Bridging the Distance

Removing the Technology Buffer and Seeking Consistent Ethical Analysis in Computer Security Research

Katherine Carpenter
University of Denver
Sturm College of Law/Joseph Korbel School of International Studies

David Dittrich
University of Washington
Applied Physics Laboratory

CS and CompSec Research

- Research on algorithms (scalability, performance, theory of computation)
- Network traffic analysis
- Botnet takedown
- Vulnerability research
  - Software and Operating Systems
  - Embedded medical devices (insulin injection, pace makers)
  - Process Control Systems (Automobile braking systems, water/sewage controls, hydroelectric generation)

"When engaged in what Markham calls 'world-fixing,' one needs to '[derive their methods] through constant, critical reflection on the goals of research and the research questions,' understanding not only the problems to be solved, but the potential effects on all parties involved."

David Dittrich, Felix Leder, and Tillmann Werner. A case study in ethical decision making regarding remote mitigation of botnets. In Proceedings of the 14th international conference on Financial Cryptograpy and Data Security, FC'10, pp. 216–230, 2010. Springer-Verlag.

A. Markham. Method as ethic, ethic as method. Journal of Information Ethics, 15(2):37–55, 2006.

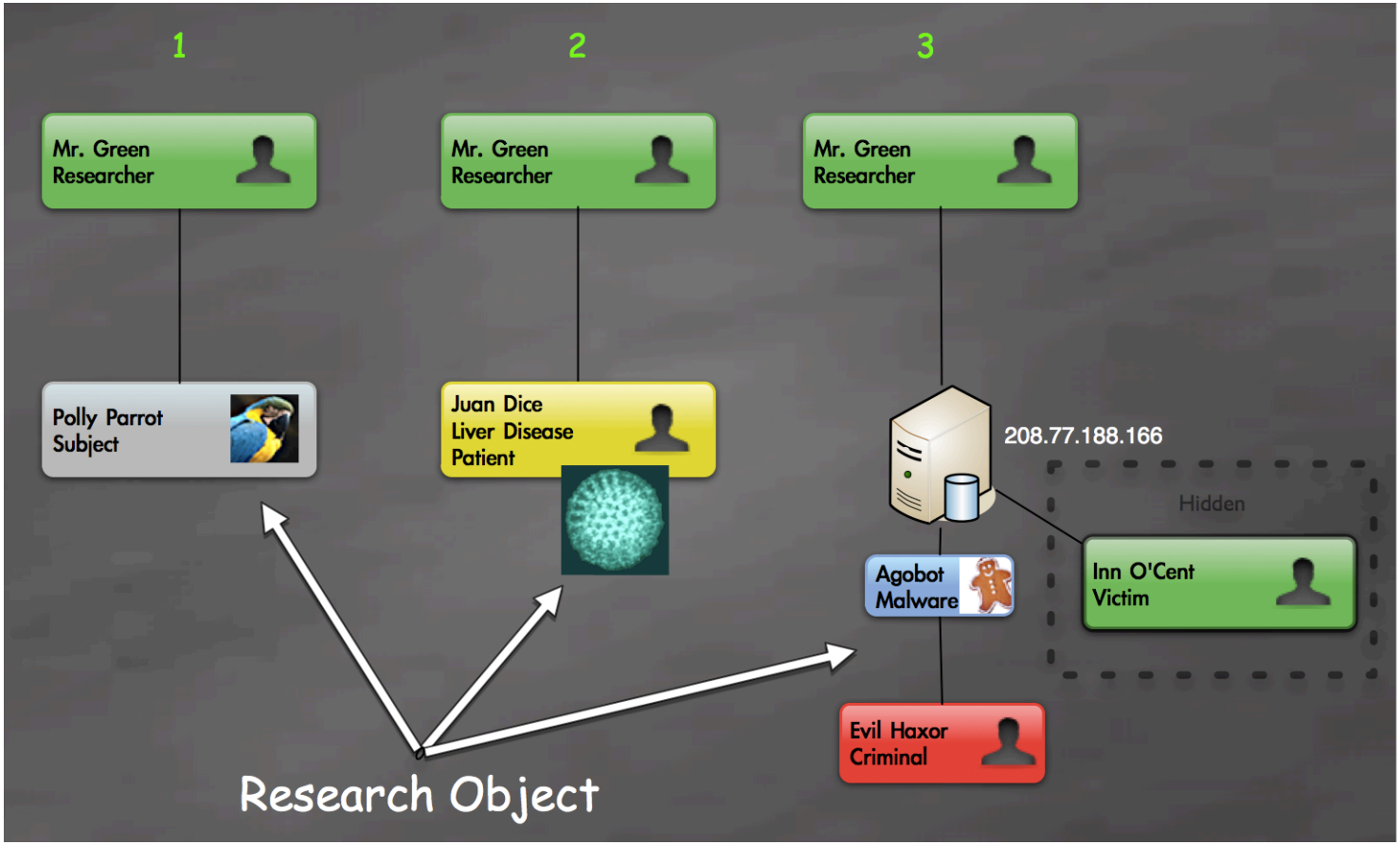
Human Subject vs. Human Harming

- 45 CFR 46.102(f)
  - "Human subject means a *living individual*"
  - "obtain[] (1) data through *intervention* or *interaction* with the individual, or (2) *identifiable private information*"
    - "Intervention includes both *physical procedures by which data are gathered* [] and *manipulations of the subject or the subject's environment* that are performed for research purposes"
    - "Private information includes information about behavior that occurs in a context in which an individual can *reasonably expect that no observation or recording is taking place*, and information which has been provided for specific purposes by an individual and which the individual can *reasonably expect will not be made public*"

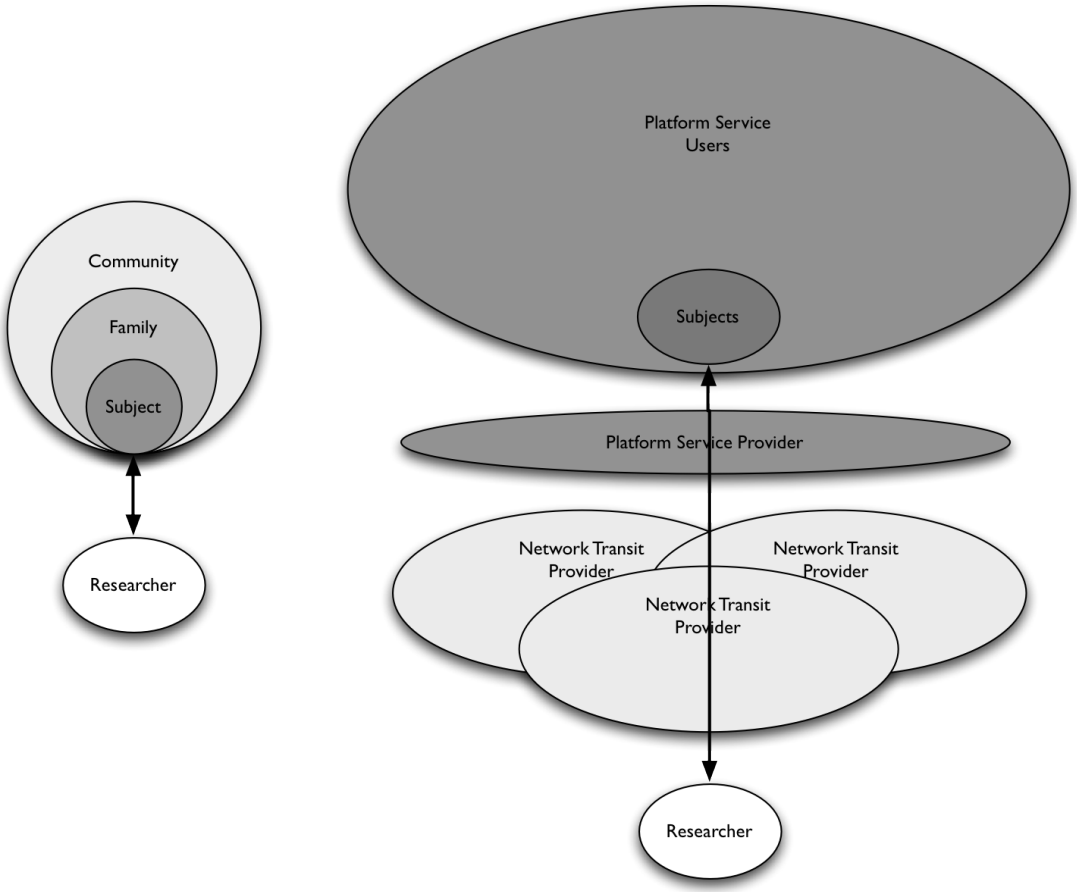
IRB Challenges

- Definitions in the Common Rule dictate exclusion vs. review, not whether humans could be harmed by researcher activities or not
- Workload is high
- New research is coming under IRB scrutiny
- IRBs have available lots of biomedical expertise, but almost no computer science expertise
- Computer Science researchers have little/no expertise with IRBs and ethical review

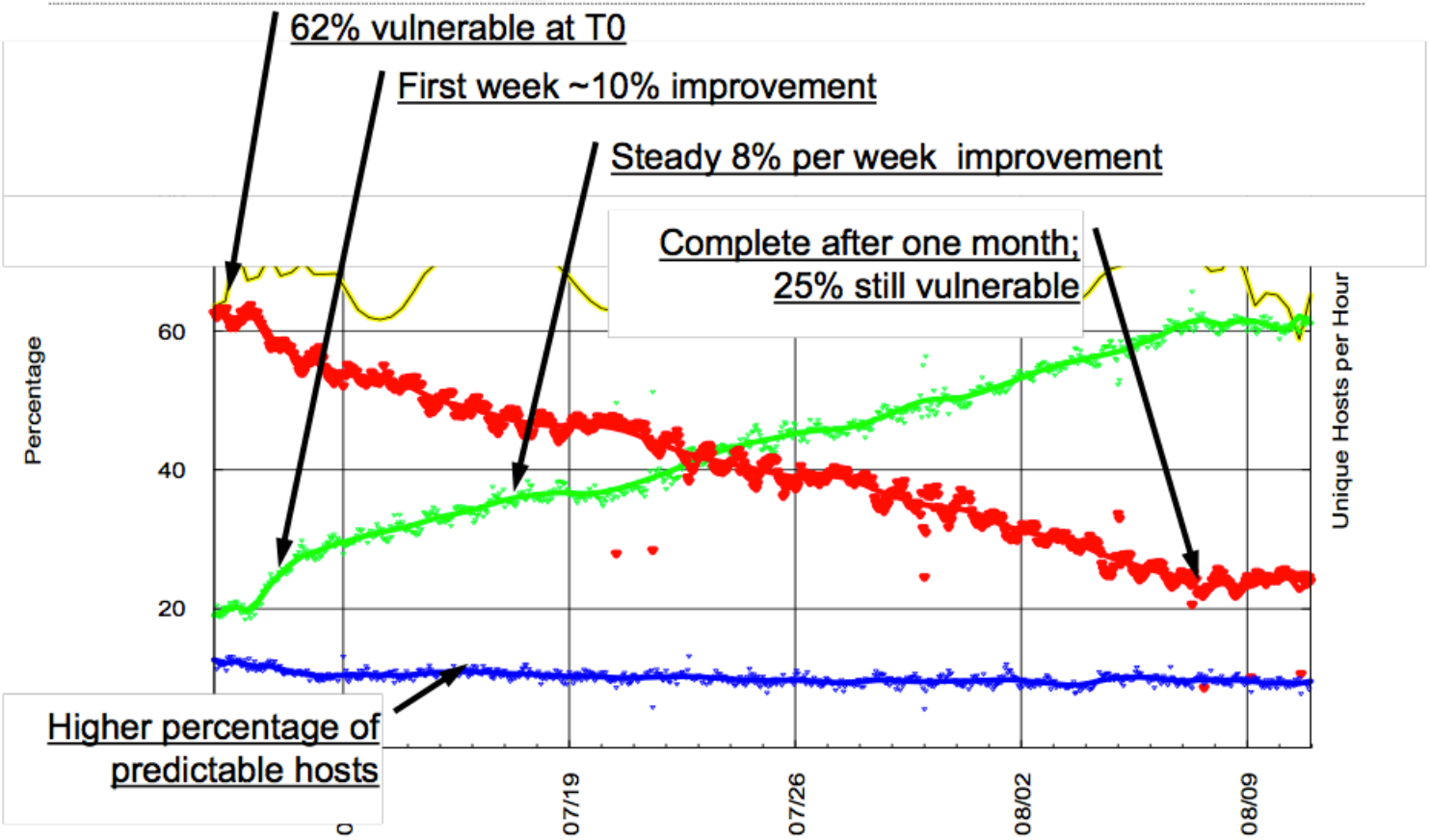
Subject or Object?



Logical Distance



Temporal Distance



Source: Responsible Disclosure: A Case Study of CERT VU#800133, “DNS Cache Poisoning Issue” Sid Faber, 2008 OARC Workshop, September 24, 2008

Identifying Stakeholders

Stakeholder Type	Positively Inclined	Negatively Inclined
Key [*Affect on producing outcome*]	Researchers Programmers Operations Staff Executives Law Enforcement	Criminals (Individuals/Gangs) Malware Programmers Botmasters Criminal Masterminds
Primary [*End users*]	Consumers (product/service) Enterprises (.edu, .com, .org) Manufacturers Government entities	Espionage Consumers Criminal Enterprises
Secondary [*Intermediaries in delivery*]	Service Providers Platform Providers Transit Providers Retailers	"Bullet Proof" Hosting Providers Malware Delivery Providers Malware Obfuscators Sellers of fake goods

In Summary

- Bridge the gap between IRB understanding of technology protocol risk to humans and researchers' ability to develop ethically defensible research protocols that appropriately balance risks and benefits
- Shift our focus from *informed consent* to *potential harm to humans*
  - It is impossible to identify and obtain consent from all involved humans
  - The humans may not be the *direct subjects* of research
  - Potentially harmed humans may not be directly interacting with researchers

Thanks and Questions

- Contacts:

Katherine Carpenter
University of Denver
kcarpenter13 [at] law.du.edu

David Dittrich
University of Washington
dittrich [at] uw.edu
http://staff.washington.edu/dittrich

- Thanks to: Michael Bailey, Erin Kenneally, the Menlo Working Group, Doug Maughan, Elizabeth Buchanan, Laura Odwazny, and Halle Showalter Salas

Supported by the Department of Homeland Security