OUTLINE OF RESEARCH ACCOMPLISHMENTS
JEDIDIAH R. CRANDALL — SPRING 2014

> My User has information that could... that could make this a free system again! No, really! You'd have programs lined up just to use this place, and no Master Control Program looking over your shoulder. —*Tron*.

The principle that guides my research is that it shouldn't be so easy for those who control the Internet to practice censorship and surveillance without full transparency. Towards this end, my research group designs and builds *illuminating instruments* that can be used to learn, through measurement and analysis, more about the Internet and the software that people use to connect to it. Just as telescopes help astronomers learn more about the cosmos and particle colliders help physicists to understand more about the workings of the universe, the tools we build in my research group help technologists, policy makers, journalists, activists, and the public in general understand more about how Internet censorship and surveillance are implemented.

"Information wants to be free" is more than a slogan, it says something about the fundamental nature of information. One thing is for sure after 40 years of computer and network security and privacy research: *keeping secrets is really hard.* My research seeks to turn this on its head and reveal the secrets of those who control the Internet.

1 Shedding light on the dark corners of the Internet

The state of the art in Internet measurement is that, if you want to know what's going on in Region X, where Region X could be a country, continent, or individual Internet Service Provider, you have to install servers (such as PlanetLab nodes, M-Lab nodes, or RIPE Atlas nodes) in Region X. **This is not good enough for measuring the things I want to know.** Regions such as South America, Africa, the Middle East, Eastern Europe, and Asia have little or no coverage by these aforementioned measurement platforms. **My research challenges a basic assumption: that in order to know what's happening on the Internet between hosts A and B you have to have access to log into A or B to run commands and perform measurements.** My research group's work in this vein includes:

- **Work on modeling network stacks [5],** which provided a theoretical underpinning for network side channels. Our SYN backlog side channel has many applications for penetration testing, and is mentioned in the book *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide* by Lee Allen. We recently used a refined version of this side channel to locate thousands of machines with routable IPv4 addresses on the Internet that were hidden behind firewalls [13].
- **A novel technique for measuring censorship between virtually any two arbitrary machines on the Internet [3, 4].** This work has generated a lot of excitement in the research community, and we are collaborating with the International Computer Science Institute (ICSI) Networking and Security Group, the Tor Project, the Citizen Lab, and others to measure Internet censorship on a global scale. We used this technique to perform a wide-scale study of how the world's largest firewall blocks the Tor network [6].
- **Several other side channel techniques,** including work to measure the Maximum Transmission Unit (MTU) between two arbitrary machines or routers anywhere on the Internet [8], work to measure the round-trip time between any two machines on the Internet [1], and an independent way to measure censorship in the routing layer that compliments the hybrid idle scan.

2 Protecting users by reverse engineering everything from program binaries to social media

Another aspect to my research is to protect users by making them aware of threats in the systems and networks that they use. The threats may be vulnerabilities, or it may be censorship and surveillance that is "baked into" software in secret, and the systems can be anything from operating systems to third-party programs to social media platforms. Threats we have helped to shed light on include:

- **Third party applications that would make it trivial for a state actor who controlled the network to backdoor a user's machine when they connect to the network [9].** This included a zero-day vulnerability that we found in Java, which is installed on virtually every device that connects to the Internet. We are currently developing a novel reverse-engineering tool based on dynamic information flow tracking to automate the process of finding this kind of vulnerability. A reverse engineer can simply invoke our tool as a plugin for IDA Pro and the tool will tell them where cryptographic keys are hidden in memory, automatically, based on information flow.
- **Censorship on Weibo, which is the Chinese equivalent of Twitter, where we found that posts were deleted in a matter of minutes, not hours or days [14].** Our work, which was a collaboration with Rice University and independent researchers, received a good amount of media coverage, in such outlets as the BBC and The Global Times, and helped corroborate, and give context to, a Reuters report that paints a fairly detailed picture of how Weibo censorship works [7].
- **Censorship and surveillance built into the Chinese version of Skype known as TOM-Skype [11].** We tracked daily changes to the censorship and surveillance blacklists for a year and a half and collaborated with the Citizen Lab at the University of Toronto to give political, legal, and social context to the data [2]. My graduate student was profiled in an article for Businessweek [12]. You can see interesting visualizations of the data at `https://china-chats.net`. This work led to a whole line of research on chat programs in Asia (see `https://citizenlab.org/tag/asia-chats/`), that will form the basis for a longitudinal study that we are collaborating with the Citizen Lab on now.
- **A security issue in the Linux kernel that gave anyone who can spoof packets on the Internet the ability to count the packets sent between two arbitrary machines anywhere on the Internet.** We accomplished this attack using TCP/IP side channels [10]. A patch to the Linux kernel was issued, but we are now investigating a separate side channel.

Currently, we have a nearly $3 million DARPA proposal pending (PI is Prof. Faloutsos, the UNM share would be about half, in collaboration with the Univ. of Florida and the Univ. of Cincinnati) that could revolutionize the way that people approach cybersecurity. A long-time dream of cybersecurity researchers and practitioners has been to tag a piece of data and have the tag be accurately tracked so that we know where the information flows to. We have proposed an approach that may finally solve the problem of tracking the many subtle ways that information can flow. This has broad applications, including preventing attacks, forensics, privacy analysis, and reverse engineering.

We also have a nearly $3 million dollar NSF proposal (my co-PIs are Prof. Faloutsos and Prof. Forrest) pending that would build an Internet connection at the UNM Center for Advanced Research Computing (CARC) to measure the whole Internet. Using side channels, we can not only illuminate the dark corners of the Internet, but also supplement the entire map with information policy makers and circumvention tool developers need to know such as physical technologies, network virtualization layers, tunnels, physical points of presence, and IP aliasing.

References

[1] Geoffrey Alexander and Jedidiah R. Crandall. Off-path round trip time measurement via TCP/IP side channels. To appear in the Proceedings of IEEE INFOCOM 2015 (INFOCOM 2015).

[2] Jedidiah Crandall, Masashi Crete-Nishihata, Jeffrey Knockel, Sarah McKune, Adam Senft, Diana Tseng, and Greg Wiseman. Chat program censorship and surveillance in China: Tracking TOM-Skype and Sina UC. *First Monday*, 18(7), 2013.

[3] Roya Ensafi, Jeffrey Knockel, Geoffrey Alexander, and Jedidiah R. Crandall. Detecting intentional packet drops on the Internet via TCP/IP side channels. In the Proceedings of the 2014 Conference on Passive and Active Measurements (PAM 2014), Springer Lecture Notes in Computer Science.

[4] Roya Ensafi, Jeffrey Knockel, Geoffrey Alexander, and Jedidiah R. Crandall. Detecting intentional packet drops on the Internet via TCP/IP side channels: Extended version. *CoRR*, abs/1312.5739, 2013. Available at `http://arxiv.org/abs/1312.5739`.

[5] Roya Ensafi, Jong Chun Park, Deepak Kapur, and Jedidiah R. Crandall. Idle port scanning and non-interference analysis of network protocol stacks using model checking. In *Proceedings of the 19th USENIX Security Symposium*, USENIX Security'10. USENIX Association, 2010.

[6] Roya Ensafi, Philipp Winter, Abdullah Mueen, and Jedidiah R. Crandall. Analyzing the Great Firewall of China over space and time. To Appear at the 2015 Privacy Enhacing Technologies Symposium (PETS).

[7] Li Hui and Megha Rajagopalan. At Sina Weibo's censorship hub, China's Little Brothers cleanse online chatter. Reuters, 11 September 2013, Available at `http://www.reuters.com/article/2013/09/11/net-us-china-internet-idUSBRE98A18Z20130911`.

[8] Jeffrey Knockel and Jedidiah R. Crandall. Spooky action at a distance: Inferring the MTU bidirectionally between arbitrary pairs of IPv6 hosts anywhere on the Internet. Under submission.

[9] Jeffrey Knockel and Jedidiah R. Crandall. Protecting free and open communications on the Internet against man-in-the-middle attacks on third-party software: We're FOCI'd. In *FOCI 12: Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet*, 2012.

[10] Jeffrey Knockel and Jedidiah R. Crandall. Counting packets sent between arbitrary Internet hosts. In *FOCI 14: Proceedings of the 4th USENIX Workshop on Free and Open Communications on the Internet*, 2014.

[11] Jeffrey Knockel, Jedidiah R. Crandall, and Jared Saia. Three researchers, five conjectures: An empirical analysis of TOM-Skype censorship and surveillance. In *FOCI 11: Proceedings of the USENIX Workshop on Free and Open Communications on the Internet*, 2011.

[12] Vernon Silver. Cracking China's Skype surveillance software. Businessweek, 8 March 2013, Available at `http://www.businessweek.com/articles/2013-03-08/`

skypes-been-hijacked-in-china-and-microsoft-is-o-dot-k-dot-with-it.

[13] Xu Zhang, Jeffrey Knockel, and Jedidiah R. Crandall. Original SYN: Finding machines hidden behind firewalls. To appear in the Proceedings of IEEE INFOCOM 2015 (INFOCOM 2015).

[14] Tao Zhu, David Phipps, Adam Pridgen, Jedidiah R. Crandall, and Dan S. Wallach. The velocity of censorship: High-fidelity detection of microblog post deletions. In *USENIX Security Symposium*, Washington, DC, USA, 2013. USENIX Association. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_zhu.pdf.