CSE 127: Introduction to Security

Lecture 19: Ethics, vulnerability disclosure, personal hygiene, and cryptocurrencies

Nadia Heninger

UCSD

Winter 2023

Some material from Eric Wustrow
Lecture Outline

• Ethical principles
• Security vulnerability disclosure
• Personal security hygiene
• Cryptocurrencies
Overarching principles/lessons

• Ethics: Try to be a good person. Be thoughtful about your actions and their effects on yourself and others.

• Legal issues: Don’t violate laws.

• If lawyers or law enforcement are involved, you have already lost. It doesn’t matter if you could in theory win the case in the end.
Legal/ethical principle: Property rights

Respect other people’s property.

**Example:** Hacking your own password.
- On your own machine: Probably ok. (DMCA “good faith security research” exemption.)
- On someone else’s machine: Get permission. (DOJ says they won’t prosecute “good faith security research” but depends on interpretation.)
Ethical Principle: Minimizing harm

Ethical research involves trying to minimize harm.

**Example:** SYN scanning

- Scanning public hosts is legal, but generates many complaints.
- Depends on intended use: Used by attackers to find vulnerable hosts, used by researchers to measure networks.
- Doing research on open networks means understanding and following best practices:
  - Publicly identifying the purpose of the research
  - Providing an opt-out mechanism
  - Not launching attacks
  - Avoiding overwhelming your or others’ networks or crashing hosts
  - Etc.
Ethical principle: Minimizing harm

Example: Botherding

- Bothering is taking over a botnet
- Is this ethical or not?
  - Interfering with a legal botnet is definitely illegal.
  - Marcus Hutchins was celebrated for activating a kill switch in WannaCry malware that halted infections.
- Is taking over a botnet for research purposes ethical? It is pursuing illegal activity to study illegal activity.
- What is harm minimization?

Your Botnet is My Botnet: Analysis of a Botnet Takeover

Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Christopher Kruegel, and Giovanni Vigna

University of California, Santa Barbara

[bstone, marco, sullivan, rgilbert, msz, kemm, chris, vigna]@cs.ucsb.edu

ABSTRACT

Botnets, networks of malware-infected machines that are controlled by an adversary, are the root cause of a large number of security problems on the Internet. A particularly sophisticated and insidious type of bot is Torpig, a malware program that is designed to

One approach to study botnets is to perform passive analysis of secondary effects that are caused by the activity of compromised machines. For example, researchers have collected spam mails that were likely sent by bots [47]. Through this, they were able to make indirect observations about the sizes and activities of different spam botnets. Similar measurements, focused on DNS queries [34, 35],
Personal and Privacy Rights

Principle: Informed consent

• Human subjects research should go through ethical review
  • At a university, this is done by IRB
  • Some companies now have review processes (Example: Facebook happiness research)

• Human subjects research includes any collection of Personally Identifiable Information
Judge Confirms Government Paid CMU Scientists to Hack Tor Users for FBI

February 25, 2016  Swati Khandelwal

**Government hires University Researchers to Hack Tor Users**

Everything is now crystal clear:

The security researchers from Carnegie Mellon University (CMU) were hired by the federal officials to discover a technique that could help the FBI *Unmask Tor users* and *Reveal their IP addresses* as part of a criminal investigation.

Yes, a federal judge in Washington has recently confirmed that the computer scientists at CMU's Software Engineering Institute (SEI) were indeed behind a hack of the TOR project in 2014, according to court documents [PDF] filed Tuesday.

In November 2015, The Hacker News reported that Tor Project Director *Roger Dingledine* accused the Federal Bureau of Investigation (FBI) of paying the CMU, at least, *$1 Million for providing information that led to the criminal suspects identification on the Dark Web.*

After this news had broken, the FBI denied the claims, saying "*The allegation that we paid [CMU] $1 Million to hack into TOR is inaccurate.*"
Legal foundations of privacy

In US, 14th amendment: “nor shall any state deprive any person of life, liberty, or property without due process of law”

Interpreted as right to privacy by 20th century US Supreme Court:
- Legality of contraception
- Roe v. Wade

In 21st century US Supreme Court? Who knows...
Law Enforcement Access Policy

Policy/ethics question: Is it preferable to have law enforcement/intelligence:

• Stockpile software vulnerabilities, write targeted malware, and hack into targets when desired

• Mandate encryption backdoors or otherwise enable mass surveillance
Unintended Consequences of Stockpiling Vulnerabilities

1. NSA develops EternalBlue exploit against Windows SMB.
3. The NSA had kept the vulnerability to itself for five years instead of informing Microsoft.
5. WannaCry, NotPetya, and other ransomware exploiting EternalBlue cause $1B+ in damages in 2017 and 2018 (NHS England, Maersk among major victims)
Unintended Consequences of Law Enforcement Access

• 2004 Greek wiretapping scandal
  • Greek politicians wiretapped through law enforcement access system present on phone network
  • System was present because of US CALEA law, not used in Greece

• 2010 China Google hack
  • Attackers entered through law enforcement access portal
Disclosure options for security flaws

• Develop fully weaponized malware and distribute on black market
• Tell no one
• Sell vulnerability to middleman and don’t report to vendor
• Report to vendor only
• Report to vendor and receive bug bounty
• Report to vendor, wait for fix, report to public (“responsible disclosure”)
• Report in full to public immediately (“full disclosure”)

The process of reporting vulnerabilities

- Some vendors have sensible reporting process
  - E.g., Firefox and Chrome teams respond and react quickly, easy to work with on fixing bugs, etc.
- Some vendors less so
  - E.g., Send email through an intermediary, receive ACK, no real conversation.
  - E.g., Send email, poke individual folks for replies, no replies. Give up.
- Some vendors are playing catch up
- Some vendors are the worst: they will try to gag/sue you
Bug bounty programs

- Many vendors have bug bounty programs: $$ for bugs
  - Mozilla and Google will even run your checkers and pay you if the checkers find real bugs
- Students have made $3-10K on some papers!

<table>
<thead>
<tr>
<th></th>
<th>High-quality report with functional exploit</th>
<th>High-quality report</th>
<th>Baseline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sandbox escape / Memory corruption in a non-sandboxed process</td>
<td>$30,000</td>
<td>$20,000</td>
<td>$5,000 - $15,000</td>
</tr>
<tr>
<td>Universal Cross Site Scripting</td>
<td>$20,000</td>
<td>$15,000</td>
<td>$2,000 - $10,000</td>
</tr>
<tr>
<td>Renderer RCE / memory corruption in a sandboxed process</td>
<td>$10,000</td>
<td>$7,500</td>
<td>$2,000 - $5,000</td>
</tr>
<tr>
<td>Security UI Spoofing</td>
<td>$7,500</td>
<td>N/A [1]</td>
<td>$500 - $3,000</td>
</tr>
<tr>
<td>User information disclosure</td>
<td>$5,000 - $20,000</td>
<td>N/A [1]</td>
<td>$500 - $2,000</td>
</tr>
<tr>
<td>Web Platform Privilege Escalation</td>
<td>$5,000</td>
<td>$3,000</td>
<td>$500 - $1,000</td>
</tr>
<tr>
<td>Exploitation Mitigation Bypass</td>
<td>$5,000</td>
<td>$3,000</td>
<td>$500 - $1,000</td>
</tr>
<tr>
<td>Chrome OS</td>
<td>See below</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chrome Fuzzer Bonus</td>
<td>$1,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chrome Patch Bonus</td>
<td>$500 - $2,000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Are companies liable for security flaws?
The FTC says yes.
- 2011 Facebook settlement for deceptive privacy policies
- 2013 HTC settlement for security flaws in phones
- 2016 LabMD liable for failure to institute reasonable security practices to protect consumer data

The stock market says not really:
Policy questions around security research

- Should exploit sales be legal?
  - Code as speech principle says yes

- Is publishing exploits ethical?

- How about mixed-use tools?
  - Privacy tools like Tor or encrypted messengers used by criminals, normal people, activists
  - Cryptocurrency enables ransomware, sanction evasion
  - Random darknet shopper art piece?
Personal security hygiene.
Back up your computers

• If you can, keep a local (auto-backup to external drive) and a remote (rsync, Dropbox, Github) backup.

What threats does this help mitigate?
Password security

- Use a different password for every single web site.
- Use a password manager to store your passwords for you.
- Turn on two-factor authentication whenever it is available.
- Use public-key authentication for SSH servers.
- Be careful about phishing attempts.

What threats does this help mitigate?
Encrypt your laptop and phone hard drive

- OS X: Filevault; Windows: BitLocker; Linux: Whatever your distribution uses.
- Also set a lock screen with a password.

What threats does this help mitigate?
Maintaining computer hygiene

- Keep your OS and software up to date.
- Don’t install random software or apps
- Use Google Drive or similar to preview files
- Use a VM to open sketchy files or run software you don’t trust.

What threats does this help mitigate?
Travel and transit

- Consider using a VPN or Tor when on untrusted WiFi
- You can also use a SSH tunnel in a pinch
- Consider having a minimal travel laptop.

What threats does this help mitigate?
Encryption applications

- Encrypted chat: Signal; WhatsApp also uses Signal protocol
- Make sure your web sites support HTTPS
- PGP (ugh) is probably still the best option for sending encrypted email or files

What threats does this help mitigate?
By request: Cryptocurrencies.
Historical background: Cypherpunks

“We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.” – Eric Hughes, A Cypherpunk’s Manifesto, 1993

• 1985: David Chaum “Security without identification: Transaction systems to make Big Brother obsolete”

• In the 1990s, the Cypherpunks mailing list was extremely active; many influential members

• Software: PGP, Tor, anonymous remailers, Off-the-record messaging...

• Cypherpunk ideas: Anonymous digital currency, WikiLeaks, assassination markets, pseudonymity...

• These ideas encode libertarian-to-anarchist politics
How do you build digital currency?

A central authority can keep a balance ledger and update with each transaction.

<table>
<thead>
<tr>
<th>Account</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave</td>
<td>$342.87</td>
</tr>
<tr>
<td>Fred</td>
<td>$32,944.09</td>
</tr>
<tr>
<td>Eve</td>
<td>$89,218.87</td>
</tr>
<tr>
<td>Charlie</td>
<td>$429,718.90</td>
</tr>
<tr>
<td>Alice</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Bob</td>
<td>$0.00</td>
</tr>
</tbody>
</table>

Alice pays Bob $200

<table>
<thead>
<tr>
<th>Account</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dave</td>
<td>$342.87</td>
</tr>
<tr>
<td>Fred</td>
<td>$32,944.09</td>
</tr>
<tr>
<td>Eve</td>
<td>$89,218.87</td>
</tr>
<tr>
<td>Charlie</td>
<td>$429,718.90</td>
</tr>
<tr>
<td>Alice</td>
<td>$800.00</td>
</tr>
<tr>
<td>Bob</td>
<td>$200.00</td>
</tr>
</tbody>
</table>
How do you build a decentralized digital currency?

Without a central authority, different entities need to agree on transactions and balances.

How do you keep someone from sending someone else’s money to themselves?

<table>
<thead>
<tr>
<th>Alice Credit Union</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$999,999,999.99</td>
</tr>
<tr>
<td>Bob</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Charlie</td>
<td>$22.15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bank of Bob</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$300.00</td>
</tr>
<tr>
<td>Bob</td>
<td>$1,234,567.89</td>
</tr>
<tr>
<td>Charlie</td>
<td>$22.15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HSBCharlie</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>$0.00</td>
</tr>
<tr>
<td>Bob</td>
<td>$1,000.00</td>
</tr>
<tr>
<td>Charlie</td>
<td>$999,999,999.99</td>
</tr>
</tbody>
</table>
Transactions: Use digital signatures to authenticate

A digital signature gives guarantees:

- The transaction has not been altered
- Only the entity with the private key can generate a valid signature
- Anyone can validate a signature with the public key
Pseudonymous identity: Derive from public key

Bitcoins are associated with an address.

The address is a hash of a public key.

Bitcoin Address

Addresses are identifiers which you use to send bitcoins to another person.

<table>
<thead>
<tr>
<th>Summary</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>1FteWv9xcSE2fzpcx2m4xsL9eKyeVydYVK</td>
</tr>
<tr>
<td>Hash 160</td>
<td>a3564709cfbc84e9dd0079a7a3a35865d97148049</td>
</tr>
<tr>
<td>Tools</td>
<td>Related Tags - Unspent Outputs</td>
</tr>
</tbody>
</table>

Transactions (Oldest First)

- **662524b59813a1bta895b1377094166043244992dc8d4479b1526c980946758**
  - No. Transactions: 2
  - Total Received: 0.07239997 BTC
  - Final Balance: 0 BTC

  **(Fee: 0.00010176 BTC - 13.46 sat/WU - 53.84 sat/B - Size: 189 bytes) 2018-06-20 20:18:40**

  1FteWv9xcSE2fzpcx2m4xsL9eKyeVydYVK (0.07239997 BTC - Output) → 3MS82DmjHPgCYvQnvw5rNx6j61YvN6qSr - (Unspent) 0.07229821 BTC

  - 3 Confirmations
  - -0.07239997 BTC

- **e33be6bf1b8e5394e2f1ceaa87d3b31c3aebd36fb0b2ac16233cd7d280d363**

- **175xKXTfLiXgX7qxA5CaskBzW4Qs3nWAM (0.24446334 BTC - Output) → 1FteWv9xcSE2fzpcx2m4xsL9eKyeVydYVK - (Spent) 0.07239997 BTC
  - 4 Confirmations
  - 0.17135825 BTC

- **175xKXTfLiXgX7qxA5CaskBzW4Qs3nWAM - (Unspent) 0.07239997 BTC**
Problem: Double-spending

1. Alice has 1 token.
2. Alice sends 1 token to Bob and 1 token to Charlie.
3. Synchronization issue: each of Bob and Charlie is able to validate that Alice had a token to send, but doesn’t know about the others’ tokens.

A decentralized system needs some way to achieve consensus before transactions are accepted to prevent double-spending.
We would like to record all transactions in a public ledger.

Use some kind of consensus protocol to ensure everyone has same view of ledger.

Bitcoin uses a hash chain: every block of transactions includes cryptographic hash of previous block.

This means that once people agree on a block, they must agree on previous blocks.
Chaining blocks together with hash functions

Network participants receive blocks from other nodes.

Which blockchain do you trust? The longest one.

How do you keep someone from making up a new super long blockchain?

Bitcoin uses “Hashcash” proof-of-work scheme to rate limit block creation.
Bitcoin consensus: Proof of work

- A block includes a set of transactions. “Miners” search for a nonce value that results in $k$ leading 0s in the SHA256 hash of the block.
- We expect this to take $2^k$ hash function evaluations.
- The first miner to find such a value sends it to the network and work continues on the next block.
- The longest chain represents the most work: an attacker can’t outcompete an honest majority.
Bitcoin Summary

Three main ideas:

• Public cryptographic keys for pseudonymous identifiers and transaction validation.

• Hash chain to ensure integrity of intermediate blocks.

• Proof-of-work-based distributed consensus scheme.
Bitcoin: Putting it all together

1. To generate an address, generate an ECDSA public key and hash it. This is your public address.

2. To receive money, another participant generates a transaction (actually a small executable script) sending bitcoin to this address and distributes it on the network.

3. Miners aggregate transactions from the network into a block and race to finish the proof of work first on that block.

4. The winning miner sends the block with proof of work on the network.

5. Once most nodes agree that the block with your transaction is part of the longest chain, you now have bitcoin.
“Smart contracts”: Ethereum

Idea: Include an expressive scripting language and have all nodes execute these scripts.

Pro: Replace governments, lawyers, accountants, and regulators with executable code.
“Smart contracts”: Ethereum

Idea: Include an expressive scripting language and have all nodes execute these scripts.

Pro: Replace governments, lawyers, accountants, and regulators with executable code.

Con: You have seen how good we are at writing secure code.

• An attacker stole $50 million of Ether from the DAO (decentralized autonomous organization) by exploiting a vulnerability in the DAO’s smart contract code.

• The Ethereum community decided to fork the blockchain to roll back the transaction.
"NFTs": Non-Fungible Tokens

Idea: Post metadata about things to a public blockchain.

Pro: Supply-chain management? Digital rights management?

Con: Actual asset stored elsewhere.

- Idea of “cryptographic tokens” seems to have become commingled with the idea of automatic mass-produced digital art.

- Protocol flaw in most implementations: Only thing on blockchain is a URL and contents aren’t even validated.
Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.

- Can replace proof of work with "proof of stake": consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.

- Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.

- Various proposals (Lightning Network). Bitcoin will never be a payment network.
Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.

- Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.

- Various proposals (Lightning Network). Bitcoin will never be a payment network.
Bitcoin and cryptocurrency criticisms

• Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  • Can replace proof of work with “proof of stake”: consensus based on coin ownership.

• Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.
Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.
Bitcoin and cryptocurrency criticisms

- Proof of work mining is environmentally wasteful. Bitcoin is now consuming more electricity than Argentina.
  - Can replace proof of work with “proof of stake”: consensus based on coin ownership.

- Bitcoin is not anonymous. Transactions are all public, and addresses are only pseudonymous and can be linked to real-world identities when used.
  - Zcash uses fancy crypto (zk-SNARKs) to validate transactions without publishing transactions publicly to network.

- Bitcoin does not scale: The transaction rate will never be high enough to be a real payment network.
  - Various proposals (Lightning Network). Bitcoin will never be a payment network.
Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.
Bitcoin and cryptocurrency criticisms

• The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

• A public blockchain is not what most people want for real-world applications.

• Cryptocurrencies are “speedrunning 500 years of bad economics”–Nick Weaver
Bitcoin and cryptocurrency criticisms

• The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

• A public blockchain is not what most people want for real-world applications.
  • A blockchain is just an append-only linked list.
  • Many proposed applications (healthcare? supply chain management?) better suited to a trusted third party with a database, an API, and maybe some digital signatures.
  • There are better distributed consensus algorithms for closed groups. Keyword: “Permissioned blockchain” which seems like it might soon come to refer to any multiparty computation.

• Irreversible transactions are not what consumers actually want in a payment system.

• Cryptocurrencies are “speedrunning 500 years of bad economics”–Nick Weaver
Bitcoin and cryptocurrency criticisms

- The cryptocurrency space is full of charlatans, ponzi schemes, and tulip mania.

- A public blockchain is not what most people want for real-world applications.
  - A blockchain is just an append-only linked list.
  - Many proposed applications (healthcare? supply chain management?) better suited to a trusted third party with a database, an API, and maybe some digital signatures.
  - There are better distributed consensus algorithms for closed groups. Keyword: “Permissioned blockchain” which seems like it might soon come to refer to any multiparty computation.

- Irreversible transactions are not what consumers actually want in a payment system.
  - Cryptocurrencies are “speedrunning 500 years of bad economics”–Nick Weaver
Cryptocurrencies: The positives

• Renewed excitement in CS research like Byzantine fault tolerance, consensus protocols, programming language design for smart contracts, exotic cryptographic primitives...

• In a gold rush, the people who get rich are not the miners following the crowds, but the people selling equipment to the miners.
Have a great end of quarter!
Good luck on the final!