EXPERT STATEMENT: Support for Security Research

April 10, 2018

Computer and network security research, white-hat hacking, and vulnerability disclosure are legal, legitimate, and needed now more than ever to understand flaws in the information systems that increasingly pervade our lives. Ethical and law-abiding information security research and evaluation are an essential part of defending against an ever-changing landscape of security threats.

In general, research in information systems is based upon *analysis* — the careful examination of existing systems and approaches in order to understand what works and what does not. This kind of examination leads to improvements that are both evolutionary and revolutionary. Researchers discover flaws. They invent new and improved ways to detect and correct flaws and approaches to system design and implementation. This investigative process has driven the computer systems field forward at an extraordinary pace for more than half a century.

The ability of researchers to find and responsibly report vulnerabilities is more important today now that traditionally unconnected devices are being connected to the Internet and more of people's lives are mediated by data, computation, and networking. Compromised systems and devices have been used to launch attacks all over the world. Vulnerability research, discovery, and disclosure are critical features of the modern digital society; the US National Institute of Standards and Technology has recognized in its Cybersecurity Framework that vulnerability disclosure is an important aspect of any effective cybersecurity program.

Security researchers who search for vulnerabilities often find themselves in areas where laws or regulations forbid or hinder tinkering with devices and software. They are at particular risk where copyright is involved or where they publicly report their discoveries.

In the US, security researchers and reporters have recently been targeted by unwarranted and opportunistic legal threats and lawsuits.

The most recent cases include *Keeper v. Goodin*[1] and *River City Media v. Kromtech*[2]; in the first case, a reporter was sued for reporting on the details of a vulnerability, and in the second case a security researcher is being sued for investigating a publicly accessible spam server. These lawsuits not only endanger a free and open press but risk a "chilling effect" towards research designed to improve cybersecurity. Security researchers hesitate to report vulnerabilities and weaknesses to companies for fear of facing legal retribution; these chilling effects invite the release of anonymous, public zero-day research instead of coordinated disclosure.

We urge support for security researchers and reporters in their work, and decry those who oppose research and discussion of privacy and security risks. Harming these efforts harms us all.

Signed,

(Affiliations are for identification purposes only.)

[1] https://www.courtlistener.com/docket/6244750/keeper-security-incv-goodin/

[2] https://www.courtlistener.com/docket/4685667/river-city-media-llc-v-kromtech-alliance-corporation/

Adam Shostack
Ashkan Soltani
Ben Adida, Clever
Boing Boing/Happy Mutants, LLC
Bruce Schneier, Harvard Kennedy School
Bryan Ford, EPFL
Catalin Cimpanu
Cory Doctorow, author and activist
Daniel M. Zimmerman, Galois
Daniel Weitzner, MIT Internet Policy Research Initiative
David Evans, University of Virginia
David J. Farber, University of Pennsylvania/Carnegie Mellon University
David Jefferson, Lawrence Livermore National Laboratory (retired)
Dell Cameron, Gizmodo
Eric Mill
Graham Cluley
Grugq, Director of Threat Intelligence, Comae
J. Alex Halderman, University of Michigan
Jake Laperruque, Project on Government Oversight
Joe Kiniry, Chief Scientist, Galois
Johnny Xmas, security researcher
Joseph Lorenzo Hall, Center for Democracy & Technology
Kenneth White, Open Crypto Audit Project
Kevin Beaumont
Khalil Sehnaoui, Krypton Security
L Jean Camp, Indiana University
Lorenzo Franceschi-Bicchierai
Marcia Hofmann, Zeitgeist Law
Mark Buell, Internet Society
Matt Blaze, University of Pennsylvania
Matthew D. Green, Johns Hopkins University
Micah Lee, The Intercept
Micah Sherr, Georgetown University
Mike Masnick, Techdirt
Nadia Heninger, University of Pennsylvania
Nick Sullivan, Cloudflare
Peter Eckersley, Electronic Frontier Foundation
Philip B. Stark, University of California, Berkeley
Philip Zimmermann, Technical University of Delft
Rebecca Wright, Rutgers University
Ronald L. Rivest, MIT
Ross Anderson, University of Cambridge
Ross Schulman, New America's Open Technology Institute
Sascha Meinrath, X-Lab
Scott O. Bradner, Harvard University (retired)
Scott Helme, Report URI
Selena Deckelmann, Firefox
Stephen Checkoway, University of Illinois at Chicago
Stephen Farrell, Trinity College Dublin
Steve Bellovin, Columbia University
Susan Landau, Tufts University
Trevor Timm, Freedom of the Press Foundation
Troy Hunt, Have I Been Pwned
Wendy Knox Everette
Wendy Seltzer, W3C
Will Strafach, Sudo Security Group
Yael Grauer
Zack Whittaker