CS 261 Scribe Notes: 4/19 Special Topics

Scribe: Yuqing Du

April 2021

1 Measuring the Changing Cost of Cybercrime (Anderson et al.)

Topic: Measurement, led by Rikhav.

Main takeaway from analyzing changes since 2012: externalities are much higher and crime is moving online (ie. rates of crime are not declining as statistics may indicate, but they are rather becoming less accurate as crime moves online).

Types of costs:

- Direct Costs – amount directly stolen from individuals. Examples: money withdrawn from victim accounts, time to reset account credentials post-compromise, attention and bandwidth lost to spam.
- Indirect Costs – hassle incurred, time wasted, and opportunity costs imposed on society by the cybercrime. Not directly attributed to individual victims or attackers. Examples: loss of trust in online banking leading to reduced revenues from transaction fees and/or higher costs for maintaining branch staff.
- Defence costs – measure prevention efforts. Examples: spam filters, antivirus software, raising awareness.

Indirect and defense costs add up to 10x the direct costs. In 2012, direct costs were estimated to be a few dollars per citizen per year. This paper now estimates that direct costs have increased to 10-30 dollars per citizen per year. However, it is difficult to estimate the costs accurately because:

- the data is scattered on the internet and resides in different jurisdictions
- online crime can be underreported in crime reports; look at victimisation studies instead: assesses crime by surveying a representative sample of the population, gives a closer look at the ground truth and specifically underrepresented crime. These studies found that overall the amount of online crime is much higher than other forms of crime, and there is a large variance in estimates of the direct costs of cybercrime.

1.1 Changes in cybercrime since 2012

1.1.1 New Categories of Crime

- Authorized pushed payments – victim authorizes purchase on behest of attacker. Potential cause is due to rise of two-factor-authentication, so direct hijacking has become harder than directly convicing the victim.
- Coupon fraud / loyalty program fraud / travel fraud. Attacker can impersonate customer and claim rewards, duplicate/forge coupons, steal/forge travel points. Here it is challenging to track down who ends up being harmed (company, individual, etc.). Can be done through hacking or through employees authorizing these transactions. Increase may be attributed to increase in online retail.
- Cryptocrime. Increase attributed to rise in use of cryptocurrencies.

1.1.2 Increased Categories

- Bank and credit card fraud. This is mostly attributed to increase in online retail since overall volume of legal transactions has increased; however, rate of fraud is down slightly.
- Ransomware. This is partly attributed to rise of cryptocurrencies which makes ransomware more profitable (can more easily carry out transactions without them being as easily tracked).
- Ad fraud, where fake users are simulated to engage with/click on ads. Attributed to increase in volume of ads / ads becoming more prevalent. Note that data here is poor (unclear how much ad fraud has increased).
- Tech support, where attackers fake tech support and charge people for installing / removing malware, mostly targeting more elderly individuals. Unclear why this category has increased since 2012.

1.1.3 Decreased Categories

- Sale of knockoff pharmaceuticals. Decrease attributed to the fact that common pills (eg. Viagra) have become cheaper and more easily obtained in legal ways.
- Counterfeit software / copyright theft. Decrease attributed to increase in subscription models, generally being more affordable for users.
- Telecom fraud. General decrease in fraud occuring over the phone due to people using phones less frequently.

Large money makers are fiscal fraud (abusing government fiscal policy through abusing things like unemployment/tax refunds/etc.) and cryptocrime. Support infrastructure for cybercrime has also grown and evolved with botnets becoming increasingly available due to increase in number of IoT devices; used for things like DDoS attacks, ad fraud, etc.

Discussion:

- With subscription models, smaller creators are still losing out and not getting paid enough. Has cybercrime succeeded in lowering people's expectations for how much these things cost?
- What is the distribution of criminal activity like – one-off cybercrime events (eg. large hacking) vs. recurring model for career criminals. Seems like large fraction of overall money lost comes from one off events.

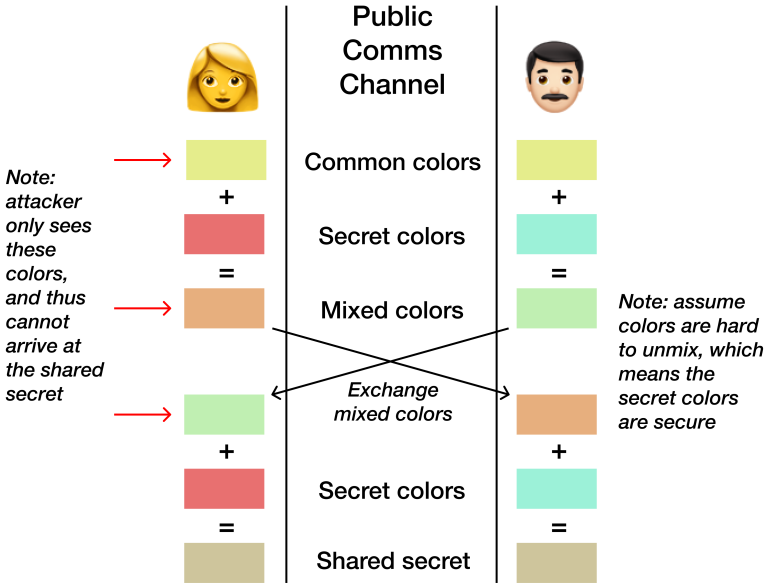
2 Imperfect Forward Secrecy – How Diffie Hellman Fails in Practice (Adrian et al.)

Topic: Surveillance, led by Zhihong.

Diffie Hellman key exchange:

- Two parties agree on a prime group (larger = more secure) and generator.
- Each party has secret integer that the use to generate a public key, which is then exchanged.
- Using their own private keys, each party can then compute the shared secret.
- this method is widely deployed, is the main key exchange mechanism for SSH and IPsec VPNs, is a popular option in TLS.

State of the art attack is to compute the discrete log of a single public value, but it is very expensive, suggesting that this practice is secure. However, this paper argues that in practice, DHE offers less security than widely believed due to precomputation.



- Number sieve algorithm for discrete log consists of precomputation state that only depends on the prime p and a descent stage that computes the individual logs. With sufficient precomputation, attacker can break any DH instances that use a specific prime p.
- the realtime computation portion is much shorter (1 minute vs. 1 week for precomputation for 512 bits)
- ie. if attacker knows which group you want to use, it is easy to reverse and calculate the secret within a minute. That being said, if there are many prime groups being used this is not too bad. However, in practice only a small number of groups are being used – eg. two groups make up 92% of uses for TLS, indicating a significant vulnerability.

2.1 Logjam Attack

Logjam Attack – proposed man-in-the-middle attack exploiting flaw in TLS.

- `DHE_EXPORT` – a reduced strength ciphersuite that resticted primes to no longer than 512 bits. While many modern browsers do not support `DHE_EXPORT`, the Logjam attack will override the ciphersuite with `DHE_EXPORT` to force TLS clients to use export-strength DH with any server that allows `DHE_EXPORT`.
- When key is exchanged btwn client and server, there is nothing to indicate which ciphersuite was chosen for client/server (flaw in TLS). From client's perspective, the communication looks good regardless of how large the prime group actually is.
- Attacker can then find 512-bit discrete log to learn the session key and read/modify communication contents by using precomputation such that finding the discrete log would take less than a minute (also include methods for working around this delay with TLS warning alerts, key caching, etc.)
- essentially tricks clients into using 512-bit DH by exploiting TLS flaws.

2.2 Why did `DHE_EXPORT` exist to begin with?

- US spy agencies were concerned about spread of cryptography making surveillance on foreign nations more difficult. Thus the US adopted the requirement that US companies were not allowed to ship strong crypto outside the US – DH keys limited to 512 bits in any software exported outside the US (`DHE_EXPORT`).

- Policy implications: the government sets these export rules with the intention of only letting US companies have strong cryptography, but the real consequence was leaving everyone with weaker cryptography overall.

To work around this, could scale to 768 or 1024 bit DH; there are also common groups of these sizes. Paper finds that scaling NFS to 768-bit DH is within reach for academic computational resources and 1024-bit DH is plausibly within reach for state-level attackers. Could indicate that NSA is breaking 1024-bit DH as how they are defeating encryption used by widely used VPN protocols, since leaked documents suggest that NSA is passively decryption IPset connections at a large scale, potentially due to leveraging precomputaitons to compute these discrete logs at scale.

Some recommendations to work around this vulnerability:

- long term solution could be to transition to elliptc curve (ECDH) which does not gain as much of an advantage from precomputation
- in meantime, can increase minimum key size to 1024, 2048, etc.
- avoid fixed prime groups and keep generating fresh groups
- more broadly, do not delibrately weaken crypto methods

Discussion:

- State level agencies have interests in surveillance and large computational resources, however they also desire that certain sets of users are protected -¿ how should they balance this?
- How can trends in increased computational resources (cloud, quantum computing) affect this?
- NSA consultation with developing DES -¿ deliberate weakening by reduced key size led to the algorithm ultimately becoming insecure / obsolete.

3 Fistful of Bitcoins: Characterizing Payments among Men with No Names (Meiklejohn et al.)

Topic: Bitcoin, led by Kelvin.

Central takeaway: using heuristics of Bitcoin transactions, it is possible to track and cluster people's activity, leading to deanonymization.

BTC has risen in profile as an alternative transaction system (eg. more prominence in finance world, being used as investments, garnering interest from regulators, etc.). The original goals of BTC were:

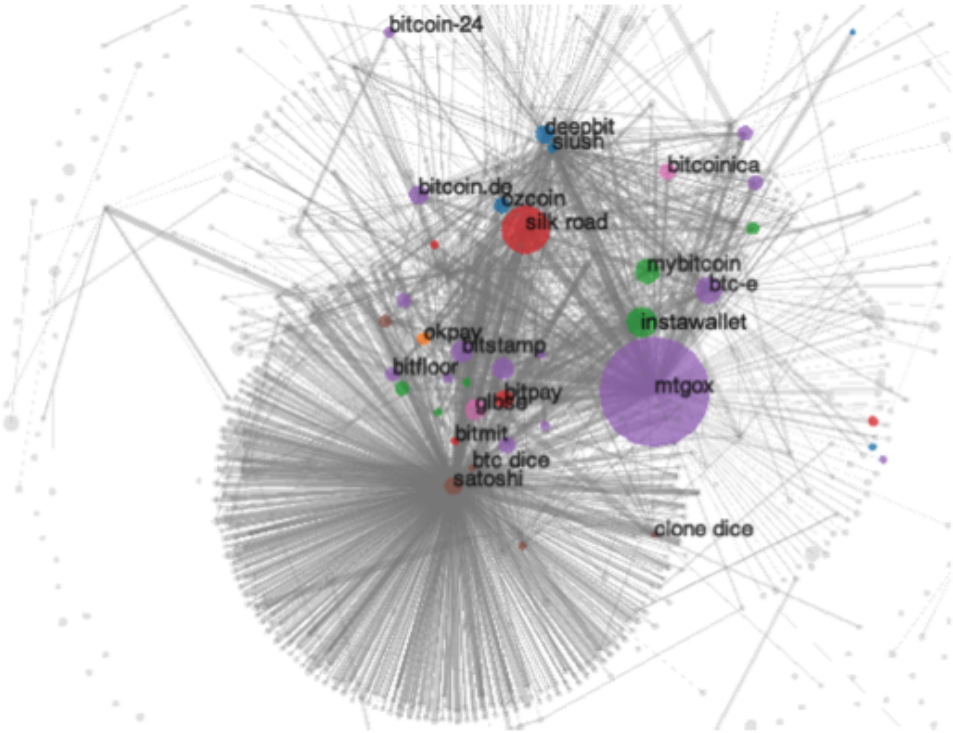
- to be a purely online virtual currency, unbacked by physical commodities and reliant on a peer-to-peer protocol for witnessing settlements
- however this means that a central issue is privacy, since by construction the ledger is fully available

The focus of the paper is *reidentification attacks*, where one can try to identify major players in bitcoin market just by transacting with them (eg. purchasing physical goods/services), clustering major operators in the network. The goal is to use heuristics derived from the nuances of BTC transactions to cluster people.

Refresher on BTC protocol: user trying to carry out transaction (eg. deposit bitcoin to a bank) -¿ incorporate own public key and bank key, broadcast transaction to peers -¿ miners attempt to validate and incorporate this transaction -¿ when successful, the transaction is added to the ledger.

Analysis from the paper:

- BTC is actively being used in transactions, not just mined and hoarded. Over time, more and more usage of BTC, spent within a certain amount of time.
- Using minimal ground truth we can try to follow the trail of transactions using two nuances:



  - Wallets comprise of a bunch of addresses, each of which have received BTC from various transactions. As a result, if two or more address are input to the same transaction, they are probably controlled by the same user.
  - Outputs of transactions have to be completely spent, where the excess is returned by a transaction with a 'change address'. Thus they categorize a public key as a change address if it's the first appearance of the key, the transaction is not a coin generation, and there is no self-change address, and for all outputs of the transaction, only the change address key is the first appearance of an output key.

- To study this approach, paper engaged in 344 transactions across an array of services (mining pools, wallet services, bank exchanges, vendors, gambling sites, etc.)
- Try to identify public keys belonging to different services and tag / cluster them, showing the resulting network

Paper found that satoshi dice was a gambling site responsible for most of the BTC transaction traffic. The authors analyzed the overall daily activity; percentage of transactions less than a certain value; how quickly satoshi spends the money it receives. The authors also analyzed the balances of large vendors and the major categories of vendors, could track specific transactions and thefts.

Discussion:

- How do we handle the cases wher ethe heuristics are flawed (leading to potential fasle positives)?
- Pros/cons of anonymity – do we want these technologies to have the ability to enable illegal activity?