COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

CSE Dissertation Defense

Zakir Durumeric

Fast Internet-Wide Scanning: A New Security Perspective

ABSTRACT: Historically, the vast majority of the devices connected to the public Internet remained out of sight to the research community. However, as the diversity of devices and the role they play in critical infrastructure has increased, understanding the dynamics of and securing these devices has become of paramount importance. Previous research techniques, including passive observation and random sampling, have attempted to shed light on the day-to-day operations of the Internet. However, these methodologies have primarily focused on the most popular services, and not on providing a more comprehensive view of the plethora of devices and services that now constitute the Internet. This dissertation argues that fast Internet-wide scanning helps provide this missing near-global perspective of the public Internet and enables researchers to uncover new security weaknesses that only emerge at scale.

First, I show that it is possible to efficiently scan the IPv4 address space by introducing ZMap, a network scanner specifically architected for large-scale research studies. ZMap is capable of surveying the entire IPv4 address space from a single machine in under an hour at 97% of the theoretical maximum speed for gigabit Ethernet and with an estimated 98% coverage of publicly available hosts. Building on ZMap, I introduce Censys, a public service that maintains an up-to-date snapshot of the hosts and services running across the public IPv4 address space, and show how Censys enables researchers to efficiently ask a range of security questions.

Next, I cover three case studies that highlight how Internet-wide scanning can (1) identify new classes of weaknesses that only emerge at scale, (2) uncover unexpected attacks and devise new defenses that resist them, and (3) shed light on previously opaque distributed systems on the Internet.

Finally, I explore how the increased contention over IPv4 addresses is introducing new challenges for performing large-scale empirical studies, and I suggest several research directions that the research community needs to consider to retain the type of visibility that Internet-wide scanning initially provided.

Chair: **Prof. J. Alex Halderman**

Tuesday, July 25, 2017 3:00 – 5:00 pm
GM Conference Room, 4th Floor, Lurie Engineering Center