Lecture 03: Ethics and the Law

Professor Adam Bates

CS 461 / ECE 422

Fall 2019

Goals for Today

- Learning Objective:
  - Understand why we care about ethics and the law
  - Provide examples of ethical philosophies
  - Provide examples of laws that govern our work
  - Identify the difference between law and ethics
  - Understand ethics and law in the context of modern security
- Announcements, etc:
  - No class or office hours on Monday (Labor Day Holiday)
  - MP1 will be released on Monday at 6pm.

Reminder: Please put away devices at the start of class

Researchers Discover Two Major Flaws in the World's Computers

查看简体中文版 | 查看繁體中文版 | Leer en español

By CADE METZ and NICOLE PERLROTH JAN. 3, 2018

208

Paul Kocher, left, moderating the RSA Conference 2016 in San Francisco. Mr. Kocher is an independent researcher who was an integral part of the team that discovered the flaws. Jim Wilson/The New York Times

SAN FRANCISCO — Computer security experts have discovered two major security flaws in the microprocessors inside nearly all of the world's

RECENT COMMENTS

Cathy January 4, 2018
Well if for the most part you look at what in memory 99 percent will be useless to anybody .

NML January 4, 2018
Looks like my faith in Pilot, Bic, Clairefontaine & Moleskine has been rewarded.

dunbar7376 January 4, 2018
I have found a third major flaw: not one woman in your RSA conference pic.

SEE ALL COMMENTS

TECHNOLOGY

The New York Times

Facebook Security Breach Exposes Accounts of 50 Million Users

One of the challenges for Facebook's chief executive Mark Zuckerberg is convincing users that the company handles their data responsibly.

Josh Edelson/Agence France-Presse — Getty Images

Malware

What is WannaCry ransomware and why is it attacking global computers?

Malicious software has attacked Britain's health service and companies in Spain, Russia, the Ukraine and Taiwan. What is it and how is it holding data to ransom?

Alex Hern and Samuel Gibbs

Fri 12 May 2017 12.16 EDT

WannaCry malicious software has hit Britain's National Health

Thank goodness for security experts

Security "Research" to the Rescue!

- White (or grey?) hats disseminate results to help, to benefit the internet community
- …but oh, t
  - First to p Show you're 31337? To fig the means…
- …and the c
  - Affecting other research; impacting LE investigations; thwarting mitigation efforts; protecting rights; helping the bad guys; less risky (and less attractive) options?

What are ethics?

- "The field of ethics (or moral philosophy) involves systematizing, defending, and recommending concepts of right and wrong behavior."
- Normative ethics, is concerned with developing a set of morals or guiding principles intended to influence the conduct of individuals and groups within a population (i.e., a profession, a religion, or society at large).
    - Consequentialism
    - Deontology
    - virtue ethics

Aside: This is serious

- Critically engaging with ethical considerations is an important and regular part of security…
  - *Is it ethical for me to conduct this experiment? Is it legal?*
  - *Does this paper I'm reviewing follow community norms for ethical research? Is it legal?*
  - *Under what circumstances should I disclose the results of my experiment, and how?*

Computer Ethics

"A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with **new capabilities** and these in turn give us **new choices** for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine **what we should do** in such cases, i.e., to formulate policies to guide our actions."

-Moor

Ethics != Law

- "Law can be defined as a consistent set of universal rules that are widely published, generally accepted, and usually enforced"
- Interrelated but by no means identical (e.g., legal but not ethical, ethical but not legal)
  - Adherence to ethical principles may be required to meet regulatory requirements surrounding academic research
  - A law may illuminate the line between beneficial acts and harmful ones.
  - If the computer security research community develops ethical principals and standards that are acceptable to the profession and integrates those as standard practice, it makes it easier for legislatures and courts to effectively perform their functions.

IANAL

- Computer Fraud and Abuse Act (CFAA)
  - "It is illegal to intentionally access a computer without authorization or in excess of authorization and thereby obtaining information from any protecting computer."
- Digital Millennium Copyright Act (DMCA)
  - "No person shall circumvent a technological measure that effectively controls access to [a work protected by copyright law]"
- Electronic Communications Privacy Act (ECPA)
  - Wiretap Act
  - Pen Register Statute
  - Stored Communications Act
- State and Local Laws
  - Illinois; 720 ILCS § 5/17-50 to -55 (e.g., Computer fraud, Computer tampering)
- Computers and networks may carry data for a variety of institutions such as hospitals, libraries, universities, and K-12 organizations
  - Family Educational Right to Privacy Act (FERPA)
  - Federal Standards for Privacy of Individually Identifiable Health Information (implements the privacy requirements HIPAA)

Contracts and Policies

- End User License Agreements (EULA)
  - Do not criticize this product publicly
  - Using this product means you will be monitored
  - Do not reverse-engineer this product
  - We are not responsible if this product messes up your computer
- Organizational Policies

UIUC Policy Documents

- The Campus Administrative Manual (especially Policy on Appropriate Use of Computers and Network Systems at the University of Illinois at Urbana-Champaign)
- Student Code (especially 1-302 Rules of Conduct, 1–402 Academic Integrity Infractions.

Existing Ethics Standards

- 1947 Nuremberg Code
- Helsinki Declaration 1964
- The IEEE, ACM, etc: Codes of Ethics
- The Belmont Report, the National Research Act, and Institutional Review Boards (IRB)
  - 45 CFR 46
- "Rules of Engagement"
  - The Law of Armed Conflict
  - Dittrich/Himma: Active Response Continuum
- Other Organizational Codes (Universities, Corporations, etc.)

The Belmont Report

- "Ethical Principles and Guidelines for the Protection of Human Subjects of Research", United States Department of Health, Education, and Welfare, April 18, 1979 (Belmont Report)
- Respect for persons
  - Individuals should be treated autonomously
  - Informed consent should be freely given
- •Beneficence
  - Do no harm
  - Maximize possible benefits/minimize risks
- Distributive Justice
  - Equitable selection of research subjects

IRB

- The primary goal of the Institutional Review Board (IRB) is to assure that, in research involving human subjects, the rights and welfare of the subjects are adequately protected.
- Although many policies they enforce are rooted in ethical standards, IRB is *not* an ethics board and an approved protocol is not proof of ethicality.
- Further, lots of CS work does not meet the IRB's definition of human subjects research! E.g., OSN analysis.
- When in doubt, contact IRB and obtain documentation that your research is not under IRB purview
- If IRB does not govern most security research, what does?

The Menlo Report

- Interprets the Belmont Report with application to computer security research.
- Challenges:
  - Researcher-Subject relationships are disconnected and intermediated by technology
  - Proliferation of data sources and analytics that heighten risk
  - Overlap between research and operations

Menlo Example: Informed Consent

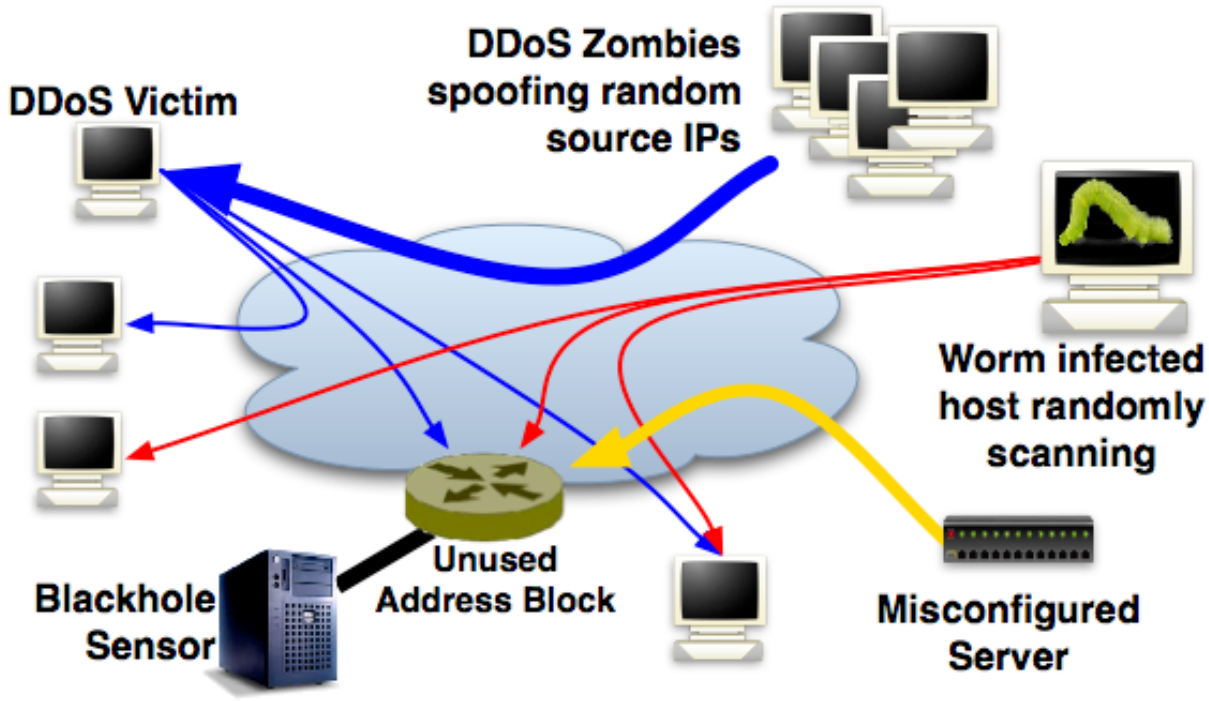
- Informed Consent? Often impossible, e.g., for network measurements.
  - Requirement can be waived with approval from research board if:
    - Entails no more than minimal risk
    - Waiver does not adversely affect rights and welfare of the subjects
    - Research would not be practical without waiver
    - Subjects will be provided with pertinent information after participation when applicable.
- Enables, e.g., IPv4-wide measurement of Heartbleed [Durumeric et al, IMC'14]

Professional Ethics Codes

- •IEEE Code of Ethics (2006)
  - commits members "to the highest ethical and professional conduct". Members agree to avoid conflicts of interest, be honest, engage in responsible decision making, accept criticism of work, etc
- •ACM Code of Ethics and Professional conduct (1992)
  - "contribute to society and human well-being", "avoid harm to others", along with six other principles (e.g., don't discriminate, be honest, respect privacy).

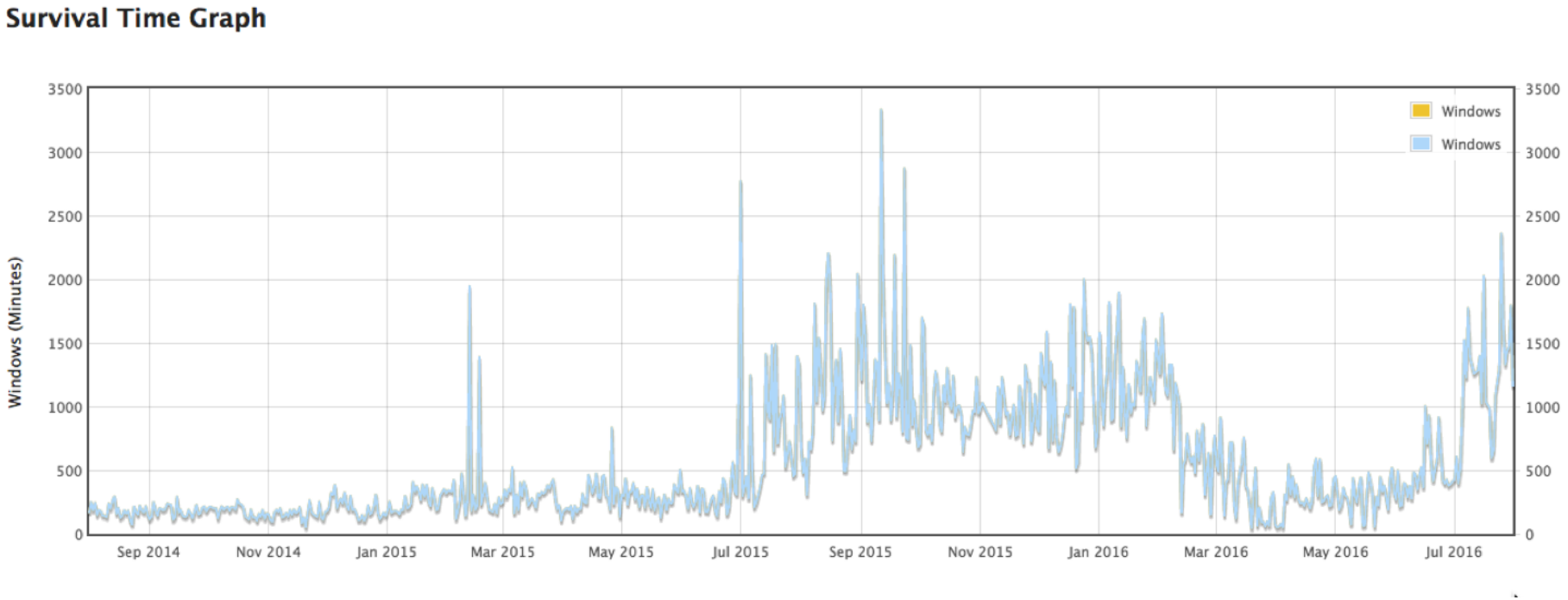
Case Study: Honeypots

- The researchers create a research testbed, connected to the Internet, which enables testbed machines to become infected.



Case Study: Honeypots

- The researchers create a research testbed, connected to the Internet, which enables testbed machines to become infected.



Case Study: Honeypots

[John et al., NSDI'09]

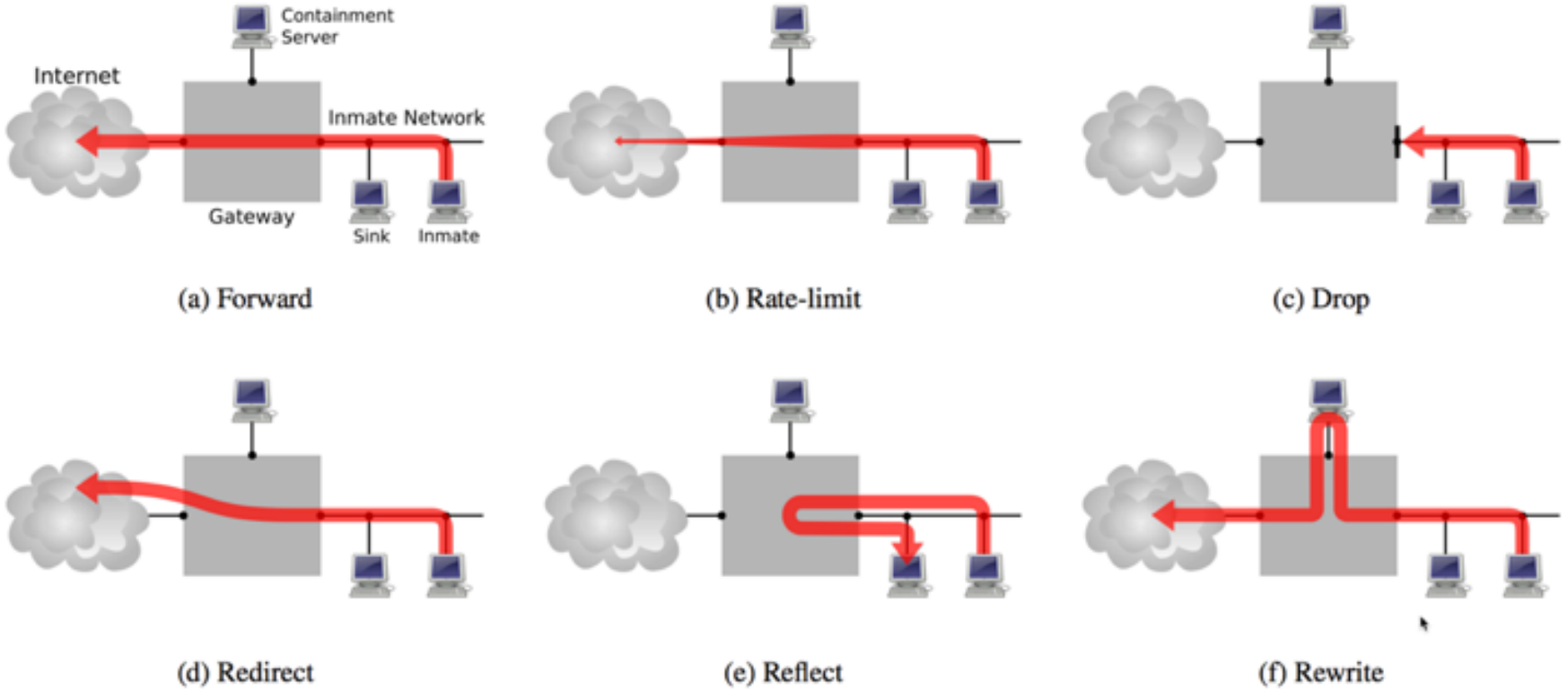
- The only provably safe way for Botlab to execute untrusted code is to block all network traffic, but this would render Botlab ineffective
- …However, botnet trends and thought experiments have diminished our confidence that we can continue to conduct our research safely
- …Given these concerns, we have disabled the crawling and network fingerprinting aspects of Botlab, and therefore are no longer analyzing or incorporating new binaries.

•https://www.usenix.org/legacy/event/nsdi09/tech/full_papers/john/john_html/

Case Study: Honeypots

[Kreibich et al., IMC'11]

- "Inmate Control" primitives



Case Study: White Worms Hack Back

- Researchers plan to clean up the botnet by enumerating the infected hosts, exploiting a vulnerability, and removing the infected code.
- What could go wrong?

InternetNews.com RealTime IT News Sign In

Software | Security | Storage | Servers | Networking & Communications | Developer | Small Business | Mobile | IT M

Understand your business at the present and anticipate the future with business intelligence applications. Get your free eBook now.

Home → Enterprise → 'Friendly' Welchia Worm Wreaking Havoc

'Friendly' Welchia Worm Wreaking Havoc

By Ryan Naraine | August 19, 2003

Page 1 of 1

It may be a friendly worm with good intentions but the W32.Welchia.Worm squirming through corporate networks has become a nightmare for IT administrators already struggling to clean up last week's "Blaster" virus.

Case Study: White Worms Hack Back

BBC NEWS

Watch One-Minute World News

News Front Page

Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science & Environment
Technology
Entertainment
Also in the news

Last Updated: Thursday, 2 December, 2004, 11:26 GMT

E-mail this to a friend Printable version

Anti-spam plan overwhelms sites

A plan to bump up the bandwidth bills of spammers seems to be getting out of control.

The screensaver uses idle computers to tackle spam sites

Earlier this week Lycos Europe released a screensaver that bombards spam websites with data to try to increase the cost of running such sites.

But analysis shows that, in some cases, spam websites are being completely overwhelmed by the traffic being directed their way.

The Lycos plan has also come under fire for encouraging vigilantism.

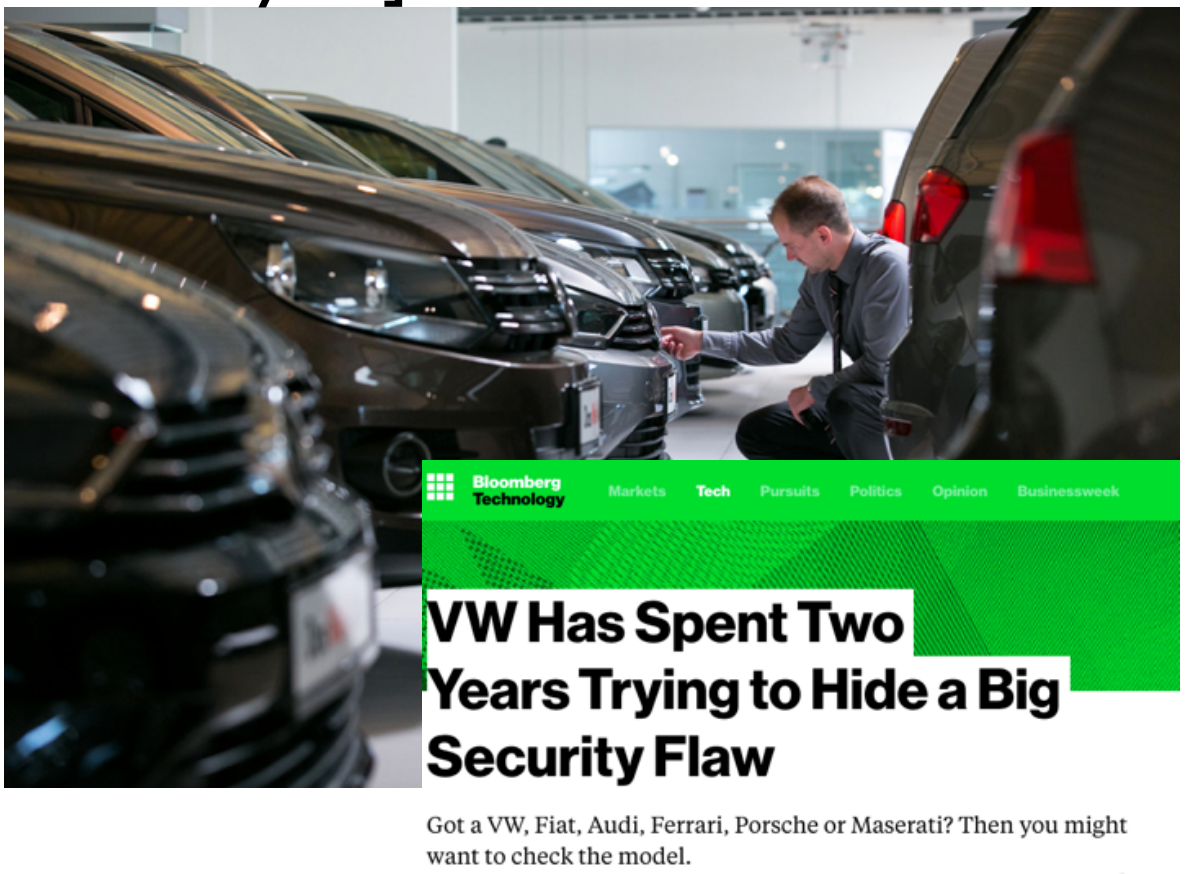
Case Study: Reverse Engineering, Vulnerability Disclosure?

- Researchers reverse engineer a system, discover a vulnerability, and generate a working exploit (attack).
- Does exposing the problem "help"?
- Nice Debate:
  - https://www.schneier.com/essays/archives/2008/05/the_ethics_of_vulner.html
  - http://www.ranum.com/security/computer_security/editorials/point-counterpoint/vulnpimps.html

Case Study: Research Suppression

On the other hand, what if the company refuses to take responsibility for the problem?

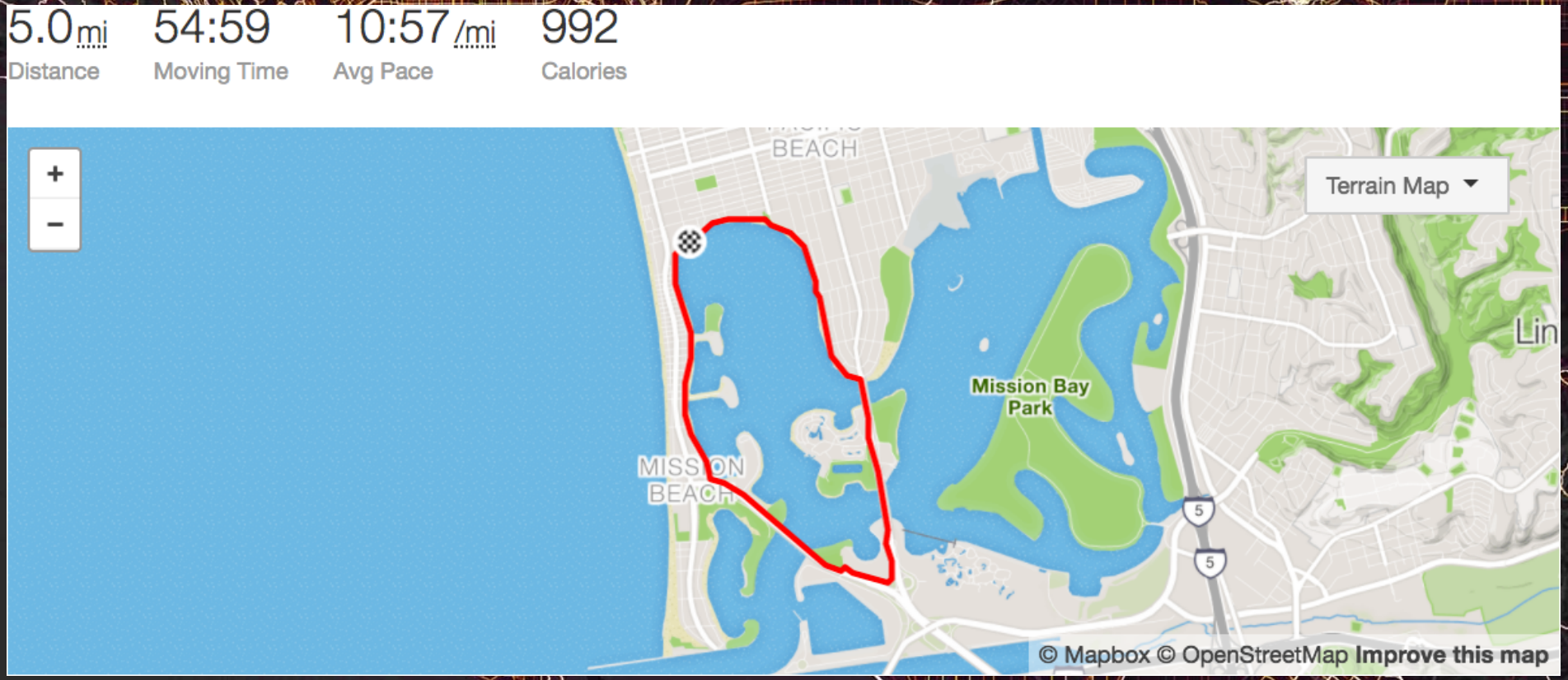
[Verdult et al., Security'15]



https://www.usenix.org/sites/default/files/sec15_supplement.pdf

Case Study: OSN Measurement

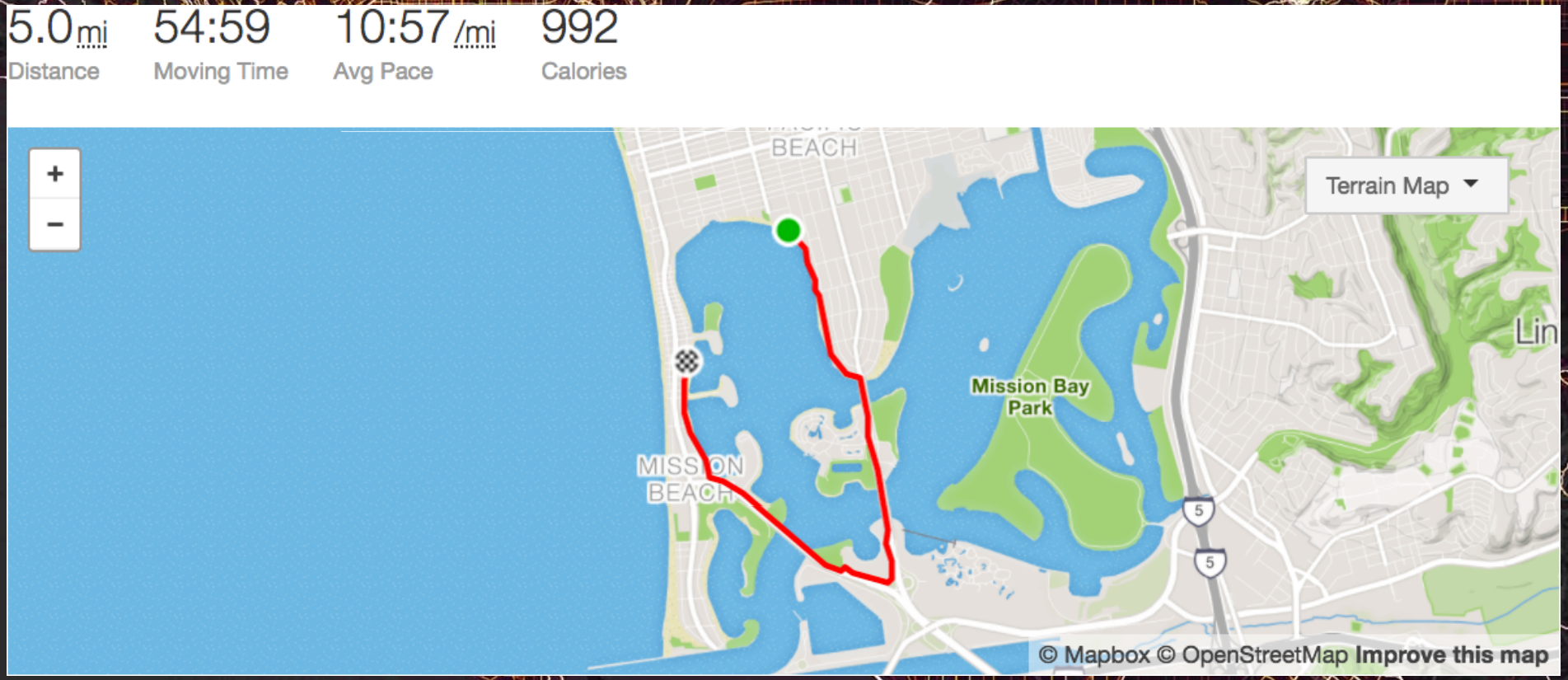
Endpoint Privacy Zones…



STRAVA™

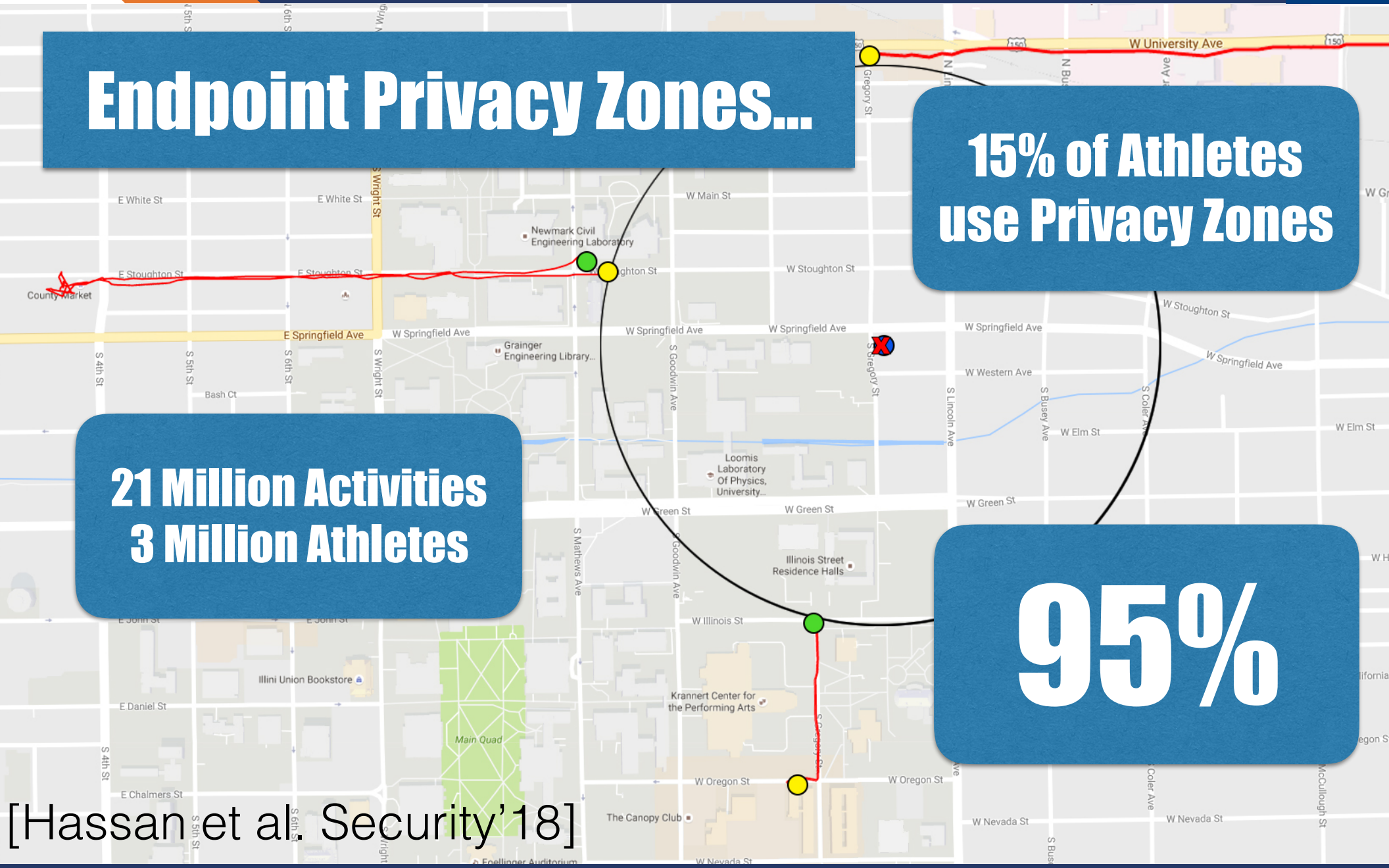
Case Study: OSN Measurement

Endpoint Privacy Zones…



STRAVA™

Case Study: OSN Measurement



[Hassan et al. Security'18]

Case Study: OSN Measurement

Research Timeline

1. Conduct the research and submit first version of paper; ethical discussion of how our work follows well-established community norms is included.
2. Notify affected companies of vulnerability
3. Reviewers unsatisfied with ethical argument, (mistakenly) think an IRB protocol is needed, reject paper.
4. Research team consults institutional IRB, receive written confirmation that study is not human subjects research, resubmit.
5. Paper accepted, but embargoed (not public)
6. Companies address issues and publicly announce fix.
7. We release the paper and present it at USENIX Security '18.

Responsible Disclosure

- **Latent Flaw**. A flaw is introduced into a product during its design, specification, development, installation, or default configuration.
- **Discovery**. One or more individuals or organizations discover the flaw through casual evaluation, by accident, or as a result of focused analysis and testing.
- **Notification**. A reporter or coordinator notifies the vendor of the vulnerability ("Initial Notification"). In turn, the vendor provides the reporter or coordinator with assurances that the notification was received ("Vendor Receipt").
- **Validation**. The vendor or other parties verify and validate the reporter's claims ("Reproduction").
- **Resolution**. The vendor and other parties also try to identify where the flaw resides ("Diagnosis"). The vendor develops a patch or workaround that eliminates or reduces the risk of the vulnerability ("Fix Development"). The patch is then tested by other parties (such as reporter or coordinator) to ensure that the flaw has been corrected ("Patch Testing").
- **Release**. The vendor, coordinator, and/or reporter release the information about the vulnerability, along with its resolution.
- **Follow-up**. The vendor, customer, coordinator, reporter, or security community may conduct additional analysis of the vulnerability or the quality of its resolution.

Moving Forward

- In this class you will not be asked to do anything that is illegal, unethical, or against university policy, so maybe you shouldn't …
- Ask permission not forgiveness
- Principle of Least Surprise: If it would surprise a technology/service representative that their product was being used in a particular way, there is potential risk that the use is unethical.

To Learn More…

- Stalling and Brown, Chapter 19
- Pfleeger and Pfleeger, Chapter 11
- Easttom, Chapter 1
- "Conducting Cybersecurity Research Legally and Ethically" - Burstein
- "The Menlo Report" - Bailey