Responsible Disclosure

Ethan Heilman
Boston University
February 2014

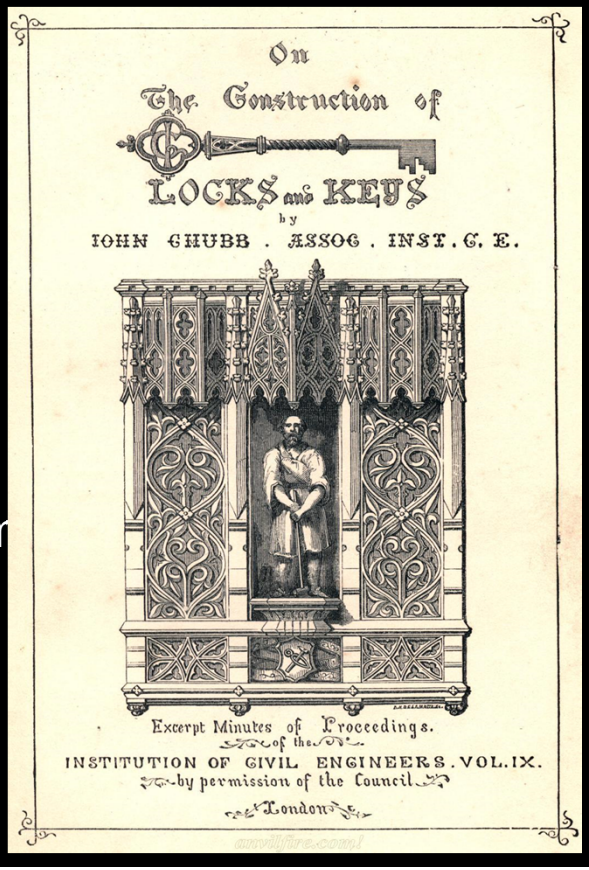
History

1. 18th C. -Vulnerabilities in locks and safes
2. 1990’s -No one fixes vulnerabilities
3. Later - Full Disclosure: Wysopal/L0pht
4. 2004 - Responsible Disclosure: Wysopal/OIS
5. Present - Age of Bug Bounties

18th C. -Vulnerabilities in locks and safes

"Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery."

- A. C. Hobbs, Boston, Ma, 1853


On
The Construction of
LOCKS and KEYS
by
JOHN CHUBB . ASSOC . INST. C. E.
Excerpt Minutes of Proceedings.
of the
INSTITUTION OF CIVIL ENGINEERS. VOL. IX.
by permission of the Council
London

18th C. -Vulnerabilities in locks and safes

- Non-disclosure is the belief that the public should not be told of vulnerabilities.
- Non-Disclosure became standard practice in the locksmithing world to this day, but it is changing.

1990’s No One Fixes Vulnerabilities

“Before full disclosure was the norm, researchers would discover vulnerabilities in software and send details to the software companies -- who would ignore them, [..]

Later on, researchers announced that particular vulnerabilities existed, but did not publish details. Software companies would then call the vulnerabilities "theoretical" and deny that they actually existed.

Then, of course, some hacker would create an exploit using the vulnerability -- and the company would release a really quick patch, apologize profusely, and then go on to explain that the whole thing was entirely the fault of the evil, vile hackers” Bruce Schneier

Full Disclosure Is Born

Publishing vulnerabilities immediately to the public without restriction.

- “Vendors have no economic incentive otherwise.”
- Shortens time to patch gives attacks less time

2004 Responsible Disclosure

- “Guidelines for Security Vulnerability Reporting and Response” 2004
- Full Disclosure with a mitigation period.
- Tell the vendor before the public, let them issue a mitigation before releasing. If they fail to release a patch within a responsable time then publicly disclose the vulnerability to protect the public (but talk to a lawyer first).

Present - Age of Bug Bounties

- Many Companies care about security, encourage researchers to find vulnerabilities as long as the company gets a responsible time period to fix the issue (6 months for Google).
- Companies publish responsible disclosure Policies.
- Some will even pay you a bounty if find a vulnerability.
- Some companies will still sue researchers vulnerability discovery (read their policies carefully).

MBTA vs. Anderson

- Students found flaw in the MBTA's Charlie Card.
- Informed MTBA 10 day before they were to publish the vulnerability.
- MBTA sued the students and won a gag-order, they were questioned by the FBI.
- MBTA eventually lost in court.

Teen Reported to Police After Finding Security Hole in Website

- Joshua Rogers 16-year-old found a security vuln in the Transportation Depts website.
- He contacted Transportation Dept but got no response.
- Then he contacted the media to report the issue.
- The Transportation Dept responded by contacting the police.

What is Responsible Disclosure?

- Working with the vendor to fix the issue before going public?
- Going public if the vendor refuses to fix the issue?
- Under debate. Different companies have different standards.
- Consult with Professor Goldberg prior to anyone else if you find a vulnerability.

IMPORTANT!!!

- To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy is that you must respect the privacy and property rights of others at all times, or else **you will fail the course**.

  Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern ``hacking." Understand what this law prohibits.

IMPORTANT!!!

- Read BU's Conditions of Use and Policy on Computing Ethics and the BU's Academic Conduct Code. As members of the university, you are required to abide by these policies.

- Consult with Professor Goldberg prior to anyone else if you find a vulnerability while enrolled in this course.