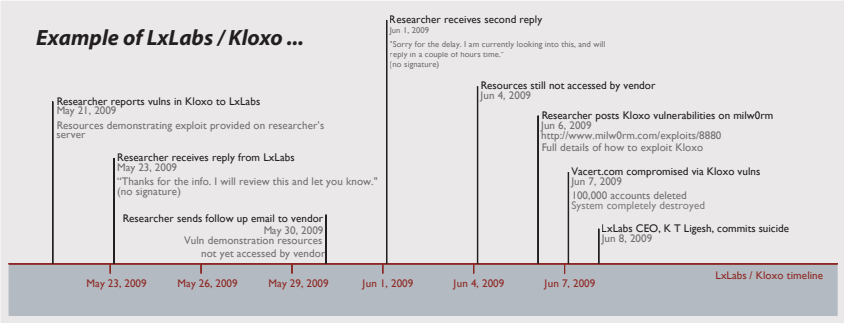
Have We Crossed the Line? The Growing Ethical Debate in Modern Computer Security Research

Authors:
David Dittrich - University of Washington
Michael Bailey - University of Michigan
Sven Dietrich - Stevens Institute of Technology

Researchers and Professionals want to benefit the Internet community

But oh, the temptations! We want to be the first to publish, show how 31337 we are, compete for funding.

The risks are high!



This is where ethics come in.

Guiding principles which help to govern conduct among groups.

Existing ethical standards:

Professional Codes of Ethics: IEEE, ACM, etc.
The Belmont Report: the National Research Act and Institutional Review Boards (IRB)
"Rules of Engagement": The Law of Armed Conflict, Active Response Continuum

When we know about them and use them, these standards can help us to:

understand the stakeholders

Entity	Activity	Type	Risk/Benefit
Researcher	Discovered vulnerabilities	Key	Reputation, altruism
Programmers	Write and maintain software	Key	Jobs
Vendor	Control programmers' activities	Key	Reputation, lost revenue
Svc. Providers	Customers of vendor; provide service to clients	Secondary	Lost revenue
Clients	Create/run virtual storefronts	Primary	Lost revenue
Customers	Buy from online stores	Primary	DoS, fraud
Criminals and attackers	Exploit services	Key	Booty, LOLZ, Arrest

understand the alternatives

1. Take high-level description of vulns to media, getting word to primary/secondary stakeholders (who can then protect themselves)

2. Report to trusted organization (e.g., CERT/CC) to get their assistance in pressuring vendor to fix bugs

3. Identify influential primary/secondary stakeholders and engage them to put pressure on vendor (e.g., stop purchasing system, file law suits) and protect themselves

4. Publish only general vulnerability information to put pressure on vendor, then wait an appropriate amount of time before fully disclosing exploit details if vendor still unresponsive

However existing ethical codes are either not suited to addressing all the issues of cyber security research, or we don't apply them appropriately in all cases.

Tomorrow's sophisticated threats will be highly resilient and sophisticated and will continue to challenge researchers to find new and potentially more risky methods to detect, characterize, and mitigate them.

We must find ways to balance societal needs and ethical issues surrounding our research, lest we drift to the extremes---becoming the very thing we deplore, or ceding the Internet to the miscreants because we fear to act.

For additional case studies and an in-depth exploration of these issues, please see:

David Dittrich, Michael D. Bailey, and Sven Dietrich. Towards community standards for ethical behavior in computer security research. Technical Report 2009-01, Stevens Institute of Technology, Hoboken, NJ, USA, April 2009. Available as http://www.cs.stevens.edu/~spock/pubs/dbd2009tr1.pdf

16th ACM Conference on Computer and Communications Security
November 9-13, 2009, Chicago, IL, USA