Lecture 02 – Ethics

Michael Bailey
University of Illinois
ECE 422/CS 461 – Spring 2018

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.

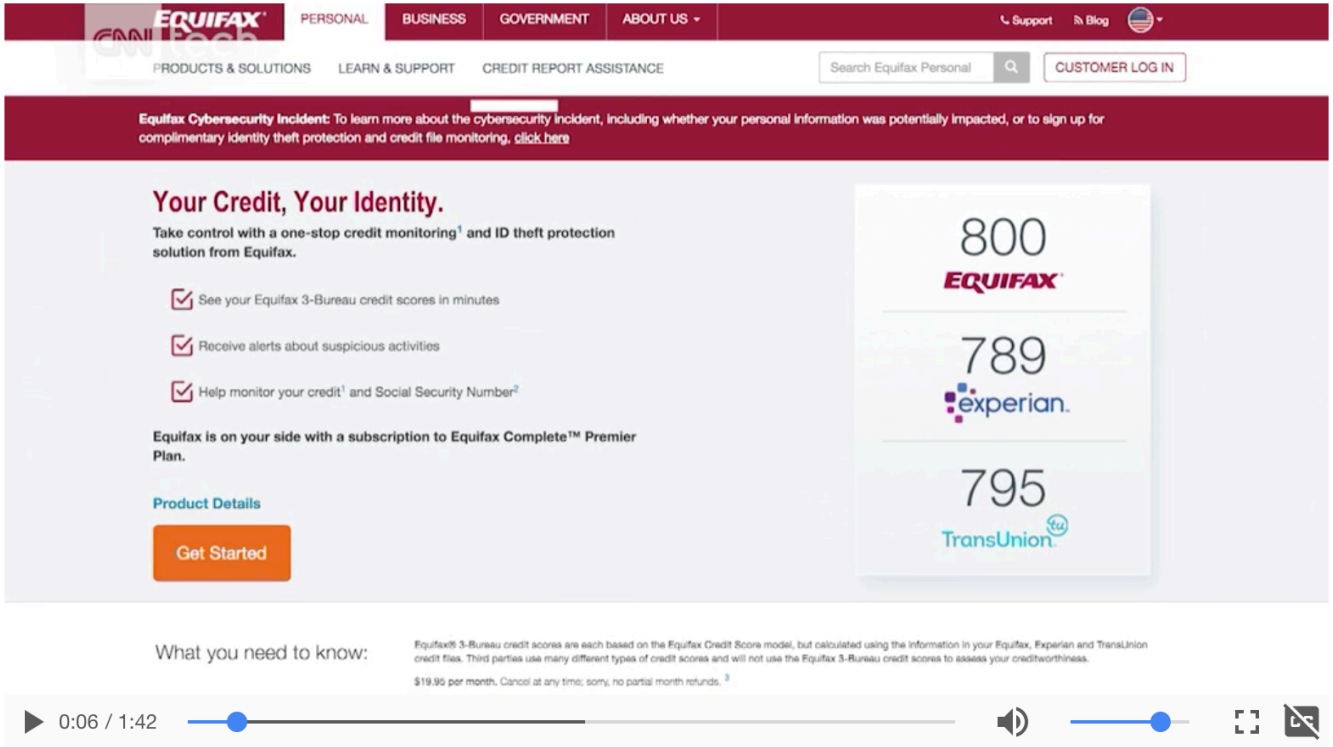
dunbar7376 January 4, 2018
I have found a third major flaw: not one woman in your RSA conference pic.

SEE ALL COMMENTS

Giant Equifax data breach: 143 million people could be affected

by Sara Ashley O'Brien @saraashleyo

September 8, 2017: 9:23 AM ET



5 of the biggest data breaches ever

Equifax says a giant cybersecurity breach compromised the

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

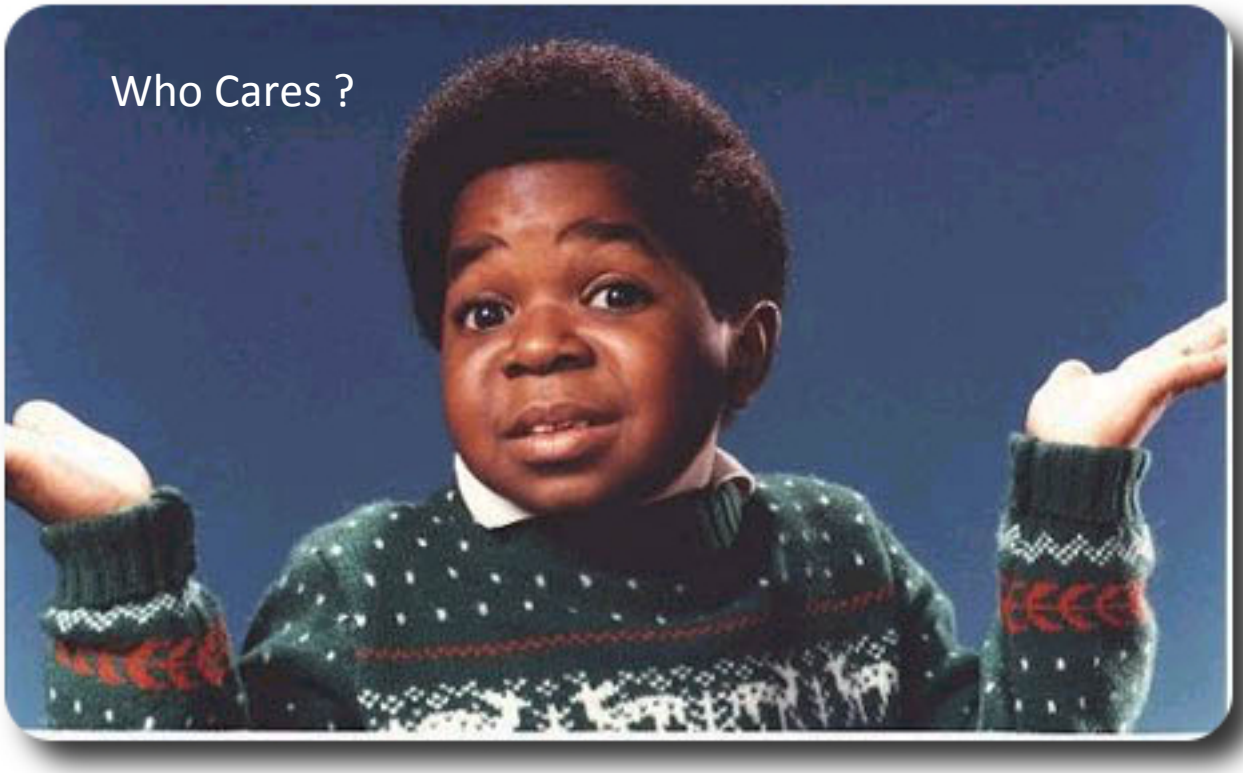
Security “Research” to the Rescue!

- White hats (grey hats?) want to help, to **benefit** the internet community
- …but oh, the temptations!

  First to publish; do something new; show how 31337 you are; fight for funding; ends justify the means
- …and the conflicts

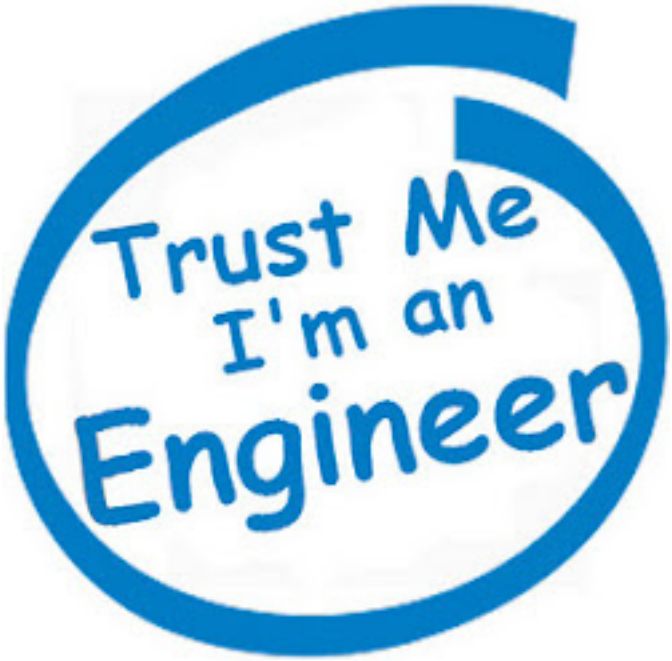
  Affecting other research; impacting LE investigations; thwarting mitigation efforts; protecting rights; helping the bad guys; less risky (and less attractive) options?

Security “Research” to the Rescue!



- Res *ernet com*
- …bu
  Firs 337
  y s
- …ar
  Affe ons;
  th elping
  the bad guys; less risky (and less sexy) options?

Don’t get caught playing …



There is gonna be an epic fail

The New Yo

January 21st, 2015

Security Students Jailed

Students in Professor Michael Bailey ECE 422 class were jailed this week after having illegally and unethically attacked University of Illinois electronic systems. Bailey's class, entitled Security I, taught students security fundamentals including Buffer overflow attacks, Cross-site scripting attacks, and other common methods used by modern attackers. Students used the techniques taught to attack the grading system

Ren
foll
imp

The
that
rela
the
beh

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

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.)

IRB and the Belmont report

- 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.
- "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

Professional Ethical Codes

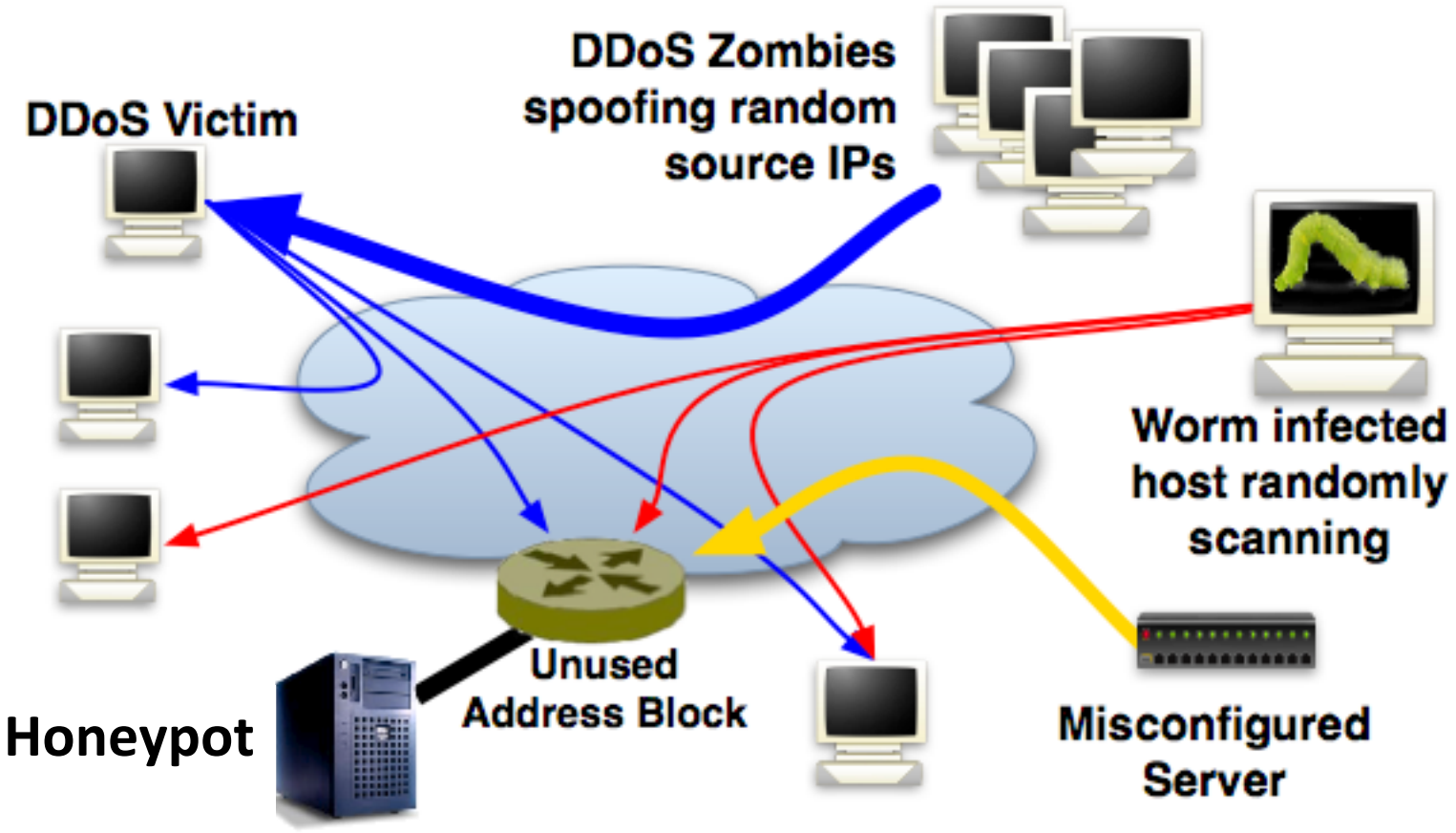
- IEEE Code of Ethics (2006)
  - commits members ”to the highest ethical and professional conduct”. Members agree to avoid conflicts of interest, be honest, engage in responsible decision making, accept criticism of work, etc
- ACM Code of Ethics and Professional conduct (1992)
  - “contribute to society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


Welcome to
NEWBIE
Please drive carefully

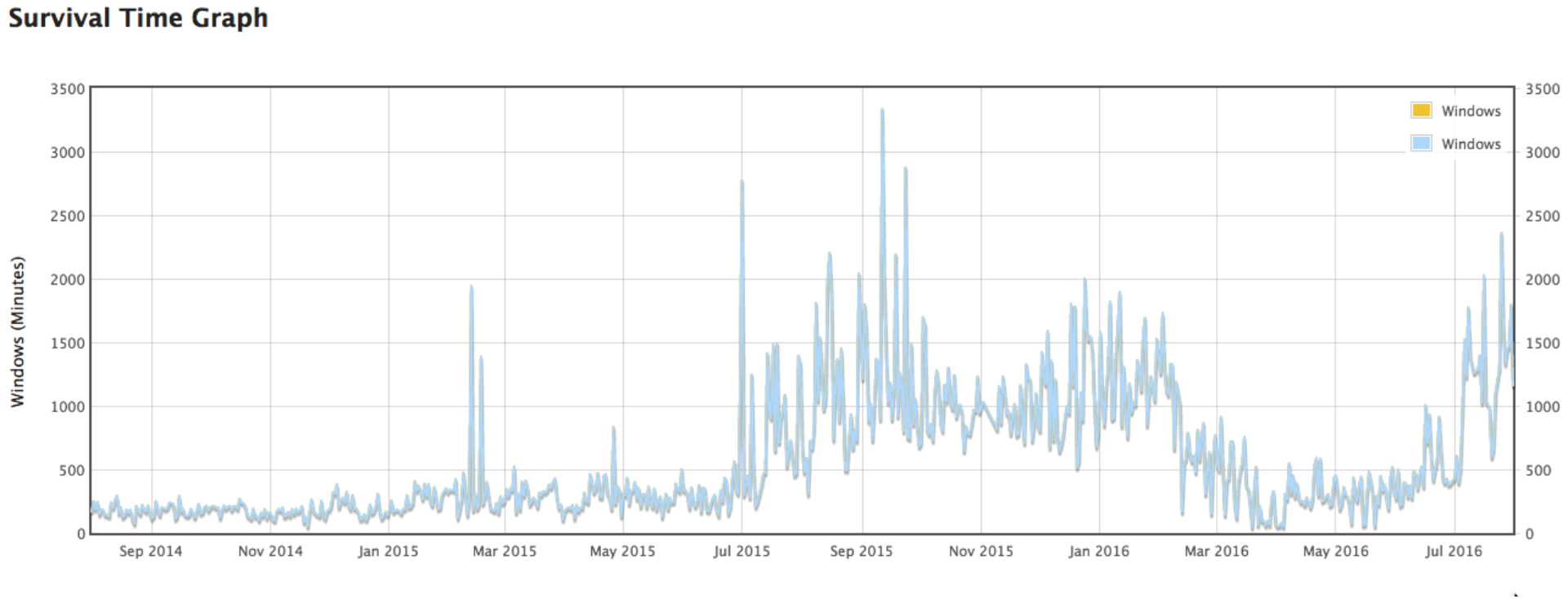
Case Study: Honeypots

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

Case Study: Honeypots



Case Study: Honeypots



Case Study: Honeypots

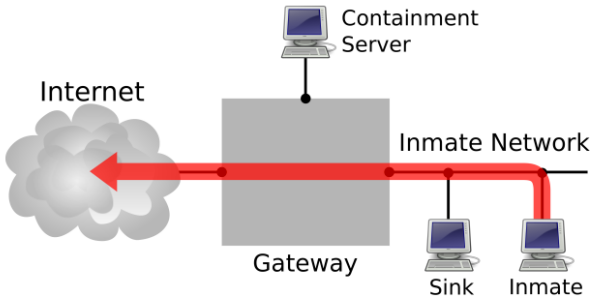
- The researchers create a research testbed, connected to the Internet, which enables testbed machines to become infected.

Honeypot Guidance

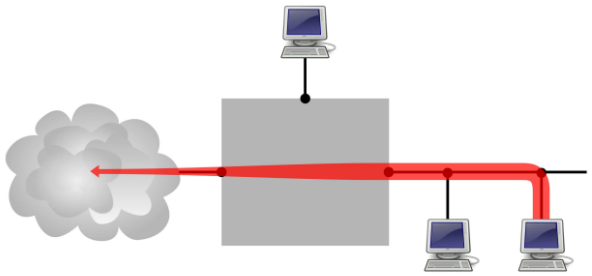
- https://www.usenix.org/legacy/event/nsdi09/tech/full_papers/john/john_html/
  - The only provably safe way for Botlab to execute untrusted code is to block all network traffic, but this would render Botlab ineffective
  - …However, botnet trends and thought experiments have **diminished our confidence that we can continue to conduct our research safey**
  - …Given these concerns, we have disabled the crawling and network fingerprinting aspects of Botlab, and **therefore are no longer analyzing or incorporating new binaries.**

Honeypot Guidance

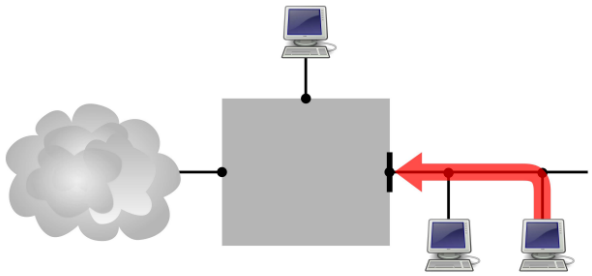
- http://www.icir.org/vern/papers/gq.imc2011.pdf



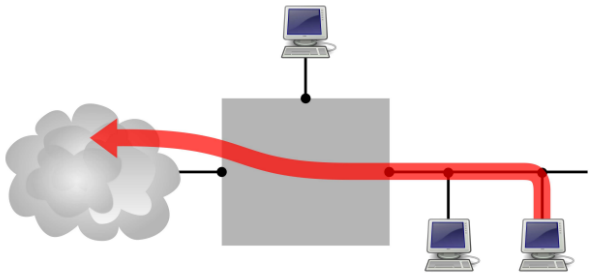
(a) Forward



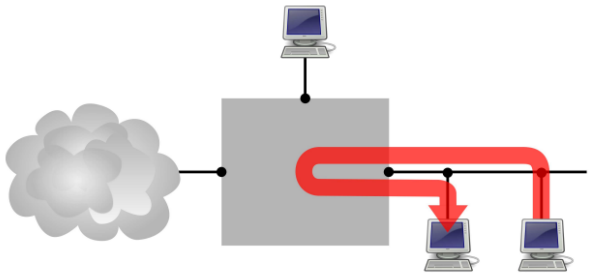
(b) Rate-limit



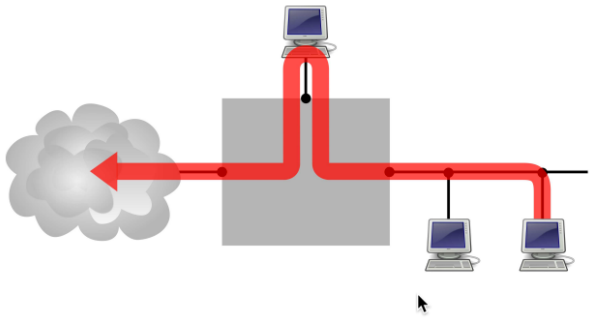
(c) Drop



(d) Redirect



(e) Reflect



(f) Rewrite

Case Study: White Worms, Hack Back

- Researchers clean up the botnet by enumerating the infected hosts, exploiting a vulnerability, and removing the infected code.

'Friendly' Welchia Worm Wreaking Havoc

By Ryan Naraine | August 19, 2003

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.

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.

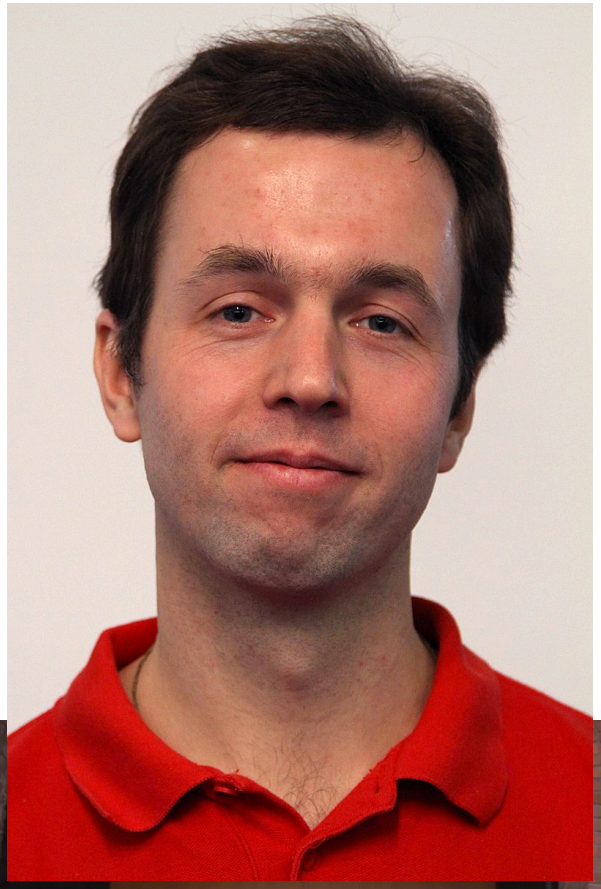
The Lycos plan has also come under fire for encouraging vigilantism.

Case Study: Reverse Engineering, Vulnerability Disclosure?

- Researchers reverse engineer a system, discover a vulnerability, and generate a working exploit (attack).
- 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

VW Has Spent Two Years Trying to Hide a Big Security Flaw

Got a VW, Fiat, Audi, Ferrari, Porsche or Maserati? Then you might want to check the model.



ROBERT S. MUELLER, III (CSBN 59775)
United States Attorney

FILED

AUG 28 2001

RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

ELCOM LTD.
a/k/a ELCOMSOFT CO. LTD. and
DMITRY SKLYAROV,

Defendants.

CR 01 20138

VIOLATIONS: 18 U.S.C. § 371 – Conspiracy; 17 U.S.C. § 1201(b)(1)(A) – Trafficking for Gain in Technology Primarily Designed to Circumvent Technology that Protects a Right of a Copyright Owner; 17 U.S.C. § 1201(b)(1)(C) – Trafficking for Gain in Technology Marketed for Use in Circumventing Technology that Protects a Right of a Copyright Owner; 18 U.S.C. § 2 – Aiding and Abetting

SAN JOSE VENUE

INDICTMENT

BACKGROUND

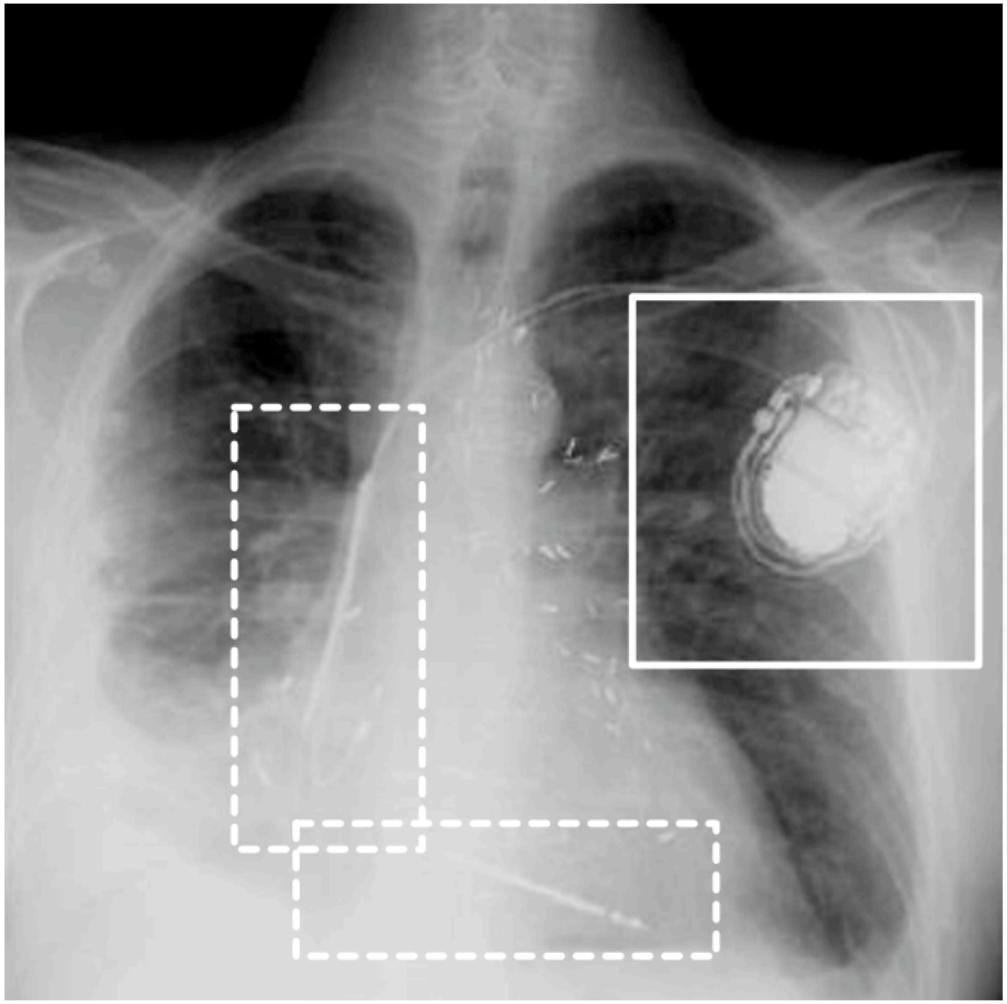
levant to the indictment:

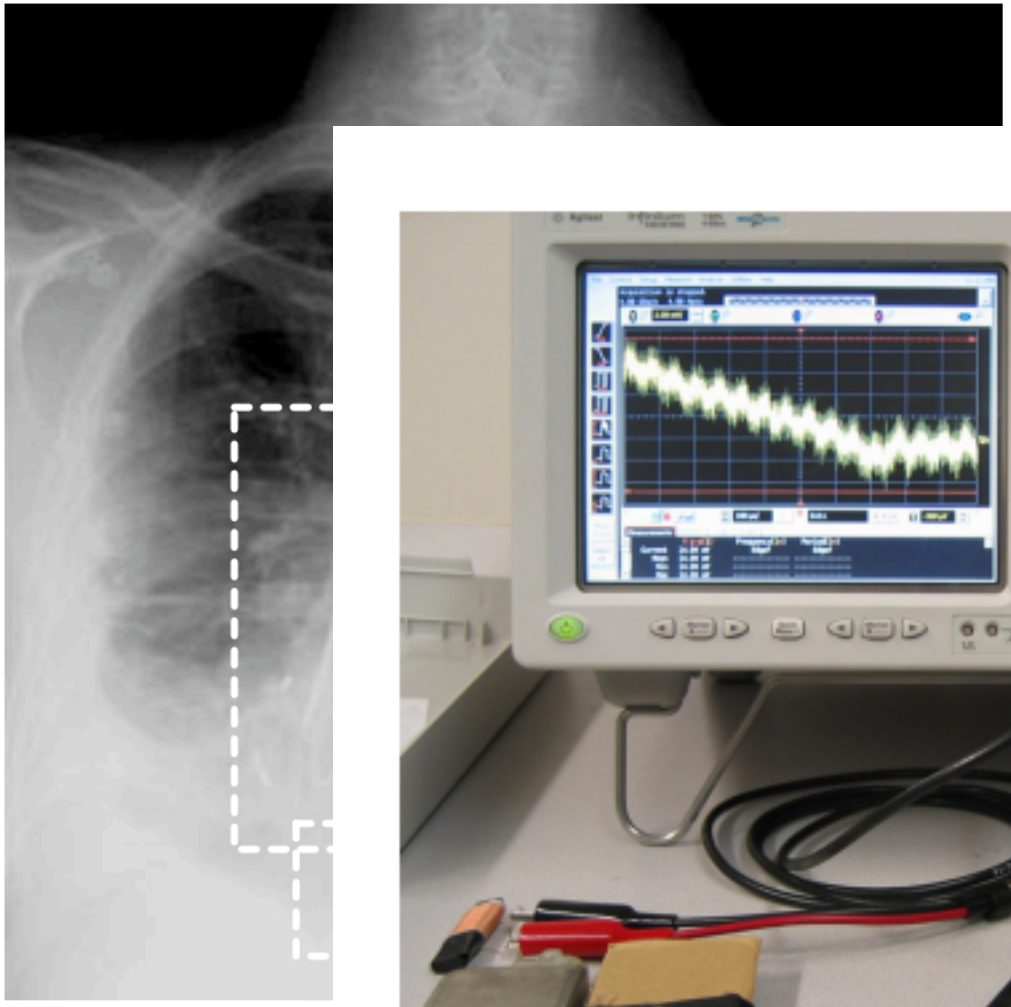
ndant Elcom Ltd., a/k/a Elcomsoft Co. Ltd. ("Elcomsoft"), was a

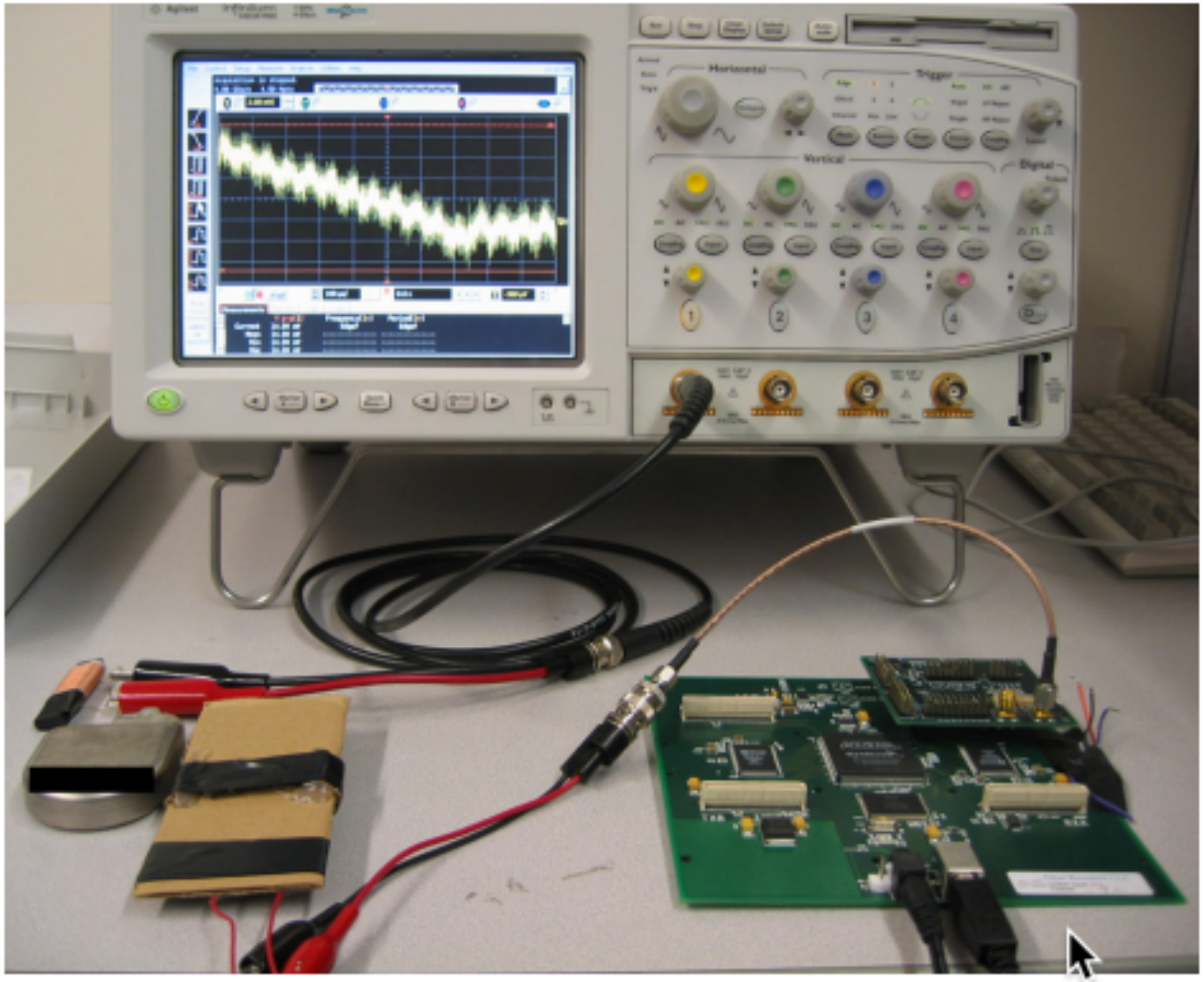
tered in Moscow, Russia.

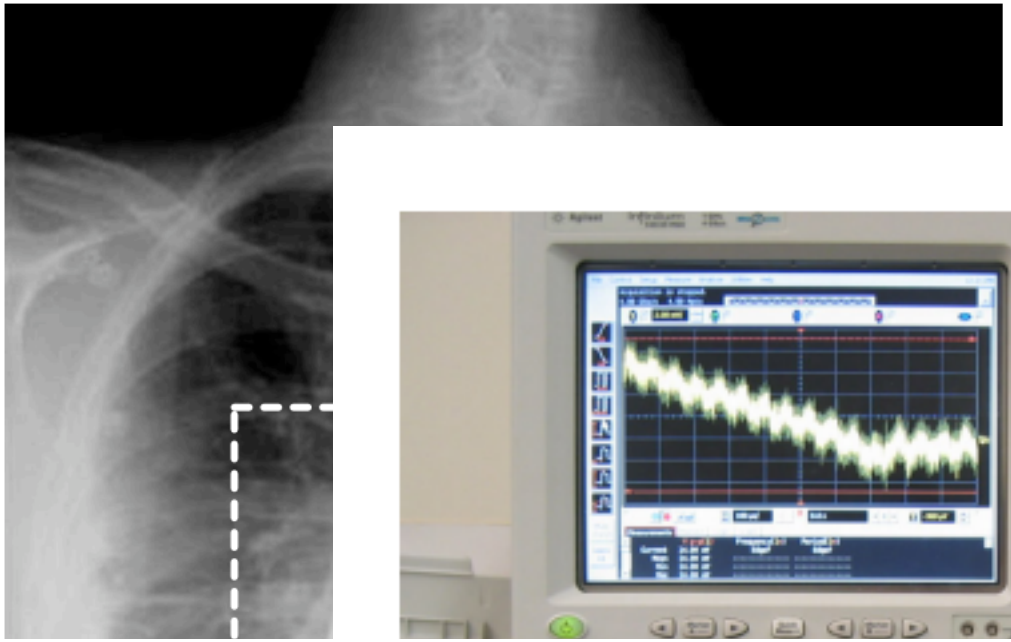
e Systems, Inc., ("Adobe") was a software company headquartered in

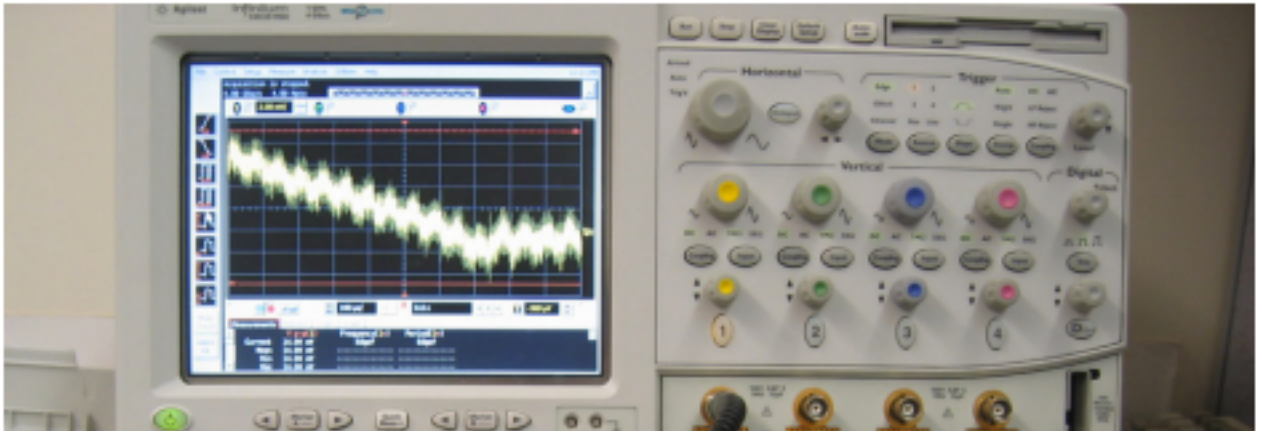
oduced publishing software for various media including the world wide



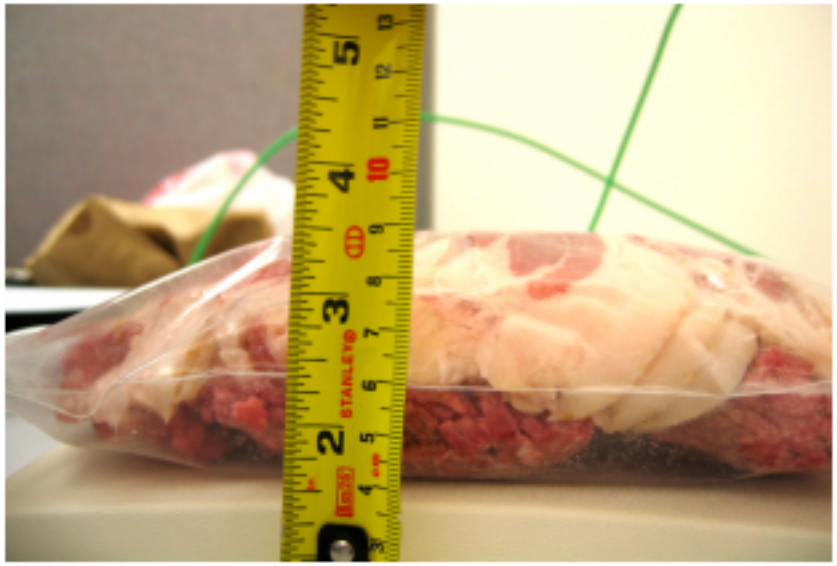


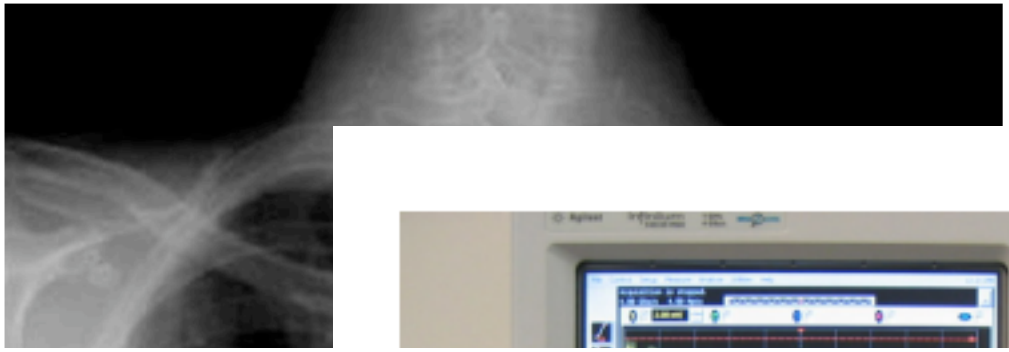

Horizontal
Trigger
Vertical
Digital

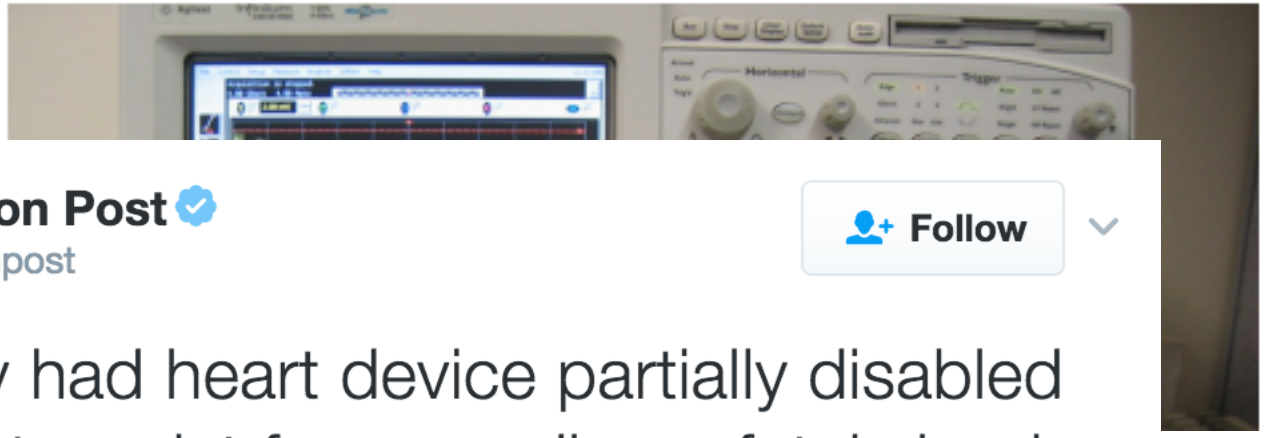



Horizontal
Trigger
Vertical
Digital


STANLEY


STANLEY





Washington Post
@washingtonpost

Follow

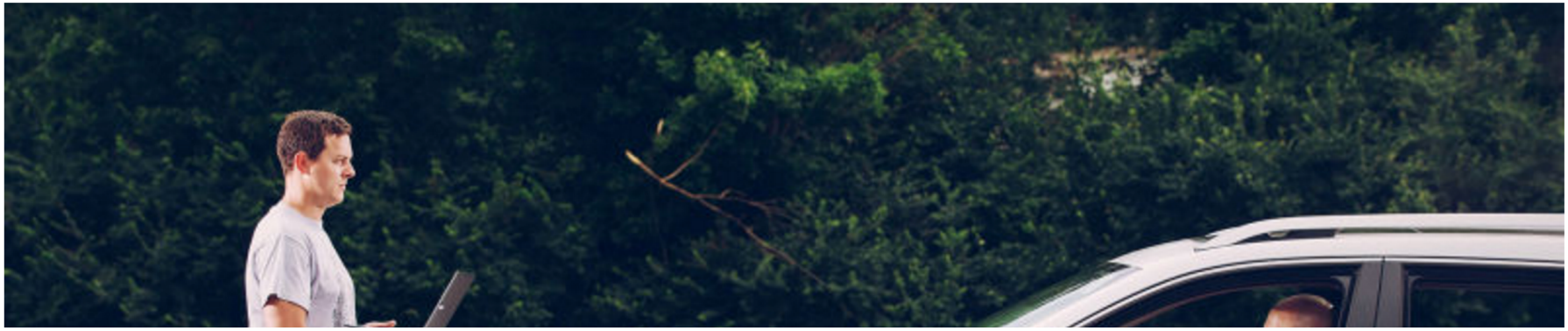
Dick Cheney had heart device partially disabled to prevent a terrorist from sending a fatal shock. Before 'Homeland' wapo.st/19hzxlR

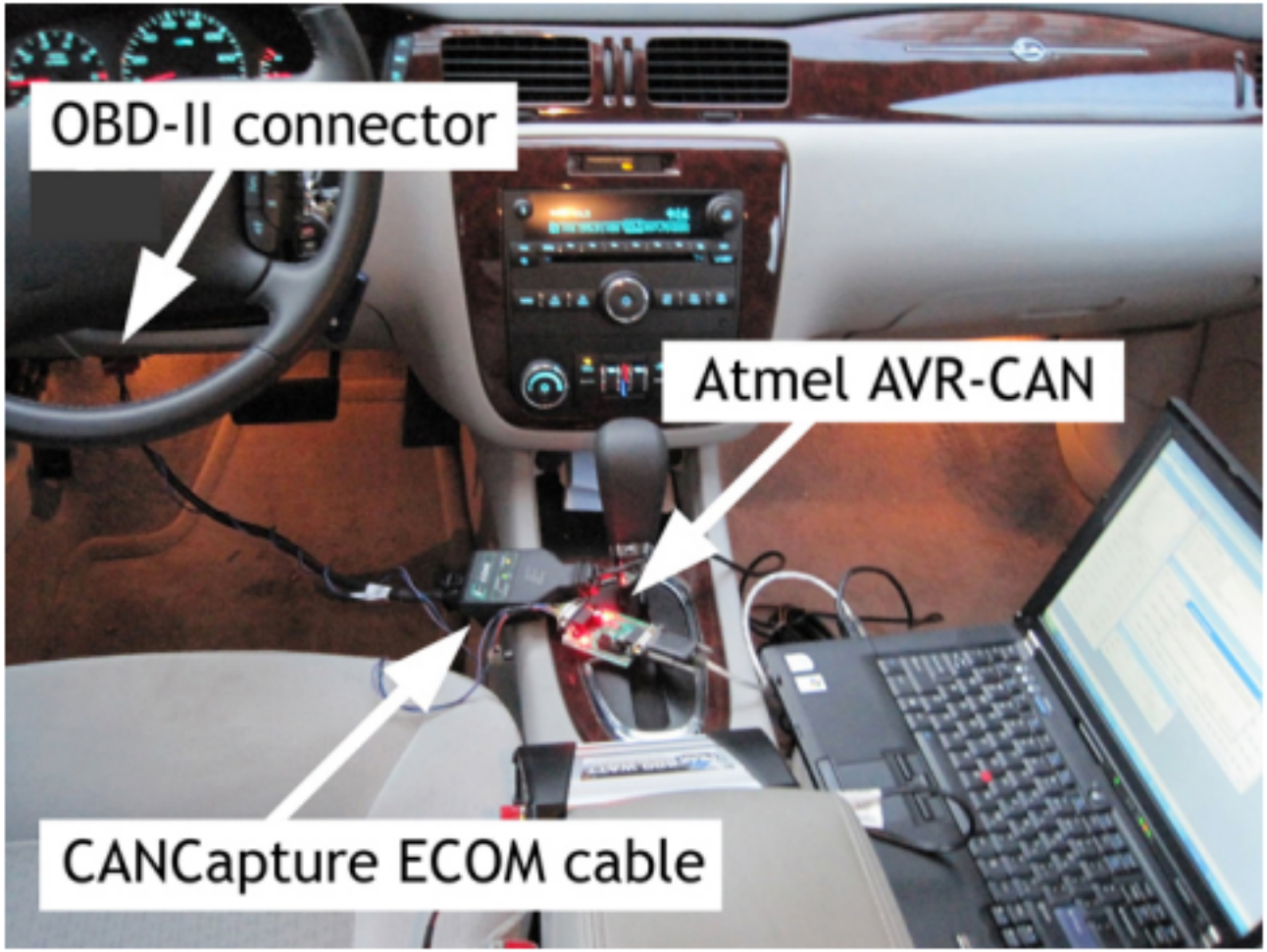
RETWEETS	LIKES
99	19

11:26 AM - 19 Oct 2013

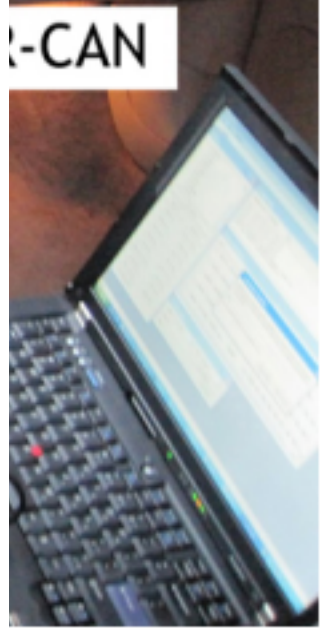
ANDY GREENBERG SECURITY 07.21.15 6:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT




OBD-II connector
Atmel AVR-CAN
CANCapture ECOM cable


OBD-II connector


-CAN


0
20
40
60
80
100
120
140
MPH
Pwned by CarShark
CARSHARKED X_X
P R N D 3 2 1

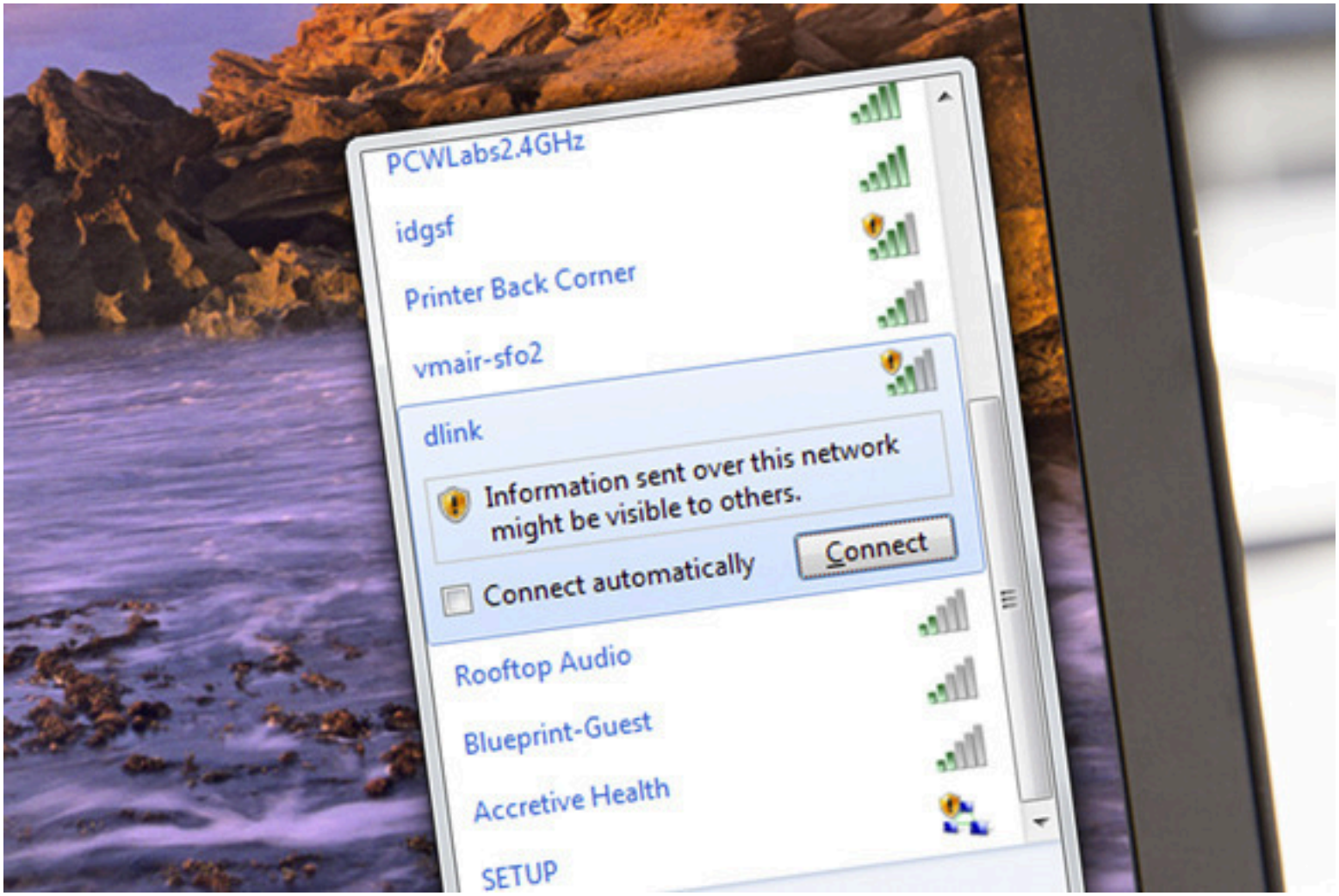

-CAN

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.

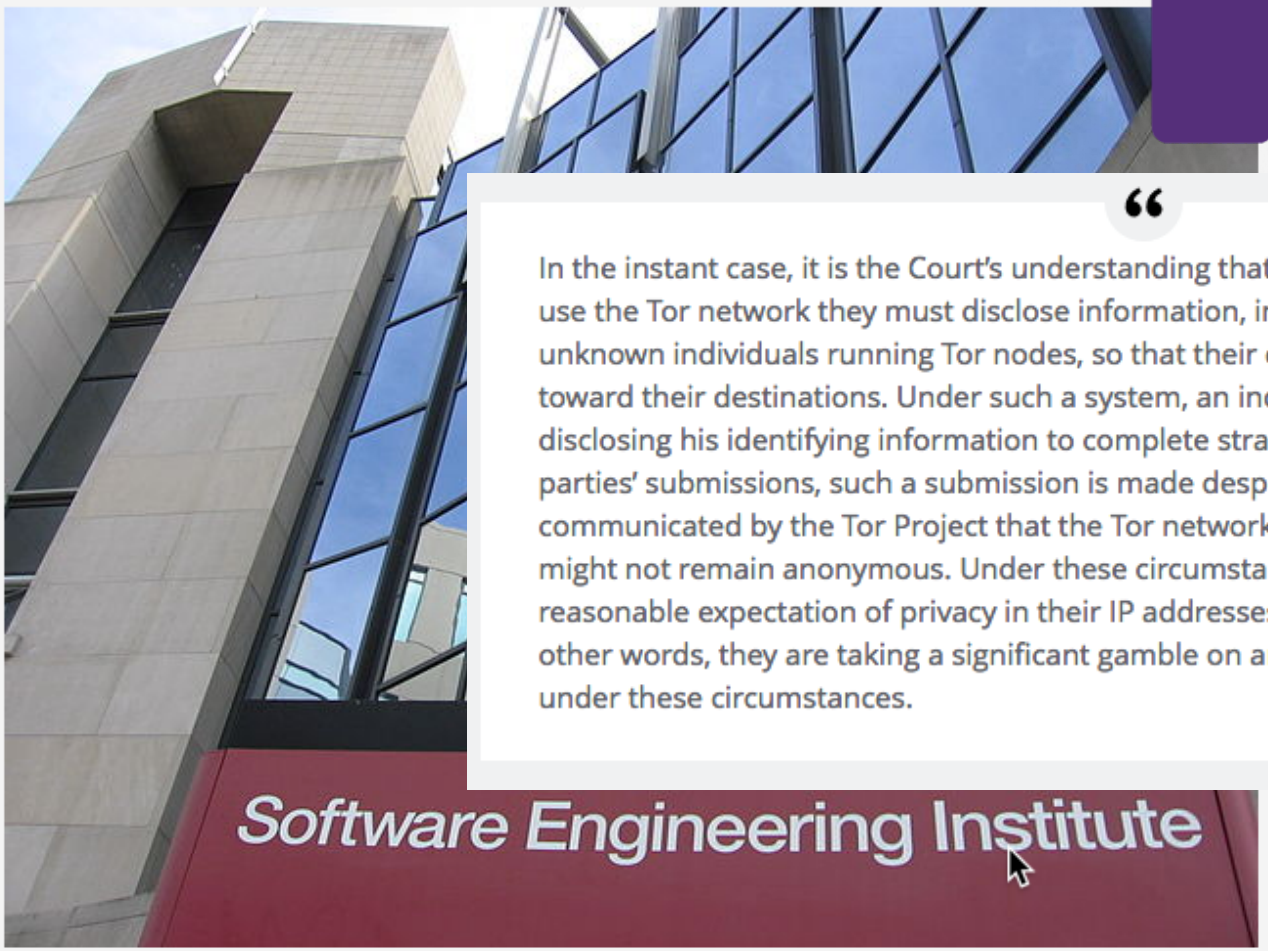
Wireless Eavesdropping

- A student in class creates a wireless network access point with no encryption or authentication and observes users who connect to it.


PCWLabs2.4GHz
idgsf
Printer Back Corner
vmair-sfo2
dlink
Information sent over this network might be visible to others.
Connect automatically
Connect
Rooftop Audio
Blueprint-Guest
Accretive Health
SETUP

Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds

February 24, 2016 // 09:05 AM EST



> In the instant case, it is the Court's understanding that in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations. Under such a system, an individual would necessarily be disclosing his identifying information to complete strangers. Again, according to the parties' submissions, such a submission is made despite the understanding communicated by the Tor Project that the Tor network has vulnerabilities and that users might not remain anonymous. Under these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network. In other words, they are taking a significant gamble on any real expectation of privacy under these circumstances.

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

To Learn More …

- http://www.icir.org/vern/cs261n/papers/burstein_legal_leet.pdf
- David Dittrich, Michael Bailey, Sven Dietrich. Building an Active Computer Security Ethics Community.
- Dittrich, David and Kenneally, Erin and Bailey, Michael, Applying Ethical Principles to Information and Communication Technology Research: A Companion to the Menlo Report
- https://www.acm.org/about/code-of-ethics
- http://www.ieee.org/about/corporate/governance/p7-8.html
- https://www.eff.org/pages/grey-hat-guide
- http://www.cam.illinois.edu/viii/viii-1.1.htm

Questions?