwieser, Sebastian, et al. *Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications*. SBA Research GGmbH, Jan. 2012, www.researchgate.net/publication/230035813_Guess_Who_Is_Texting_You_Evaluating_the_Security_of_Smartphone_Messaging_Applications.

(10) "WhatsApp Privacy Policy." *WhatsApp*, WhatsApp, 4 Jan. 2021, www.whatsapp.com/legal/updates/privacy-policy/?lang=en.

(11) Singh, Jagmeet. "WhatsApp Privacy Policy Update: What Happens When You Don't Accept?" *NDTV Gadgets 360*, Gadgets 360, 22 Feb. 2021, gadgets.ndtv.com/apps/news/whatsapp-privacy-policy-update-changes-what-happens-if-you-dont-agree-details-facebook-data-2376020.

(12) Tripathy, Atmaja. "WhatsApp Privacy Policy - a Reboot to a Dangerous Precedent?" *Lexology*, TMT Law Practice, 3 Mar. 2021, www.lexology.com/library/detail.aspx?g=51be5759-742a-4323-b0ce-e80e57997cb2.

(13) Statt, Nick. "WhatsApp Clarifies It's Not Giving All Your Data to Facebook after Surge in Signal and Telegram Users." *The Verge*, The Verge, 12 Jan. 2021, www.theverge.com/2021/1/12/22226792/whatsapp-privacy-policy-response-signal-telegram-controversy-clarification.

(14) -, Cisomag. "Telegram Suffered a Data Breach after Hackers Exposed Personal Details." *Cisomag Cyber Security Magazine*, 26 June 2020, cisomag.eccouncil.org/telegram-data-breach/.

(15) Schuman, Evan. "WhatsApp's New 'Privacy' Policy Is a Gift to Other Messaging Apps." Computerworld, 25 Feb. 2021, www.computerworld.com/article/3608988/whatsapps-new-privacy-policy-is-a-gift-to-other-messaging-apps.html.

Domain Name System (DNS) and Encryption

- Francisco G. Ventura -

Overview

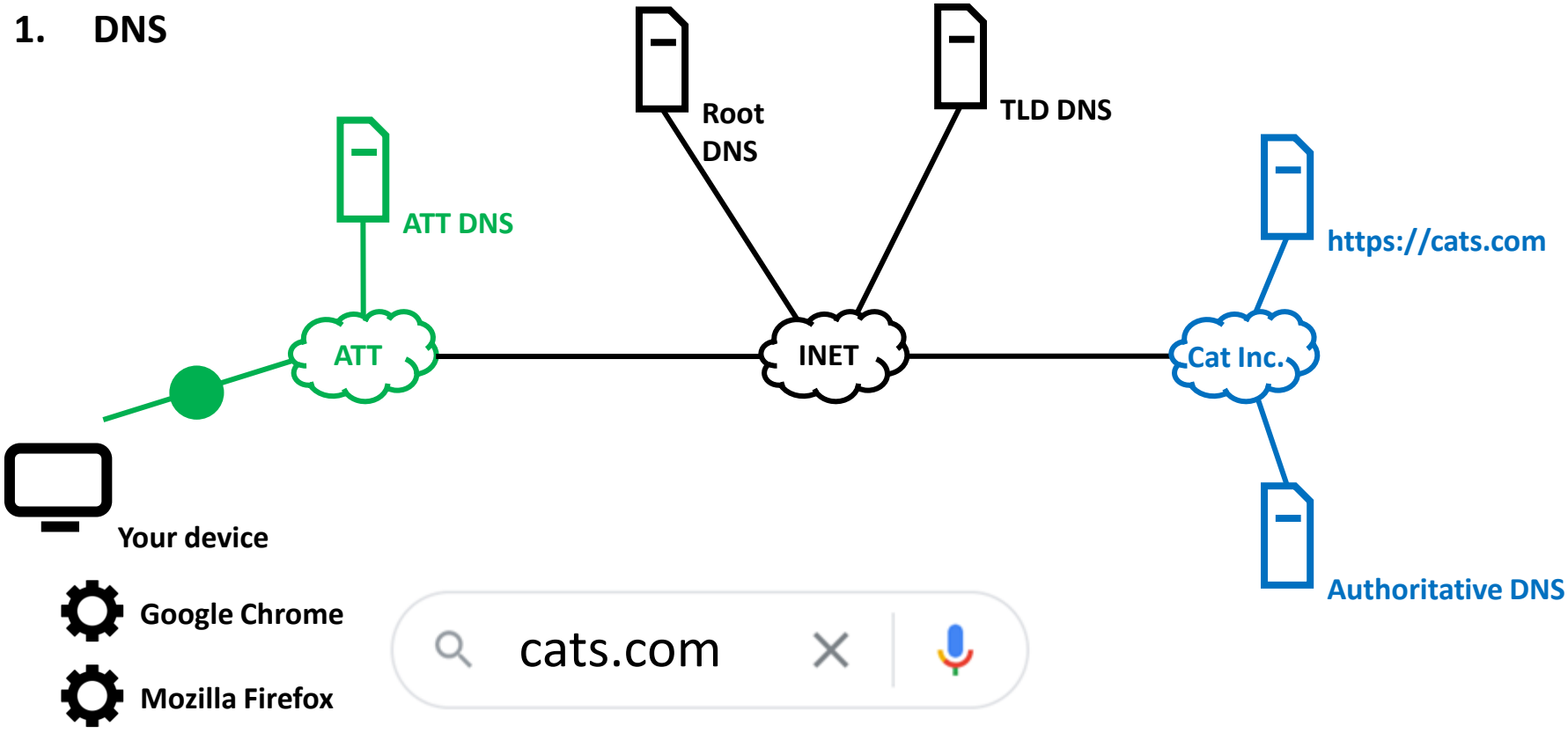
1. **Technology**
   - DNS
   - DNS over HTTPS (DoH)

2. **Debate**
   - Internet Service Providers
   - Google and Mozilla/Cloudflare
   - Government

3. **Implications**

Technology

1. DNS



Technol

1. DNS

Command Prompt

```
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : attlocal.net
   IPv6 Address. . . . . . . . . . . : 2600:1700:9a20:3d80::21
   IPv6 Address. . . . . . . . . . . : 2600:1700:9a20:3d80:8d23:c962:59af:22c9
   Temporary IPv6 Address. . . . . . : 2600:1700:9a20:3d80:9935:e4cd:b071:65cd
   Link-local IPv6 Address . . . . . : fe80::8d23:c962:59af:22c9%16
   IPv4 Address. . . . . . . . . . . : 192.168.1.95
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::8a96:4eff:fe1e:d0c0%16
                                       192.168.1.254
```

ats.com

Your de

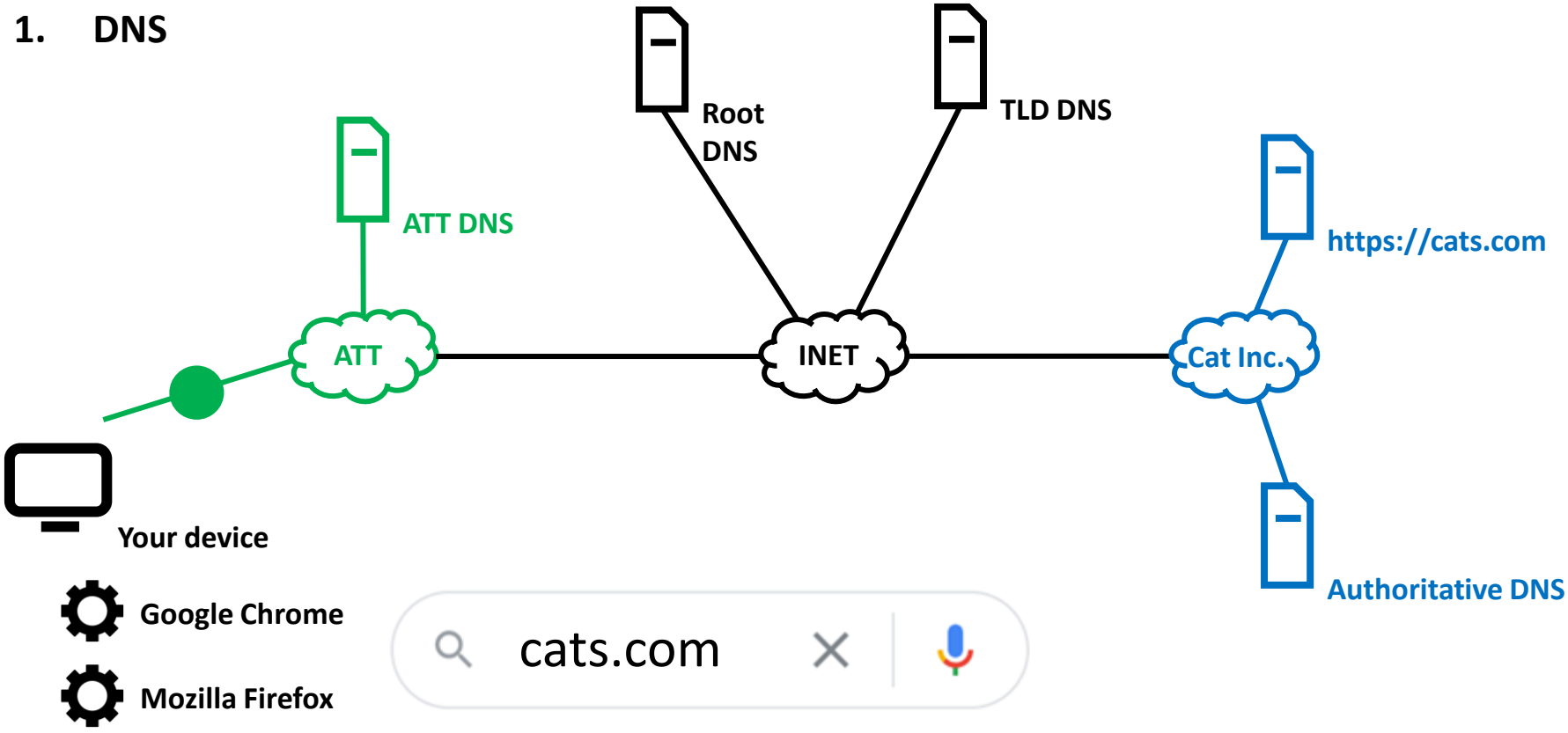
tive DNS

Goog

Mozilla Firefox

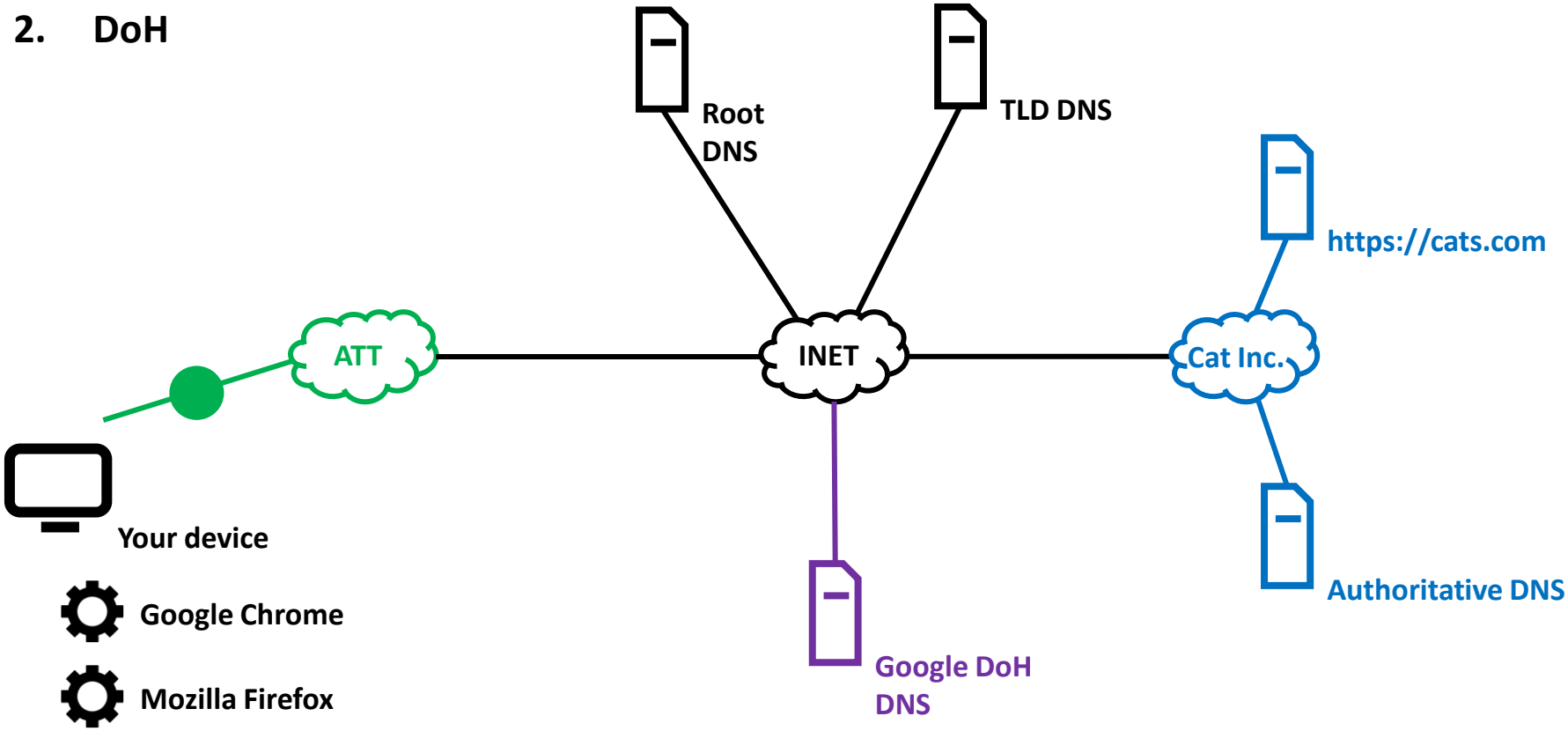
Technology

1. DNS



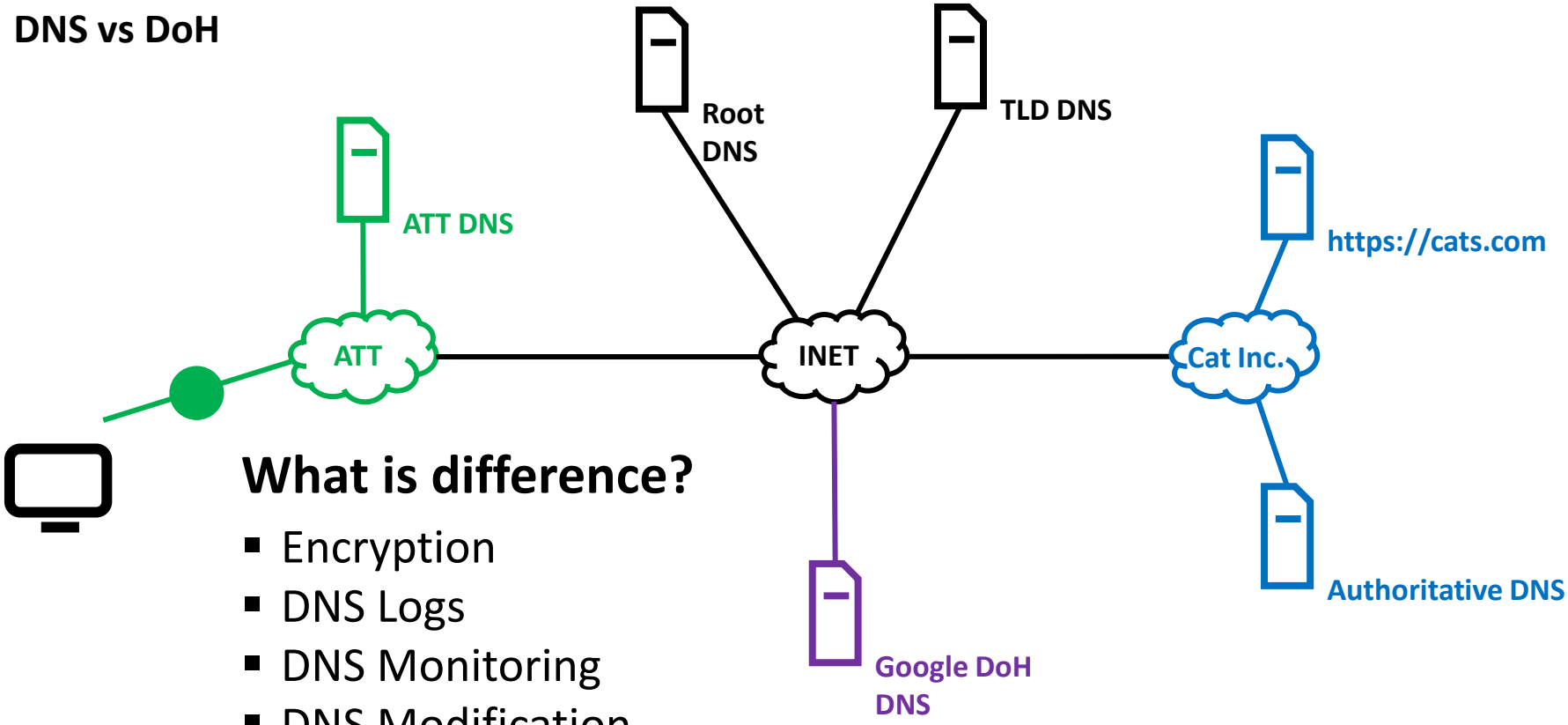
Technology

2. DoH



Debate

DNS vs DoH



What is difference?

- Encryption
- DNS Logs
- DNS Monitoring
- DNS Modification

Debate

DNS vs DoH

"this debate does not centre on the arrival of a new technology… it centres on power… who should regulate the web, and who should be able to exploit our data?"

- Gareth Tyson and Timm Bötger, *The Conversation*, 2019

"digital advertising spending… will grow to 389 billion dollars in 2021"

- *Statista*, 2021

Debate

DNS vs DoH

ncta THE INTERNET & TELEVISION ASSOCIATION

ctia

September 19, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Hon
Ranking
Commit
United S
Washing

The Hon
Ranking
Commit
United States House of Representatives
Washington, DC 20515

The Honorable Roger Wicker
Chairman
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science,
and Transportation
United States Senate
Washington, DC 20510

The Honorable Frank Pallone
Chairman

The Honorable Greg Walden
Ranking Member

moz://a

November 4, 2019

The Honorable Frank Pallone
Chairman
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Greg Walden
Ranking Member
Committee on Energy and Commerce

The Honorable Jan Schakowsky
Chairwoman
Subcommittee on Consumer Protection
and Commerce
U.S. House of Representatives

The Honorable Michael F. Doyle
Chairman
Subcommittee on Communications
and Technology
U.S. House of Representatives

Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

DNS over HTTPS—What Is It and Why Do People Care?

October 16, 2019

Internet pioneer David Clark said: "It's not that we didn't think about security. We knew that there were untrustworthy people out there, and we thought we could exclude them." Those who created the internet were focused on enabling the utility of the network, and a repercussion of their design decisions is that internet security is not inherent but must be retrofitted. Efforts to change one of the internet's hardwired insecurities—the Domain Name System (DNS)—are ongoing but will be disruptive.

How We Get to Websites Today

Debate

DNS vs DoH

Internet Service Providers

- "data competition… in advertising"
  - Chrome > 60% browsers
  - Android OS > 80% mobile
- "fastest, cheapest, most reliable" content distribution networks for consumers
- "creates single point of failure for global internet services"

NCTA, CTIA, and US Telecomm, *Letter to Congress, 2019*

Google/Mozilla

- "necessary to protect users in light of extensive record of ISP abuse of personal data"
  - Selling real time location
  - Verizon's 'Supercookies'
  - ATT's charges to avoid collection

Mozilla Corporation, *Letter to Congress, 2019*

Government

- "complying with law enforcement requests"
  - Content filtering
  - Visibility into logs
- "load management for content delivery networks"
- "international data flow and advertising competition"

Congressional Research Service, *IN11182, 2019*

Implications

Consumer Reports · Electronic Frontier Foundation · NCL

October 22, 2019

The Honorable Lindsey Graham
Chairman
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

The Honorable Jerrold Nadler
Chairman
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable Doug Collins
Ranking Member
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

The Honorable Roger Wicker
Chairman

The Honorable Maria Cantwell
Ranking Member

"ISPs want to protect an illegitimate market of privacy invasive practices to compete with Google's privacy invasive practices; Congress should abolish both."

- Ernesto Falcon, *Electronic Frontier Foundation, 2019*

Questions?

Today's Agenda

12:00 – 12:05 Introduction and Announcements

12:05 – 12:45 Student Presentations – Payments

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – Cryptocurrency - History and Technology
- Saurabh Jain – Privacy of Payment Information
- Yifeng Shi - Financial value of personal Data

12:45 – 13:15 Class Discussion – Payments - Dr. Neuman

13:15 – 13:25 Break

13:25 – 14:15 Student Presentations – Privacy Preserving Technology

- Haipeng Yu - Comparison of privacy preserving technologies
- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

14:15 – 14:50 Class Discussion – Privacy Preserving Tech

14:50 – 15:20 Current Event Discussions

Today's Agenda

12:00 – 12:05 Introduction and Announcements

12:05 – 12:45 Student Presentations – Payments

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – Cryptocurrency - History and Technology
- Saurabh Jain – Privacy of Payment Information
- Yifeng Shi - Financial value of personal Data

12:45 – 13:15 Class Discussion – Payments - Dr. Neuman

13:15 – 13:25 Break

13:25 – 14:15 Student Presentations – Privacy Preserving Technology

- Haipeng Yu - Comparison of privacy preserving technologies
- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

14:15 – 14:50 Class Discussion – Privacy Preserving Tech

14:50 – 15:20 Current Event Discussions

Privacy Preserving Technologies

Technologies that can be employed by users to improve their privacy and security.

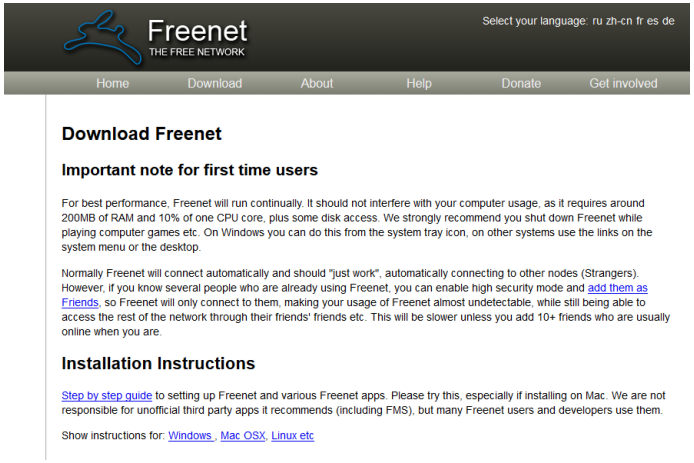
And the negative implications of these technologies.

Storage Encryption

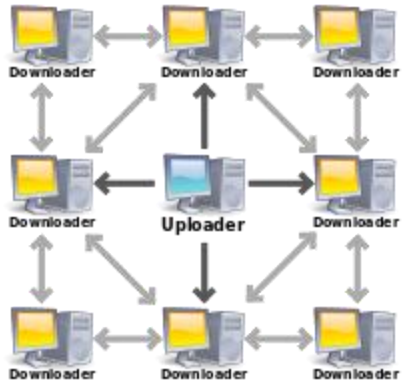
- File Sharing (not necessarily encrypted)
- TrueCrypt
- PGP

File Sharing

- Freenet, bitTorrents, and related protocols and applications support the decentralized storage and distribution of files on the internet.
- Originally intended to provide repositories for data that could not be “silenced”, the content of files are spread across many servers, with duplicate pieces. These pieces are reassembled when users request access to the files.
- They are often used to share protected content in violation of copyright.
- Dangers to users of file sharing services:
  - Most are configured by default to make your machine a distribution point. Download a file, and other may get that file from you.
  - Or worse, files you never requested can be loaded onto your computer and retrieved by others.
- Comparison with TOR

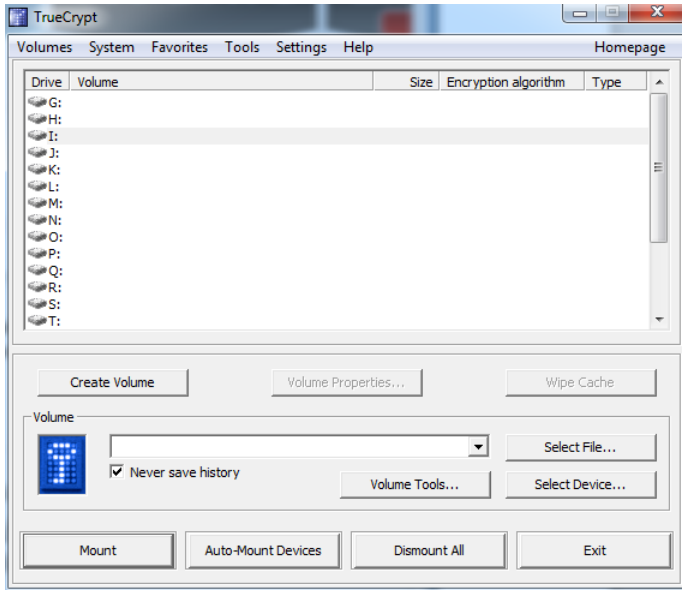


Bittorrent (figure from Wikipedia)



File Encryption

- There are many tools and packages available to encrypt individual files or entire drives. Among these are the whole drive encryption discussed in the intro class, but software tools are also available.
- PGP file encrypt – part of the PGP package discussed earlier allows encryption of files or folders using the public key of an intended recipient (or yourself).



- TrueCrypt was for some time the best option for file encryption, but the last release removed the ability to encrypt files, and was accompanied by statements urging that it not be used. It is widely believed that the previous version is safe.

Some Readings on The Dark Web

- Readings:
  - Time Magazine **The Secret Web: Where Drugs, Porn and Murder Live Online November 11, 2013.**
  - It's About To Get Even Easier to Hide on the Dark Web, Wired 1/28/2017.
  - https://www.vice.com/en_us/article/ezv85m/problem-the-government-still-doesnt-understand-the-dark-web
  - **US government funds controversial Dark Web effort**

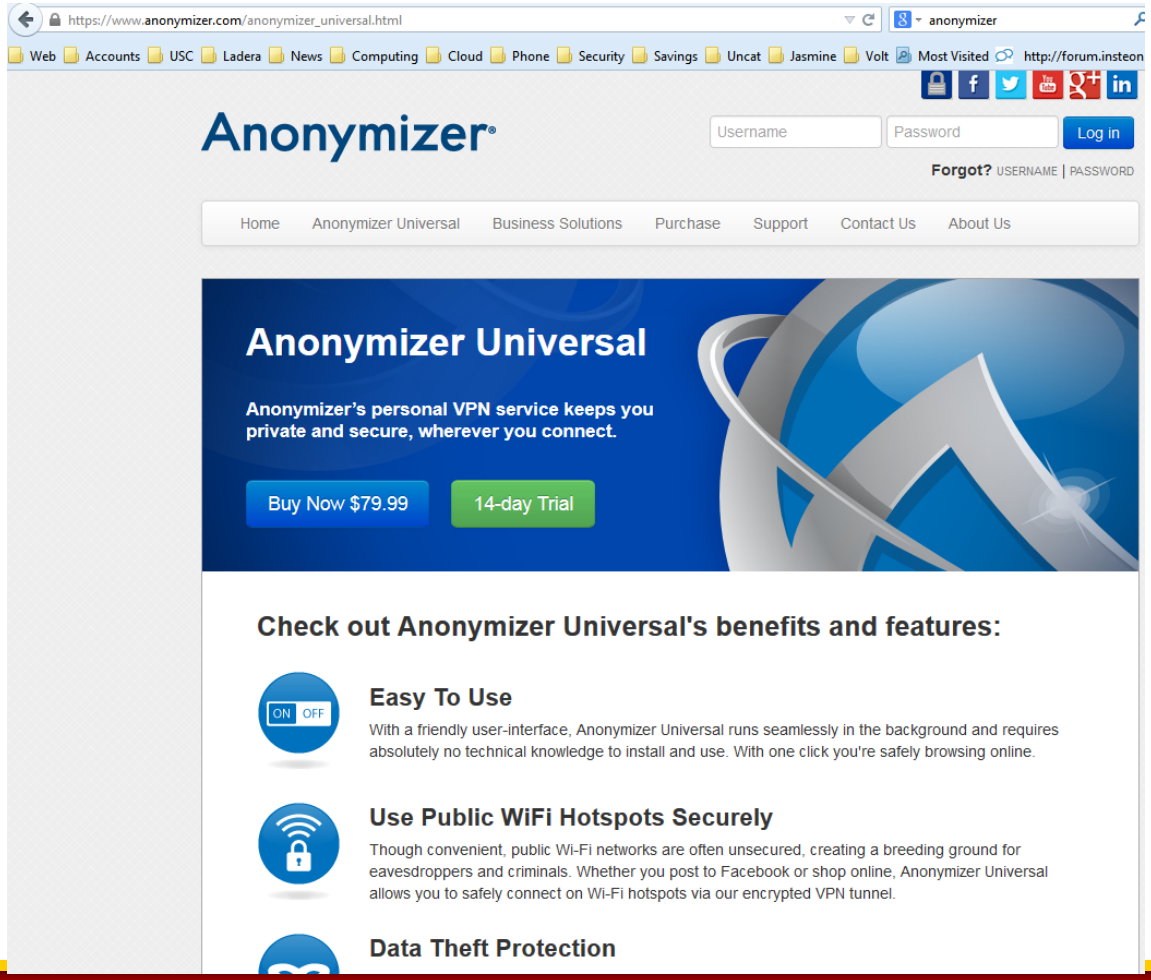
Anonymization

- For internet communication (email, web traffic) even if contents are protected, traffic analysis is still possible, providing information about what sites one visits, or information to the site about your identity.

- Tools are available that will hide your addresses
  - Proxies
  - Networks of Proxies – Onion Routing and TOR

Anonymizer and similar services

- Some are VPN based and hide IP addressed.
- Some of proxy based, where you configure your web browser.
- Need the proxy to hide cookies and header information provided by browser.
- You trust the provider to hide your details.
- Systems like TOR do better because you don’t depend on a single provider.



TOR

- Originally developed by US Navy to protect Internet communications
- The problem:
  - Internet packets have two parts – header and payload
  - Even if payload is encrypted, header is not
  - Header lists originator and destination nodes – all nodes along the way can read this information
- Why might this be a problem:
  - Law enforcement or criminals may not want it known they are visiting a site
  - General privacy protection.

TOR


WHISTLEBLOWER
AID
LEGAL ADVICE
FOR PATRIOTS.
AFFORDABLE AND
CONFIDENTIAL.
Learn more at:
whistleblowersaid.org
Anonymous access using Tor Browser:
wbaidlaw6quwv7h3.onion

TOR

- Continued development and improvement with US funding (Dept of State)
- SAFER project:
  - Develop improvements or similar technologies that are less vulnerable to persistent attempts to track users, e.g. dissidents, etc.

TOR

From Engadget, 7/28/2014

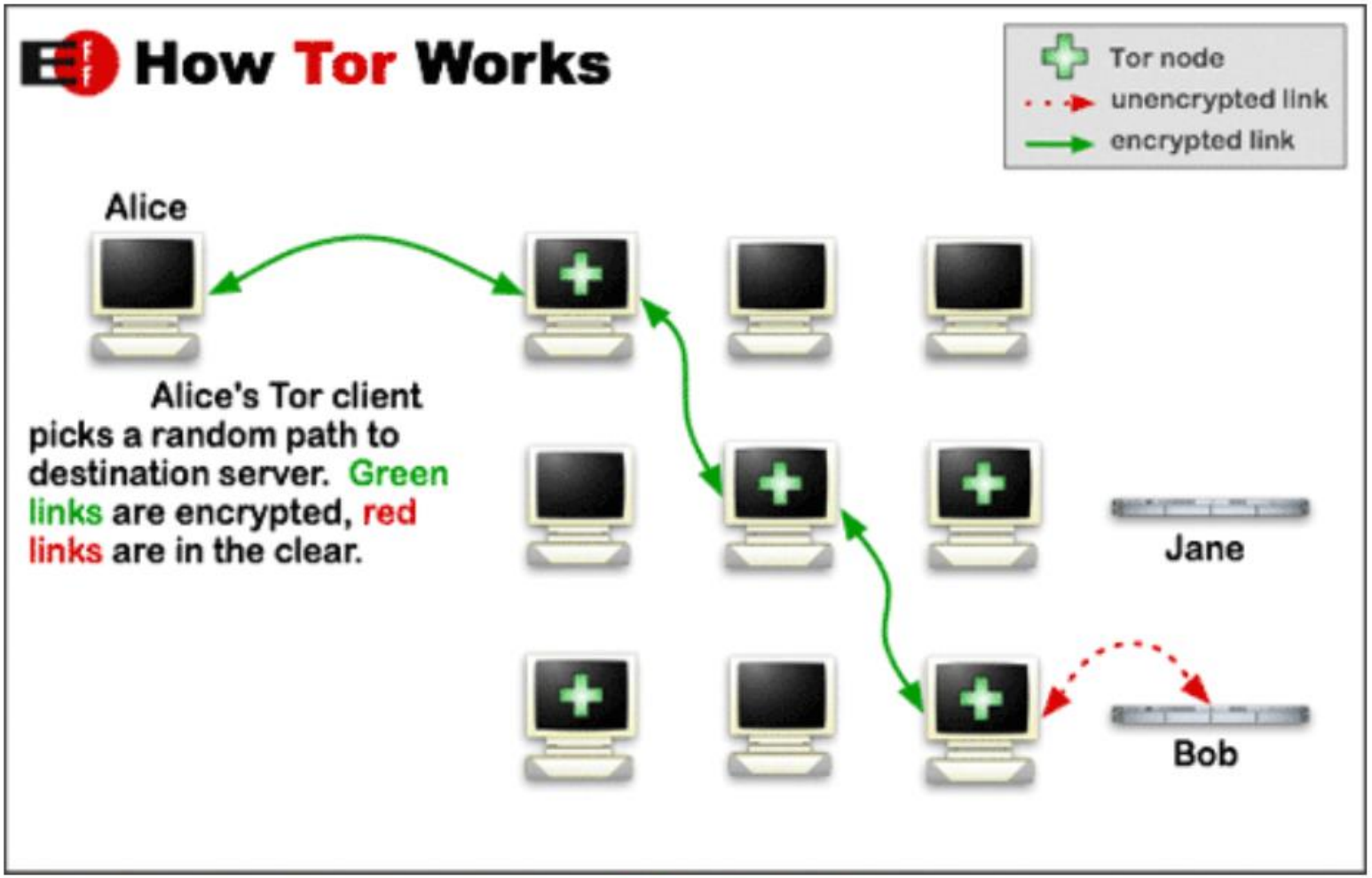
Russia offers a $110,000 bounty if you can crack Tor

Countries that have less-than-stellar records when it comes to dissenting voices must really, really hate Tor. Coincidentally, Russia's Interior Ministry has put out a bounty of around $110,000 to groups who can crack the US Navy-designed privacy network. After the country's vicious crackdown on dissenting voices back in 2012, protestors who hadn't escaped or been jailed began using anonymous internet communication as their first line of defense against the Kremlin. If you're considering taking part in the challenge (and earning yourself a tidy stack of cash to quell your conscious), be warned -- the bounty is only open to organizations that already have security clearance to work for the Russian government.

TOR - Fundamentals

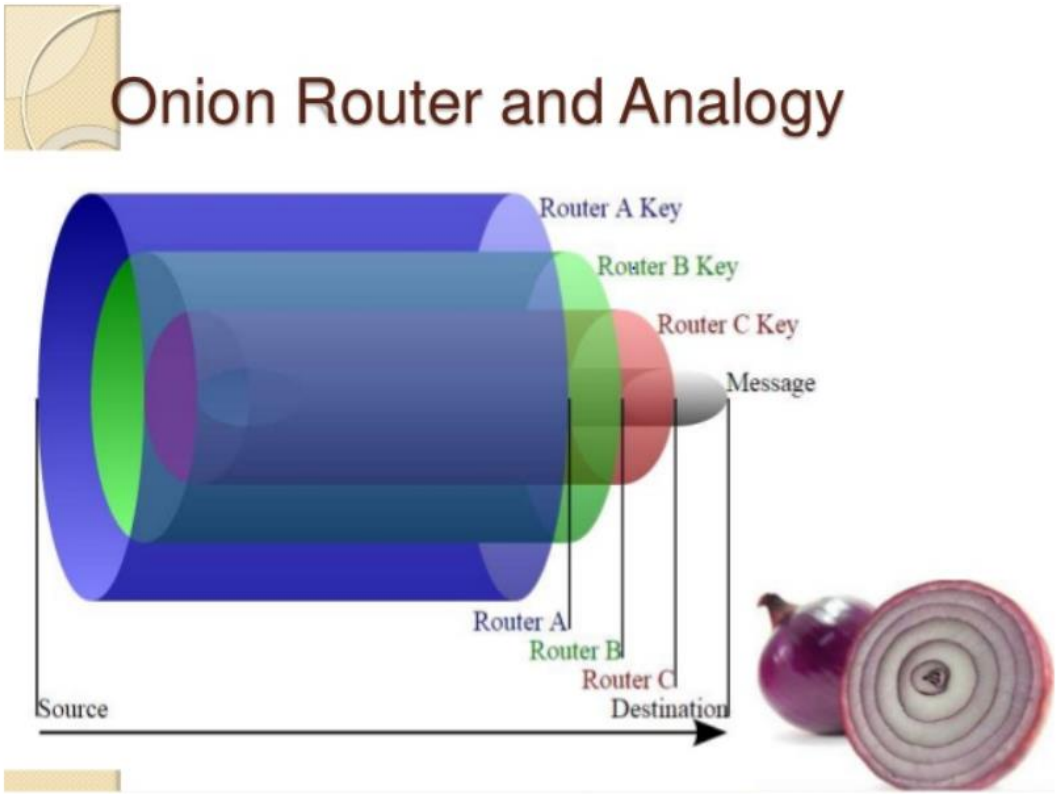
- Origin node accesses list of TOR nodes and creates the packet:
- Starts by creating a packet consisting of payload and header – header contains desired destination node and final TOR node in zigzag route
- Now treats the above packet as a payload and creates a header with origin and destination consisting of two TOR nodes
- This is repeated until final packet contains a header with original source node and first TOR node identified
- …**Hence the term "Onion Routing"**

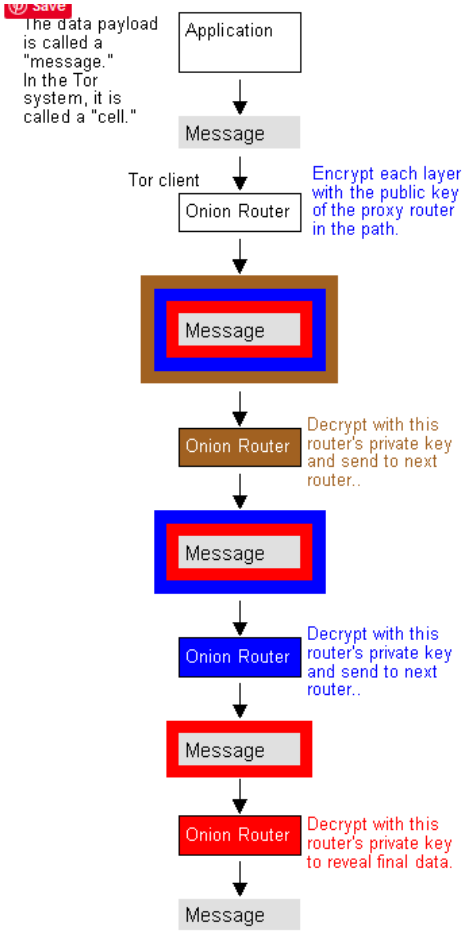
TOR - Fundamentals



A simplified version of how Tor works (Source: EFF via Wikimedia)

TOR – Fundamentals





Source cybersolutons.ga and yourdictionary.com

TOR - Fundamentals

- List of TOR nodes periodically changes
- Zigzag route is periodically changed

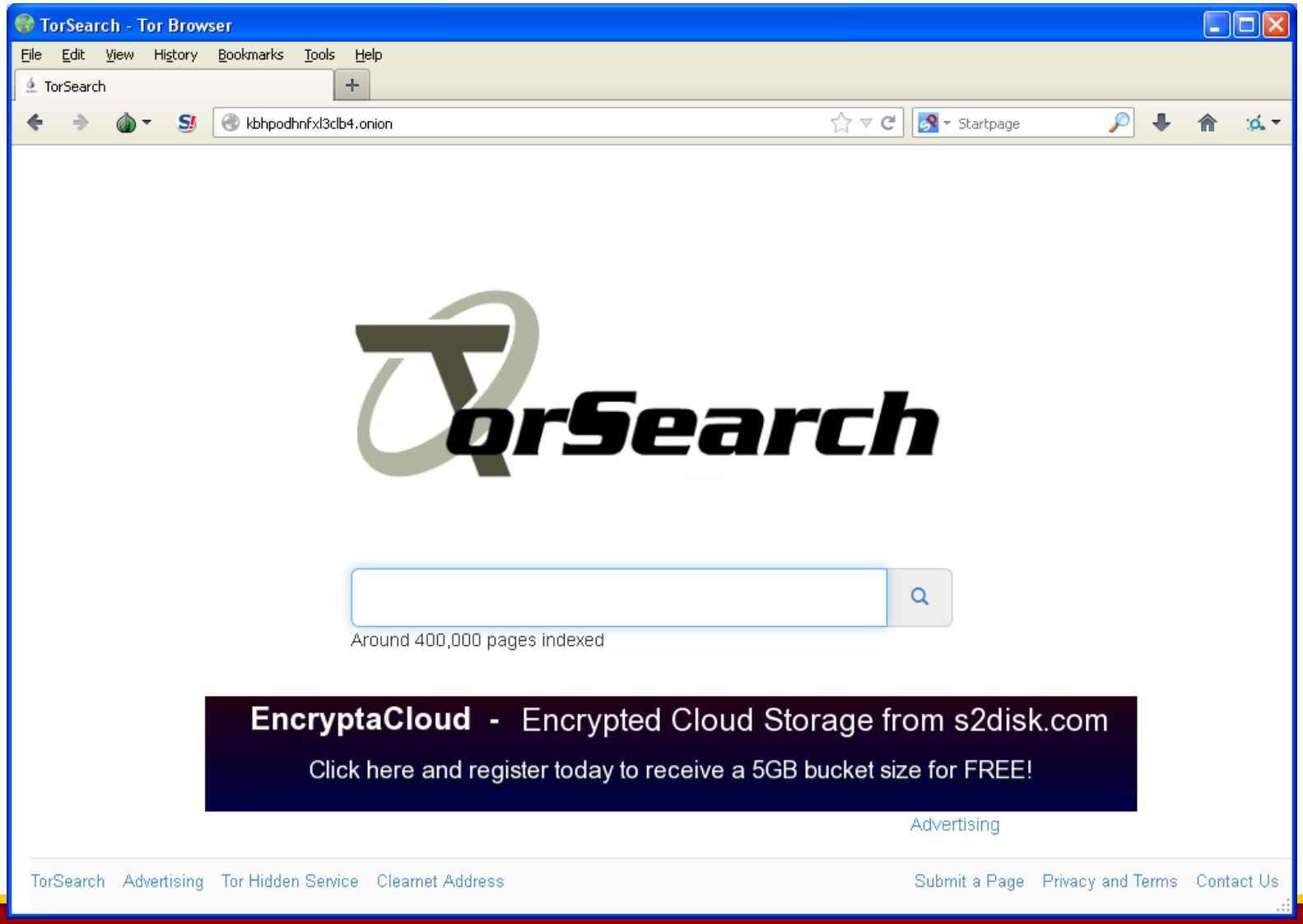
- Not totally fool proof:
  - If non-TOR browser opened within TOR browser, security measures are void – basically going back to “direct routing”
  - Someone monitoring source and destination node may note synchronization of packets being sent/received.
    - …**to avoid: increase TOR traffic**


About Tor - Tor Browser
File Edit View History Bookmarks Tools Help
About Tor
about:tor
Startpage
Tor Br
3.6.3-Wi
Congratulations!
This browser is configured to use Tor.
You are now free to browse the Internet anonymously.
Test Tor Network Settings
Search securely with Startpage.
What Next?
Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe.
Tips On Staying Anonymous »
You Can Help!
There are many ways you can help make the Tor Network faster and stronger:
Run a Tor Relay Node »
Volunteer Your Services »
Make a Donation »
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »

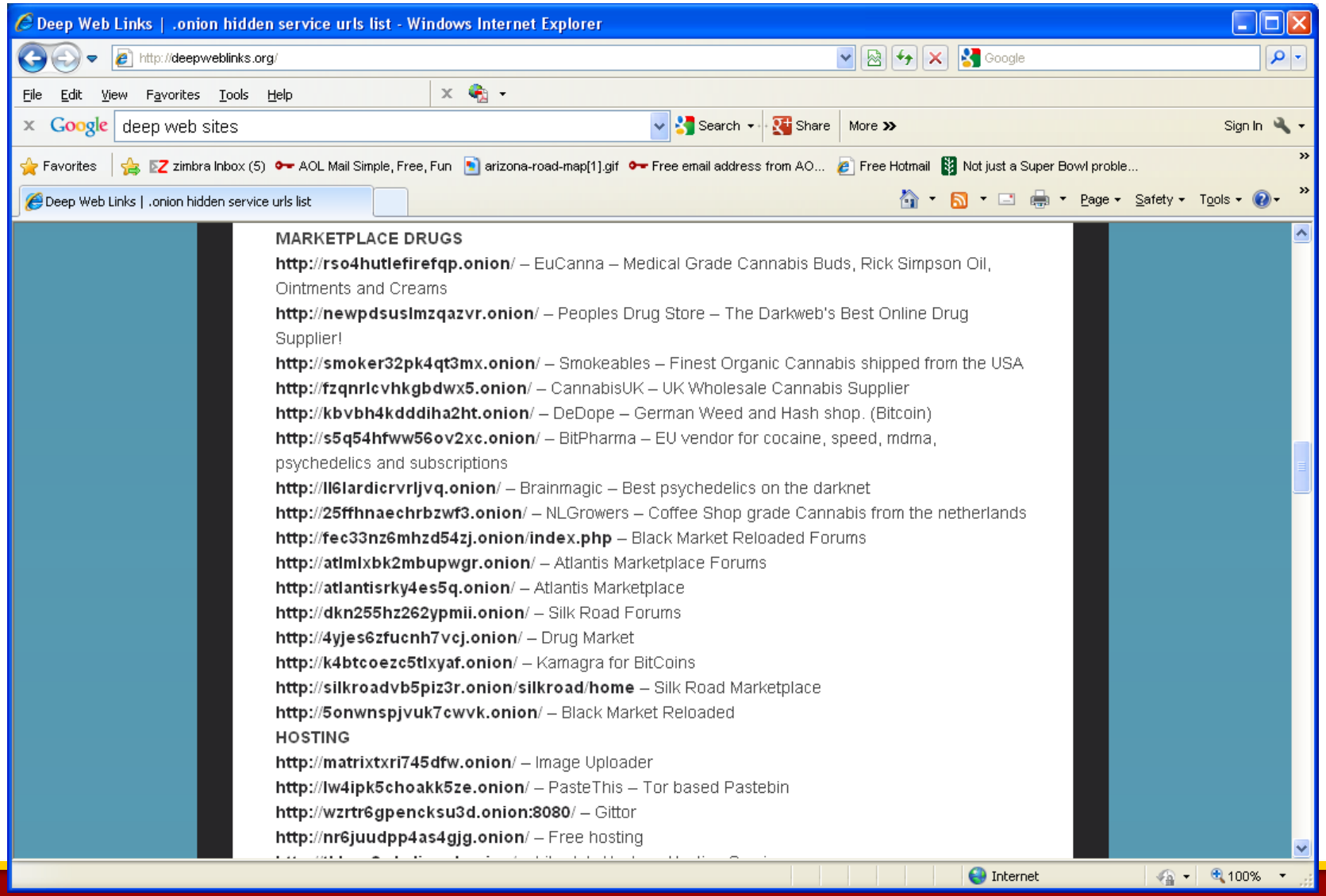
Deep Web – TOR (These are old addresses)

- TOR (https://www.torproject.org/about/overview.html.en)
- http://deepweblinks.org/ - Lists sites in deep web
- http://ybp4oezfhk24hxmb.onion/ - lists a hitman website
- http://xfnwyig7olypdq5r.onion/ - lists a USA Passport site
- http://jv7aqstbyhd5hqki.onion/ - a hackers site
- http://2ogmrlfzdthnwkez.onion/ - rent-a-hacker
- http://www.infosniper.net/

TorSearch - http://kbhpodhnfxl3clb4.onion/

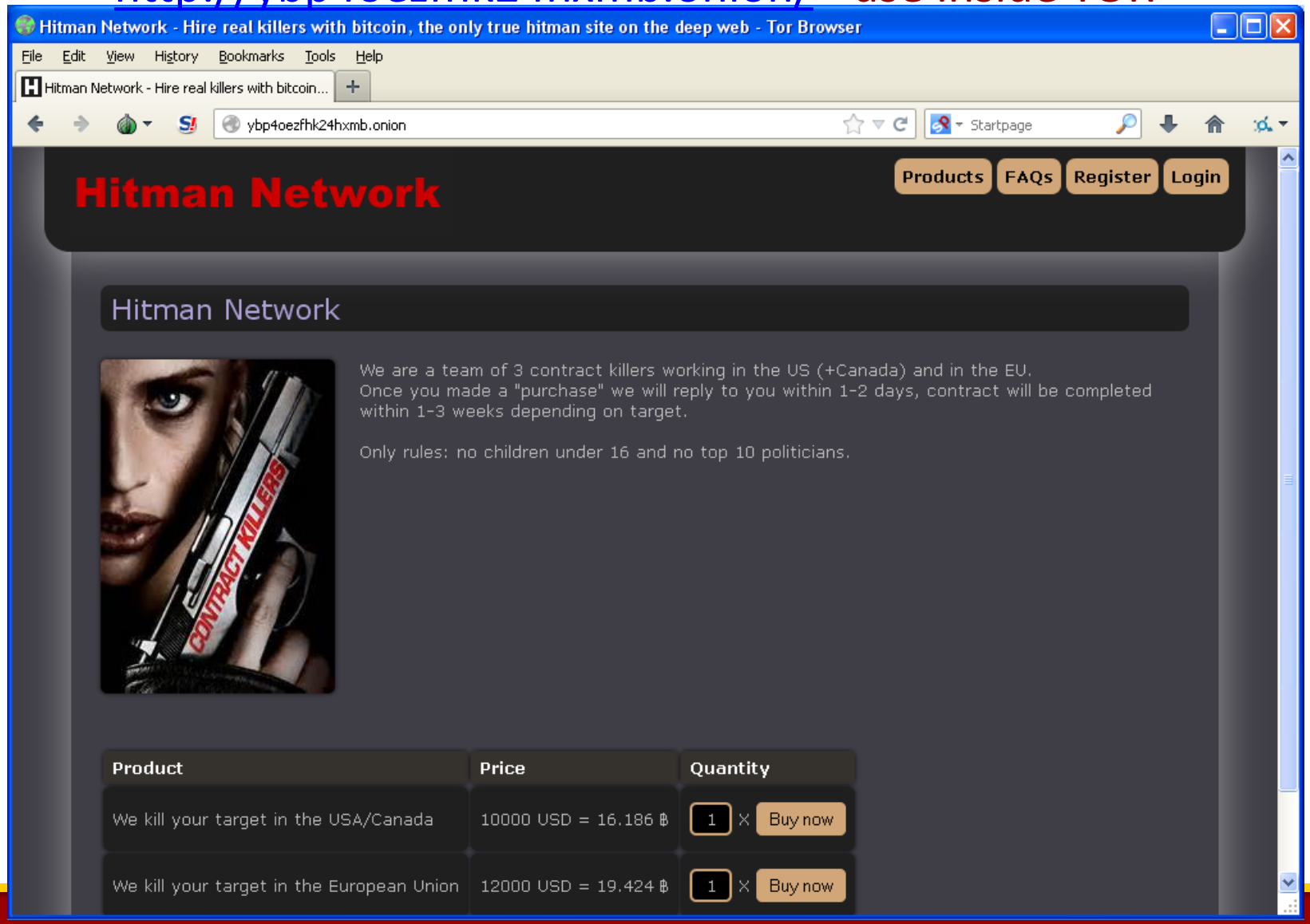


http://deepweblinks.org/



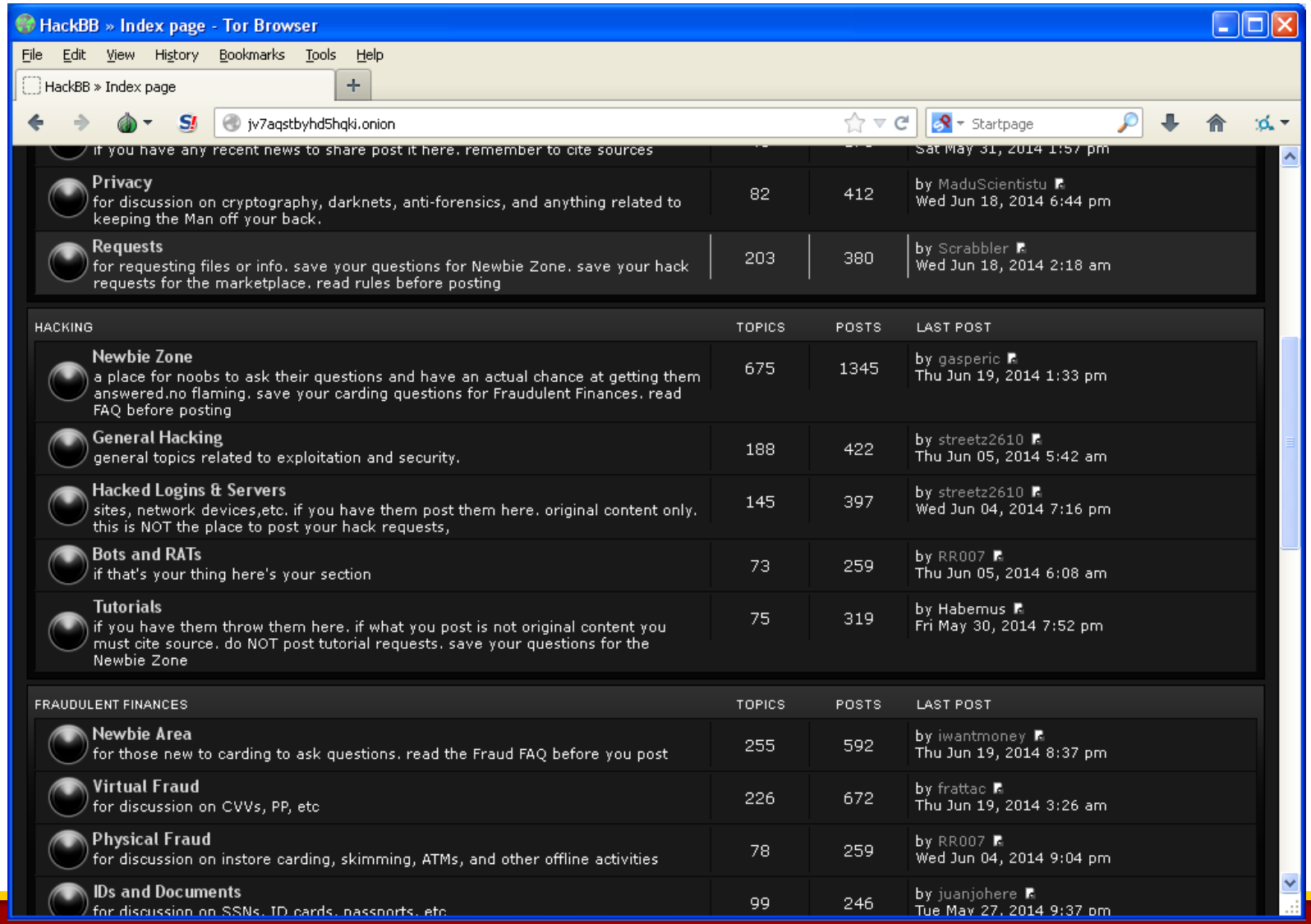
http://2ogmrlfzdthnwkez.onion/ - use inside TOR

http://ybp4oezfhk24hxmb.onion/ - use inside TOR



http://xfnwyig7olypdq5r.onion/ - use inside TOR

http://jv7aqstbyhd5hqki.onion/ - use inside TOR



Discussion

- Readings:
  - Society deserves privacy, but at what cost.
  - Who defines “good use”
  - Dark v. Deep Web
  - How to control the dark web (technically)

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec13-ce.html