Lecture 2:
Ethics and The Law

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Fall 2017

Security News

- Enigma (cryptocurrency company) compromised and 1.5k Ethereum stolen (worth $500k)
- 8 cybersecurity experts resigned from National Infrastructure Advisory Council in
- MalwareTech gets donations from stolen credit cards

CNN tech business culture gadgets future startups search

Yahoo says data stolen from 1 billion accounts

by Seth Fiegerman @sfiegerman

December 15, 2016: 4:30 AM ET

Timeline: The rise and fall of Yahoo

Gary Cameron / Reuters

Did Putin Direct Russian Hacking? And Other Big Questions


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt


Thank goodness for the white hats

Hacker “Hats”

- Black hat – maliciously breaks into systems for personal gain
- Grey hat – may violate laws or ethical standards, but not maliciously
- White hat – breaks into systems to improve security

White Hats 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 1337 you are; cash in 💰💰💰; ends justify the means
- …and the conflicts

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

White Hats to the Rescue!

- White
- …but

  First t

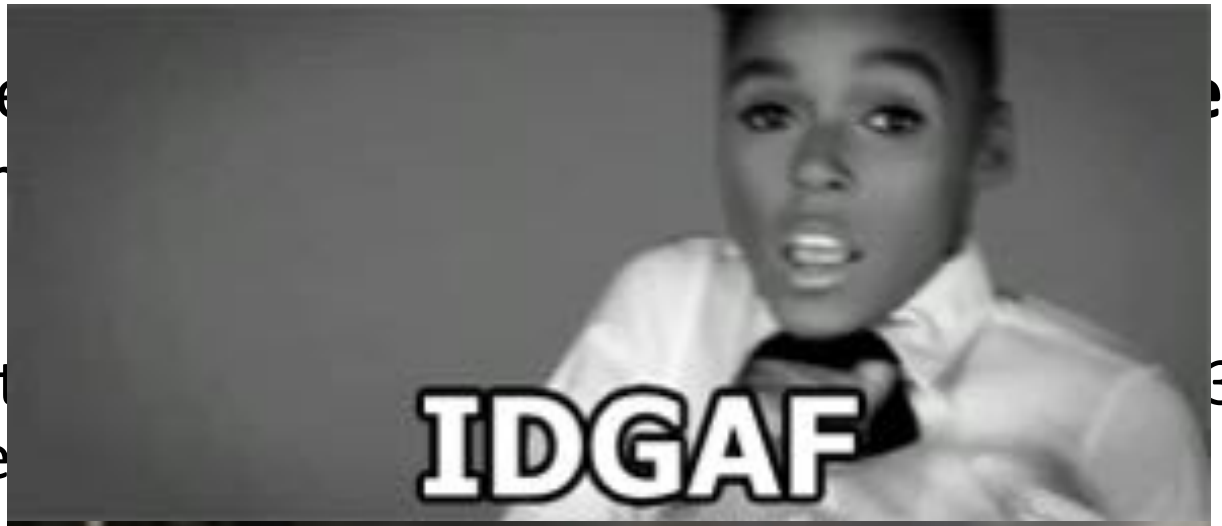
  are
- …and

  Affec

  thw

  priv

  att



enefit

337 you

tions;

iolating

ess

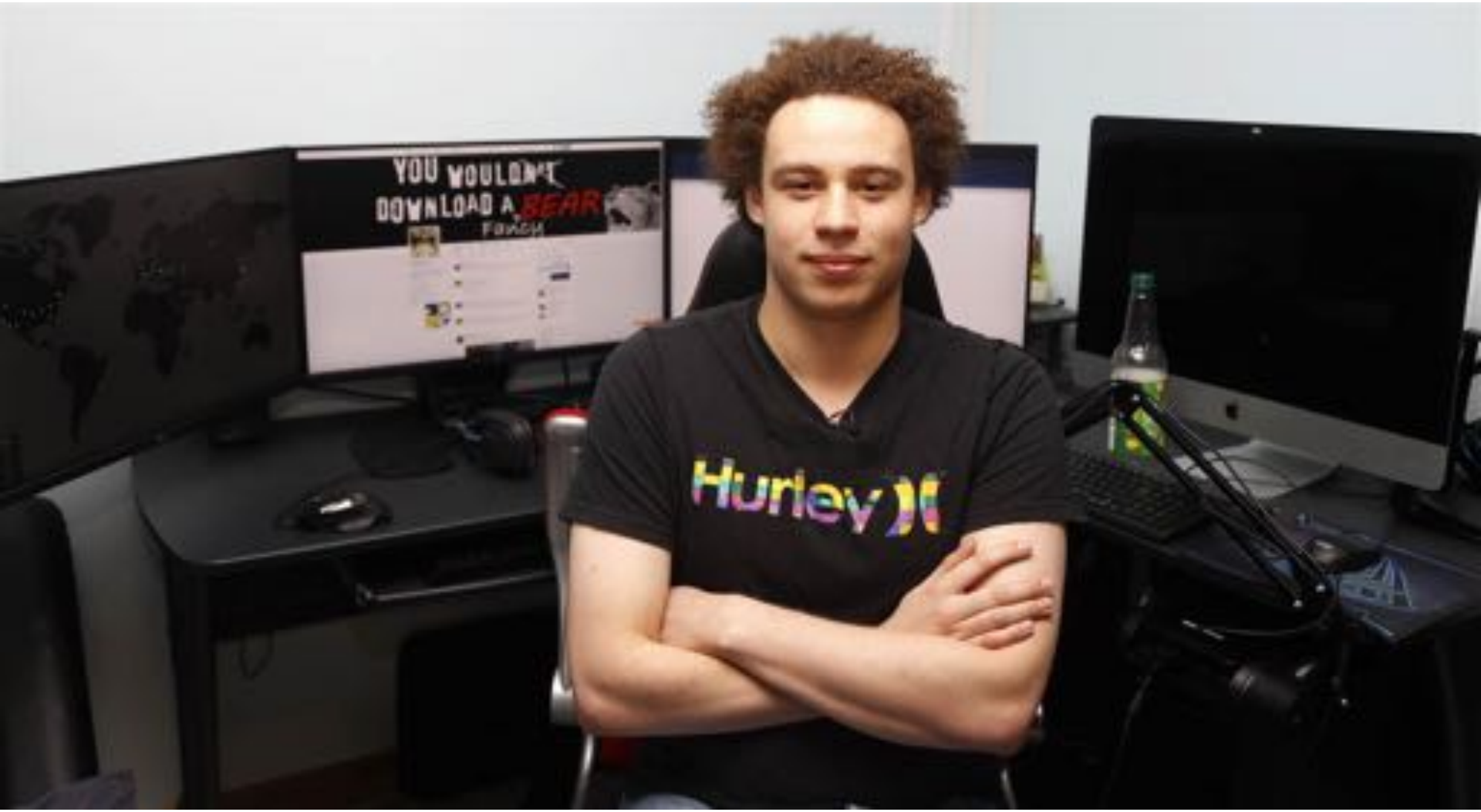
Former UI student arrested in computer incidents, building damage

Tue, 01/22/2013 - 9:00am | Julie Wurth

URBANA — An investigation that involved bomb squads, falsified emails, computer hacking and damage to a campus building resulted in the arrest of a former University of Illinois engineering student over the weekend.

Daniel Beckwitt, 21, of Bethesda, Md., was arrested by University of Illinois Police on Friday for computer tampering and taken to the Champaign County Jail. He was released Sunday after posting $1,000 bond and is scheduled to appear in arraignment court Tuesday afternoon.

Beckwitt was enrolled in the UI Department of Electrical and Computer Engineering last fall but is not a registered student this semester, according to UI police.


YOU WOULDN'T
DOWNLOAD A BEAR
Hurley

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.
  - Consequentialism
  - Deontology
  - Virtue ethics

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)

- 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 a
- D
ci
a
- E
R
- S
C
- C
ir

organizations - Family Educational Right to Privacy Act (FERPA), Federal Standards for Privacy of Individually Identifiable Health Information (implements the privacy requirements HIPAA)

DOJ Computer Crime Manual

TABLE 1. SUMMARY OF CFAA PENALTIES

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

Other Laws

- 18 U.S. Code § 1037 - Fraud and related activity in connection with electronic mail
- 18 U.S. Code § 1462 - Importation or transportation of obscene matters
- 18 U.S. Code § 1466A - Obscene visual representations of the sexual abuse of children
- 18 U.S.C. § 2252 – Certain activities relating to material involving the sexual exploitation of minors
- 18 U.S. Code § 2252A - Certain activities relating to material constituting or containing child pornography
- 18 U.S. Code § 2252B - Misleading domain names on the Internet
- 18 U.S. Code § 2252C - Misleading words or digital images on the Internet
- 31 U.S. Code § 5361-5365 – The Unlawful Internet Gambling Enforcement Act

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).

Professional Ethical Codes

- ACM Code of Ethics and Professional conduct (1992) - "**Assess computing and communication resources only when authorized to do so**."

CASE STUDIES

Case Study 1: Honeypots

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

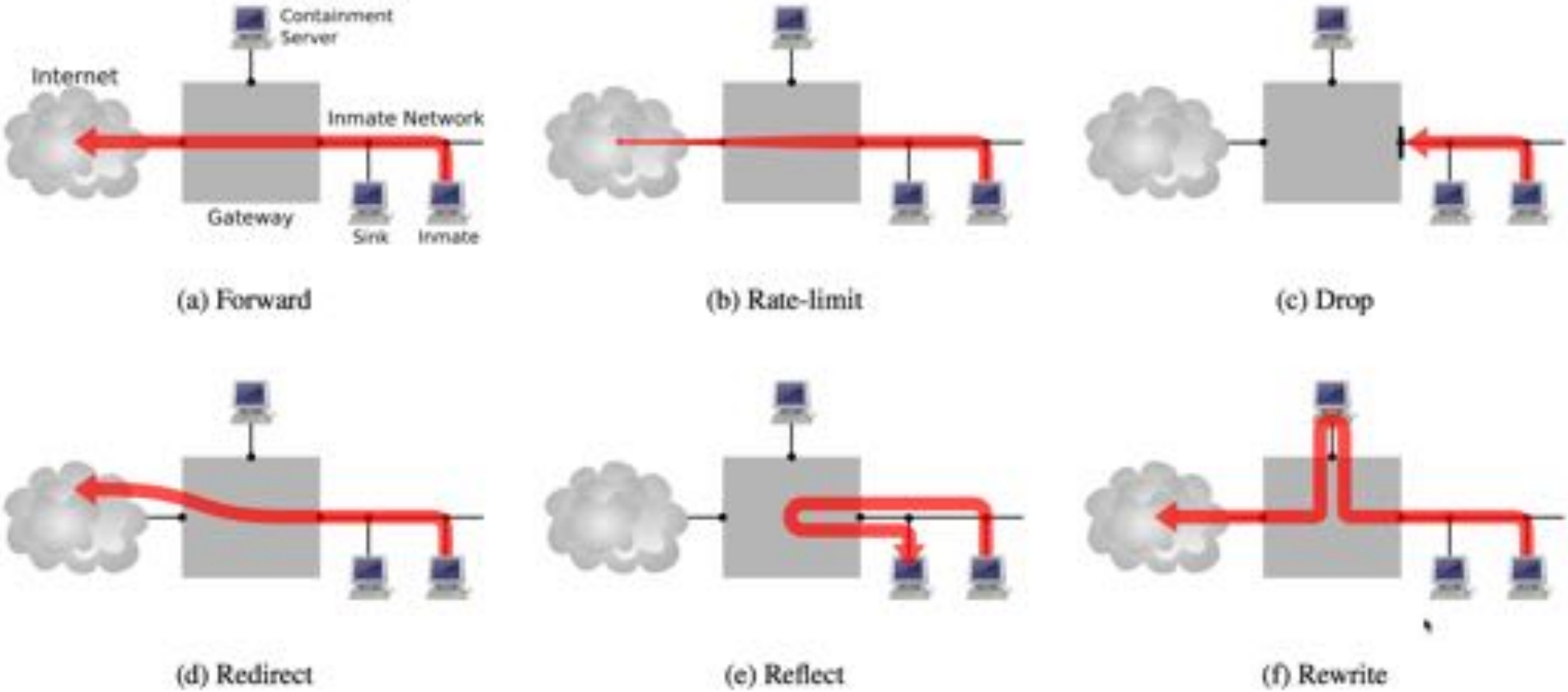
Case Study 1: Honeypots

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 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.

Honeypot Guidance

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



Case Study 2: Hack Back

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

WORM vs. WORM: Preliminary Study of an Active Counter-Attack Mechanism

Frank Castañeda[*†] castanef@us.ibm.com
Emre Can Sezer[†] ecsezer@ncsu.edu
Jun Xu[†] jxu3@ncsu.edu

[*] Pervasive Computing Division IBM Software Group
[†] Department of Computer Science North Carolina State University

ABSTRACT

Self-propagating computer worms have been terrorizing the Internet for the last several years. With the increasing density, inter-connectivity and bandwidth of the Internet combined with security measures that inadequately scale, worms will continue to plague the Internet community. Existing anti-virus and intrusion detection systems are clearly inadequate to defend against many recent fast-spreading worms. In this paper we explore an active counter-attack method - anti-worms. We propose a method that transforms a malicious worm into an anti-worm which disinfects its original. The method is evaluated using the CodeRed, Blaster and Slammer worms. We show through simulation the effectiveness of an anti-worm with several propagation schemes and its impact on the overall network. We also discuss important limitations of the proposed method.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*invasive software (e.g., viruses, worms, Trojan horses)*; C.2.0 [**Computer-Communication Networks**]: Security and Protection—*worms*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*invasive software (e.g., viruses, worms, Trojan horses)*

General Terms

Experimentation, Security

Keywords

Anti-worm, Good worm, Worm

1. INTRODUCTION

We consider computer worms that do not require human activation. Such a worm infects a server by exploiting a vulnerable application, usually through a specially crafted TCP or UDP message. It then continues to infect other servers with the same vulnerability. The questions we explore in this paper are: how to deploy an active immunization mechanism and how effective is it?

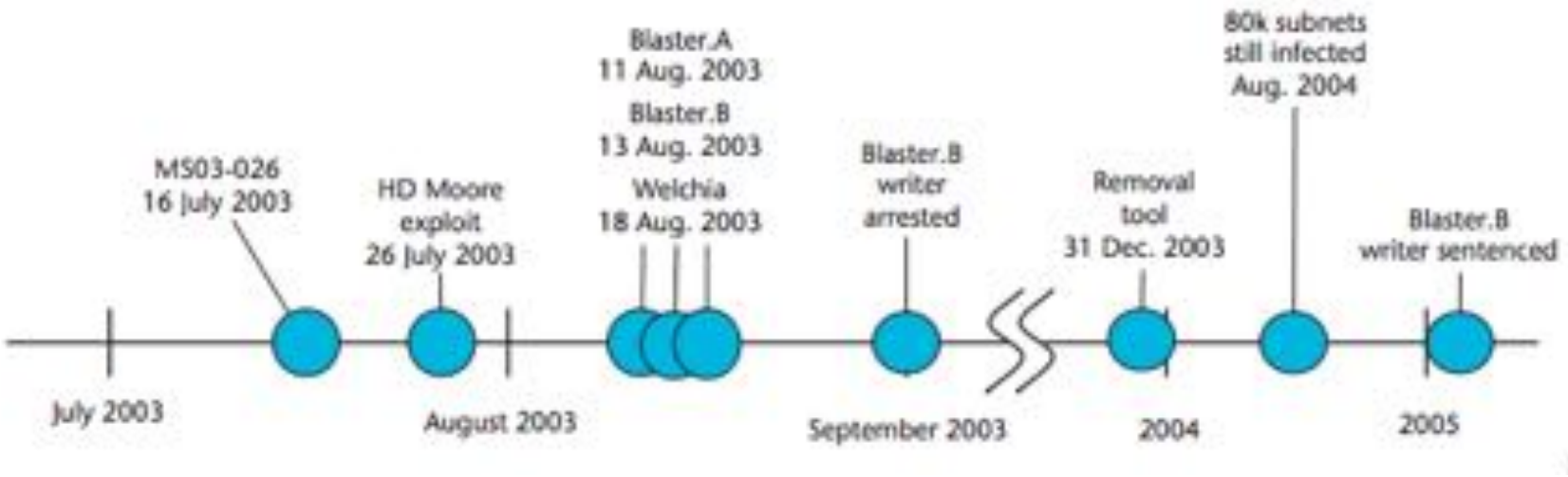
Current defense mechanisms such as anti-virus (AV) software and Intrusion Detection Systems (IDS) passively analyze file system activities or network traffic. Both systems use pre-defined attack signatures provided by AV/IDS vendors for detection. Vendors use network traffic monitors and analysis tools to discover new attacks and update their signature database. Users then need to download the signatures once they are updated. There may be significant delays at both the vendor and end-user signature updates before new attacks will be recognized. Stanford et. al. [28] predicts that, with better scanning algorithms, it is possible for worms to infect 90 percent of the susceptible hosts in mere minutes. Recent fast spreading worms (e.g., Slammer, Blaster) have proven this, and these worms clearly defeat current defenses. Anomaly detection systems use statistical methods to detect attacks but have not been very successful due to high false positive rates [1, 7].

Another defense is to ensure that each system is up-to-date with latest vendor patches. Many system administrators are reluctant to apply patches until they have been thoroughly tested in their environment. Combined with the magnitude of patches being released, an organization can be easily overwhelmed with patch testing and software updating. Small businesses and end consumers simply cannot keep up with the pace. It has been observed that most worms are actually created after the exploited vulnerability has been published on the Internet [6]. Our study of the Symantec worm and virus database [31] also shows that many recent worms are discovered weeks after Microsoft had released the patches. This clearly shows that manually applied patches are not effective in countering worms because they require human reactions and they are usually slow and do not scale well. Automatic patching at the software vendor level has also been considered, but end users basically do not feel comfortable with software vendors pushing new code to their systems. Not only does the consumer lack the ability to test the code, but there now exists a new security problem: how much do you trust your vendor [5, 6].

Due to the inadequacies in current defense mechanisms, it is imperative that better defenses be developed to detect a worm and to immunize hosts before the worm reaches epidemic proportions. Weaver et. al. [34] have also pointed out the need for better defense mechanisms and the possible research areas in this field. In this paper we explore an active immunization method by the use of a *good worm* or *anti-*

WORM'04, October 29, 2004, Washington, DC, USA.

Welchia, or Nachi as it's sometimes called, was an antiworm that attempted to patch the vulnerability and ended up causing significant damage of its own



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 3: Reverse Engineering, Vulnerability Disclosure?

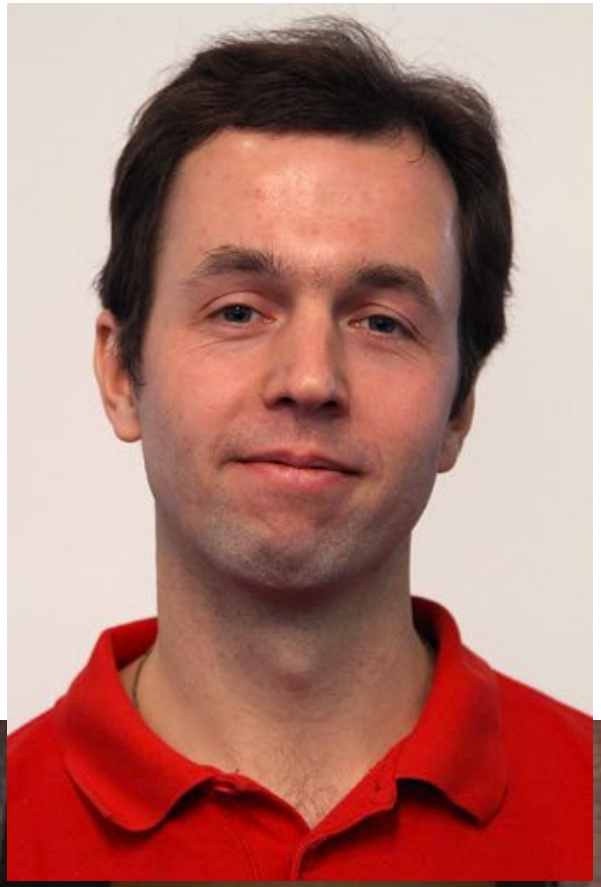
Researchers reverse engineer a system, discover a vulnerability, and generate a working exploit (attack).

Bloomberg Technology

Markets Tech Pursuits Politics Opinion Businessweek

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

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:

...efendant Elcom Ltd., a/k/a Elcomsoft Co. Ltd. ("Elcomsoft"), was a ...ssian company based in Moscow, Russia.

...dobe Systems, Inc., ("Adobe") was a software company headquartered in ...an Jose, California that developed publishing software for various media including the world wide

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

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

TECHNOLOGY NEWS | Wed Sep 7, 2016 | 7:11pm EDT

St. Jude sues short-seller over heart device allegations

Vulnerability Disclosure

- Nondisclosure – keep vulnerability secret
- Full Disclosure – distribute knowledge of the vulnerability, so potential victims can protect themselves
- Limited Disclosure – privately disclose to the vendor only, so they can develop a patch

Responsible Disclosure

- Disclose vulnerability to vendor in private
- Agree on a deadline for full disclosure
- Both parties maintain communication during patch development

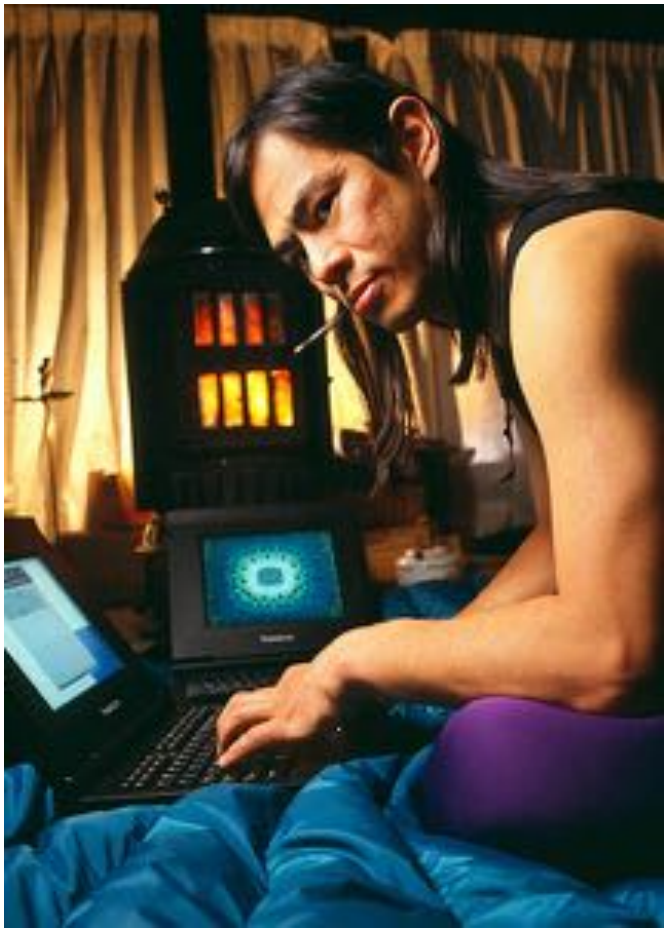
Responsible Disclosure

1. **Latent Flaw**. A flaw is introduced into a product during its design, specification, development, installation, or default configuration.
2. **Discovery**. One or more individuals or organizations discover the flaw through casual evaluation, by accident, or as a result of focused analysis and testing.
3. **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").
4. **Validation**. The vendor or other parties verify and validate the reporter's claims ("Reproduction").
5. **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").
6. **Release**. The vendor, coordinator, and/or reporter release the information about the vulnerability, along with its resolution.
7. **Follow-up**. The vendor, customer, coordinator, reporter, or security community may conduct additional analysis of the vulnerability or the quality of its resolution.

Ethical Hacker

- Hacking systems with:

1. *permission*
2. *expertise*
3. *document vulnerabilities*



Moving forward

- In this class you will not be asked to do anything that is illegal, unethical, or against university policy…
- so maybe…

Moving forward

- Ask **permission** not forgiveness.
- Use principle of least surprise.
- Be an ethical hacker.

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