Undecidable Problems: Ethical and Policy Questions in Cybersecurity

Michael Kahn, BrainGu

Security is about humans

- Human motives
  - Greed
  - Ideology
  - Lulz
- Human vulnerabilities
  - Phishing
  - Social Engineering
  - Exploiting insecure coding practices

Prove It

- Encryption algorithm correctness
- Encryption implementation correctness
- Application correctness under normal inputs
- System correctness with human interaction
- Correctness of human behavior

Encryption algorithms have specific criteria for testing correctness. Applications and systems can (even if they are normally poorly defined). How do we define “correctness” for human behavior?

Topics

- Strong encryption vs. lawful searches
- Responsibility for offensive capabilities
- Coordinated disclosure
- Security research and the law

Ethics
“the discipline dealing with what is good and bad and with moral duty and obligation”
Policy
“a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions”

Law and regulations can be a binding implementation of policy.

Strong Encryption

Strong Encryption

- Cryptographic algorithms/protocols that are impractical to break using brute force
- Strong transport encryption: TLS 1.2
- Strong at-rest encryption: BitLocker, iOS 8+
- AES-256 common, but there are many others

Crypto Wars

Encrypt All the Things

- Strong end-to-end encryption allows secure e-commerce/banking
- Protects against criminals and authoritarian governments
- Encourages free speech and free press, reduces chilling effects

“if the United States takes the CALEA-like position that companies should build in decryption capacity to be utilized in accord with our laws, it follows that we think it’s legitimate for other countries—including Russia and China—to require the same technical capability to be utilized in accord with their laws.”

Encryption isn’t just for Americans — also used by dissidents and activists in China, Iran, etc.

Chilling effects: “any legal action that would cause people to hesitate to exercise a legitimate right (freedom of speech or otherwise) for fear of legal repercussions”
Even for completely legal and acceptable discussions, people speak more freely in person than online, and more freely in encrypted channels than unencrypted.

StrongBad: G  ing Dark

- Strong encryption limits law enforcement access even with a search warrant
- Even with physical device access, may block access to data
- Roadblocks for terrorism, child abuse, violent crime investigations

Between September 17, 2014 and October 1, 2015, the Manhattan District Attorney’s Office was unable to execute approximately 111 search warrants for smartphones because those devices were running iOS 8

All of this has happened before…

- Clipper Chip: 1993-1996
  - Encryption for voice calls, with hardcoded keys provided to USGOV in escrow
  - Classified, non-public algorithm
- Export restrictions
- CALEA

What's an alternative?

- "Lawful hacking"
  - Plenty of unintentional vulnerabilities around encryption protocols
  - Create or procure exploits to use under legal authority
- Rule 41
  - Allowed any US judge to authorize computer searches anywhere

http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip



Great! Lawful Hacking!

…for sanctioned, authoritarian regimes?



Hacking Team:
Sudanese Rights Abuses for Fun and Profit

- Italian-based company selling offensive security software for monitoring
- Hacked in 2015, 400GB of internal documents posted online
- Leaked client list included Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Morocco, Nigeria, Oman, Saudi Arabia, Sudan

http://foreignpolicy.com/2016/04/26/fear-this-man-cyber-warfare-hacking-team-david-vincenzetti/

Looking back, Vincenzetti claims that had he been more informed about Sudan, he “would have never sold to them.” But he will not say he regrets the deal. “We didn’t break any law,” he goes on, nonplussed about the experience. “It just happened.”

Division of Responsibility

Vulnerability Researcher

Finds flaw in Java

Exploit Developer

Writes malicious applet targeting Farsi language pack to report back user's location

Sales Representative

Sells packaged exploit to Iranian government or shell corporation

Government of Iran

Deploys exploit to dissident forum, gathers locations of dissidents, dissidents arrested by secret police

We can generally agree that the responsibility is attenuated the farther up the chain we go.

Assume that everybody involved except Iran thinks that arresting and torturing dissidents is undesirable.
What level of culpability do the researcher and developer have?
What responsibility do the developer and sales rep have to ask what the exploit will be used for?
What if the exploit targets Arabic or English instead of Farsi? Does that change the developer's culpability?
What if the customer is Saudi Arabia (Western ally with history of human rights abuses) instead of Iran?

Division of Responsibility

Vulnerability Researcher

Finds flaw in Java

Exploit Developer

Writes malicious applet targeting **English** language pack to report back user's location

Sales Representative

Sells packaged exploit to Iranian government or shell corporation

Government of Iran

Deploys exploit to dissident forum, gathers locations of dissidents, dissidents arrested by secret police

We can generally agree that the responsibility is attenuated the farther up the chain we go.

Assume that everybody involved except Iran thinks that arresting and torturing dissidents is undesirable.
What level of culpability do the researcher and developer have?
What responsibility do the developer and sales rep have to ask what the exploit will be used for?
What if the exploit targets Arabic or English instead of Farsi? Does that change the developer's culpability?
What if the customer is Saudi Arabia (Western ally with history of human rights abuses) instead of Iran?

Division of Responsibility

Vulnerability Researcher

Finds flaw in Java

Exploit Developer

Writes malicious applet targeting **Arabic** language pack to report back user's location

Sales Representative

Sells packaged exploit to **Saudi** government

Government of Saudi Arabia

Deploys exploit to dissident forum, gathers locations of dissidents, dissidents arrested by secret police

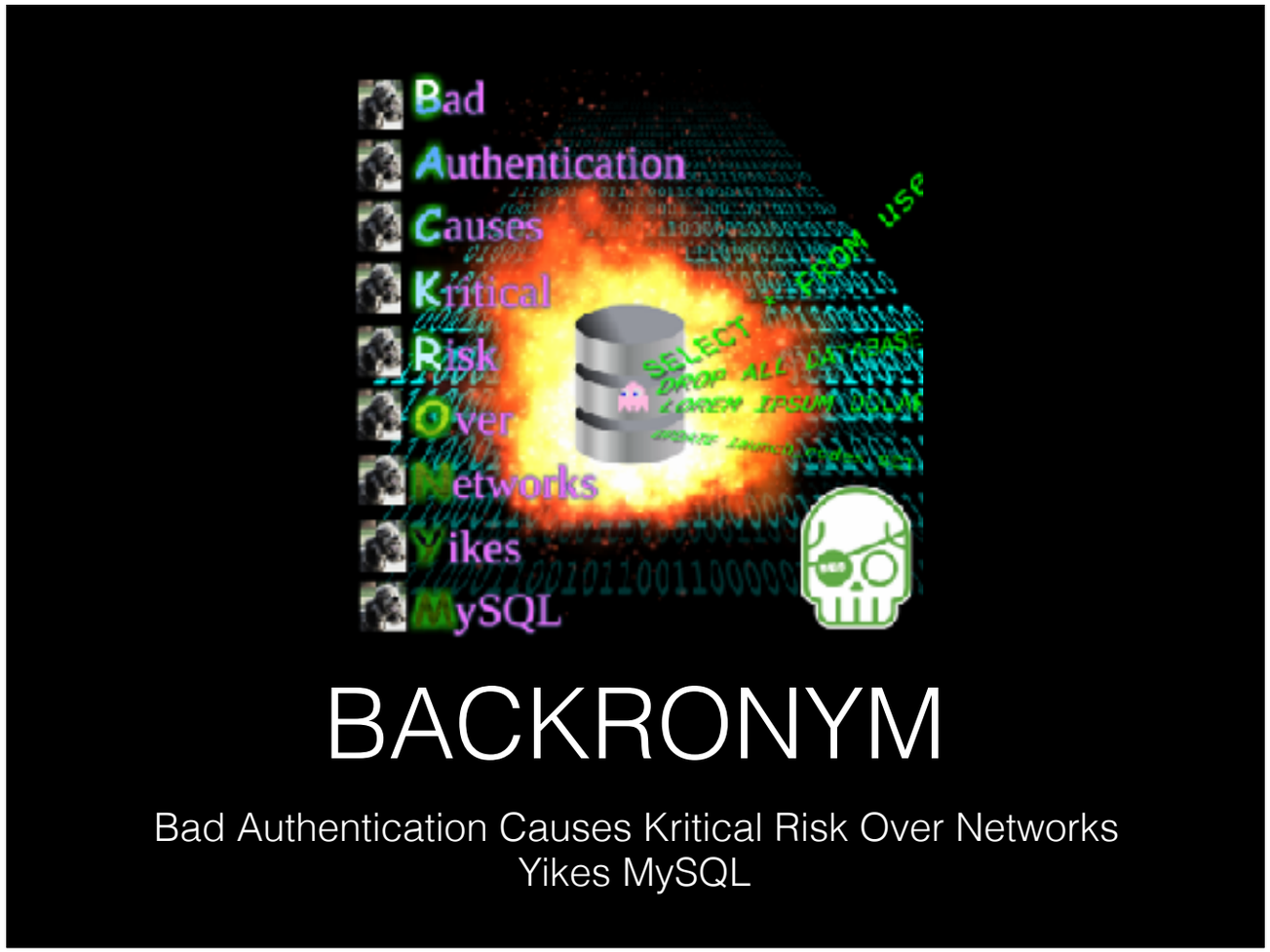
We can generally agree that the responsibility is attenuated the farther up the chain we go.

Assume that everybody involved except Iran thinks that arresting and torturing dissidents is undesirable.
What level of culpability do the researcher and developer have?
What responsibility do the developer and sales rep have to ask what the exploit will be used for?
What if the exploit targets Arabic or English instead of Farsi? Does that change the developer's culpability?
What if the customer is Saudi Arabia (Western ally with history of human rights abuses) instead of Iran?


Vulnerability
Disclosure
DIRTY COW
STAGEFRIGHT

Proper Vulnerability Disclosure

1. Choose a catchy name
2. Register the domain with name from Step 1 (if taken, return to Step 1)
3. Turn the name into an acronym
4. Design an exciting logo
5. Tweet and contact tech news sites, as many as possible



BACKRONYM

Bad Authentication Causes Kritical Risk Over Networks
Yikes MySQL

backronym.fail

Vulnerability Disclosure

- Nondisclosure
  - Keep vulnerability for use or private sale
- Vendor disclosure
  - Notify vendor without threat of public release
- Public disclosure
  - Release details of vulnerability to public

Other than nondisclosure, disclosure methods seek to balance two main goals: Providing the vendor with a chance to patch the vuln before it goes public, and using public release as encouragement for the vendor to create a patch in a timely manner. Public disclosure also allows for end-users to start monitoring and mitigation before a patch.

Public Disclosure

- Responsible/Coordinated Disclosure
  - Notify vendor immediately
  - Post publicly after 15-90 days
- Full/Instant Disclosure
  - Post details publicly, sometimes with POC

CERT policy is 45 days (http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm?)

Legal Framework

- Computer Fraud and Abuse Act
- Digital Millennium Copyright Act
- Wassenaar Arrangement

CFAA

- Primary federal criminal statute for “hacking”
- Forbids accessing a computer “without authorization” or “exceeding authorized access”
  - Also outlaws trafficking in passwords
- Extremely broad in scope

Effectively criminalizes any and all offensive activity against any computer not controlled by the actor or specifically authorized for testing
Critical to have protections in any pen testing agreement to define limits of “authorized access”
Sometimes interpreted to forbid Terms of Use violations
Used to prosecute Aaron Swartz for using MIT’s network to download bulk documents from JSTOR. Maximum penalty was up to 50 years in prison and $1 million in fines.

DMCA

- Copyright law protecting DRM and restricting circumvention of copy-protection mechanisms
- Best-known for protecting DVDs, etc. from being copied and being infringed by torrents
- Can be interpreted to limit security research into copy-protection mechanisms

Wassenaar Arrangement

- International forum on arms and “dual-use” export controls
- Modern organization established 1996
- Intended to limit proliferation of military and related technologies
- Updated in 2013 to add controls for “intrusion software” and “carrier class network surveillance tools”
- New controls could severely limit security research

http://www.steptoecyberblog.com/2017/02/15/cybersecurity-and-the-wassenaar-arrangement-what-needs-to-be-done-in-2017/

Changes could prevent coordination about new vulnerabilities among researchers from different countries
Exports of many tools and services would require export licenses
Opposed by many internet companies and researchers
Implementation by US still in progress

Additional Topics

- Active defense by corporations
- Great Firewall of China
- Uber: God View, Greyball, Hell
- Algorithmic biases

http://gizmodo.com/report-uber-had-yet-another-secret-tracking-program-ca-1794292693

Links to relevant papers/articles available in slack after talk