Defense-in-Depth in Practice

Josephine Wolff, PhD Candidate

Start: September 2010
Research Group: Advanced Network Architecture Group
Thesis Advisor: Dr. D. Clark, Senior Research Scientist

Explorations in Cyber International Relations
Massachusetts Institute of Technology Harvard University

Workshop on
Complexity, Contention & Cooperation
MIT, January 6 and 7, 2014

Problem

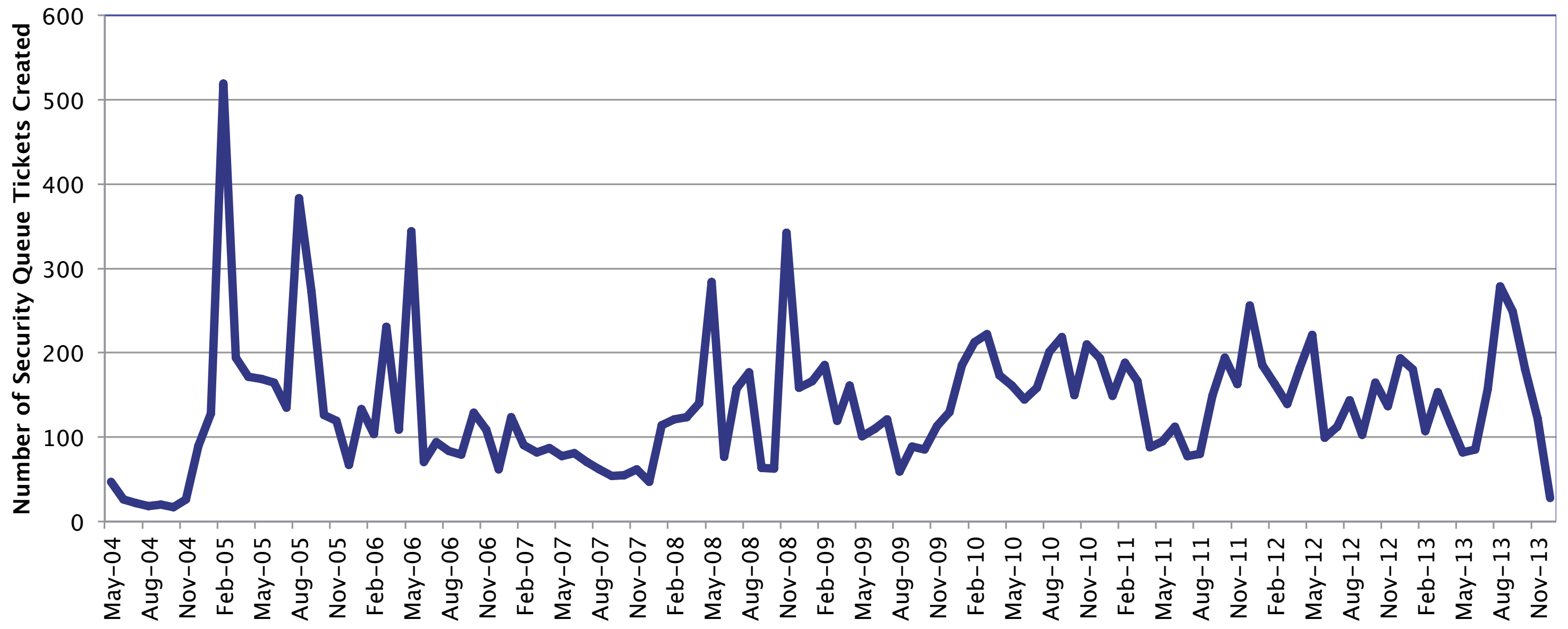
As network defense mechanisms—ranging from firewalls and antivirus programs to encryption packages and intrusion detection systems—have become more numerous and complex, it has become increasingly difficult to understand how they can most effectively be combined and layered together. This research looks at how—and to what end—combinations of these defenses are implemented in practice to protect the networking infrastructure and resources at MIT and aims to draw some more generalizable conclusions from that data about how organizations can design and implement effective defense-in-depth.

Key Questions

- **What types of threats do university campus networks face and how have those threats changed over time?**
- **How do universities make decisions about implementing new defensive measures and what categories of costs and benefits are considered?**
- **To what extent have different defenses—ranging from technical measures to policy changes—been effective at addressing these threats?**
- **How have different defenses complemented each other or reinforced holes in others?**

Data

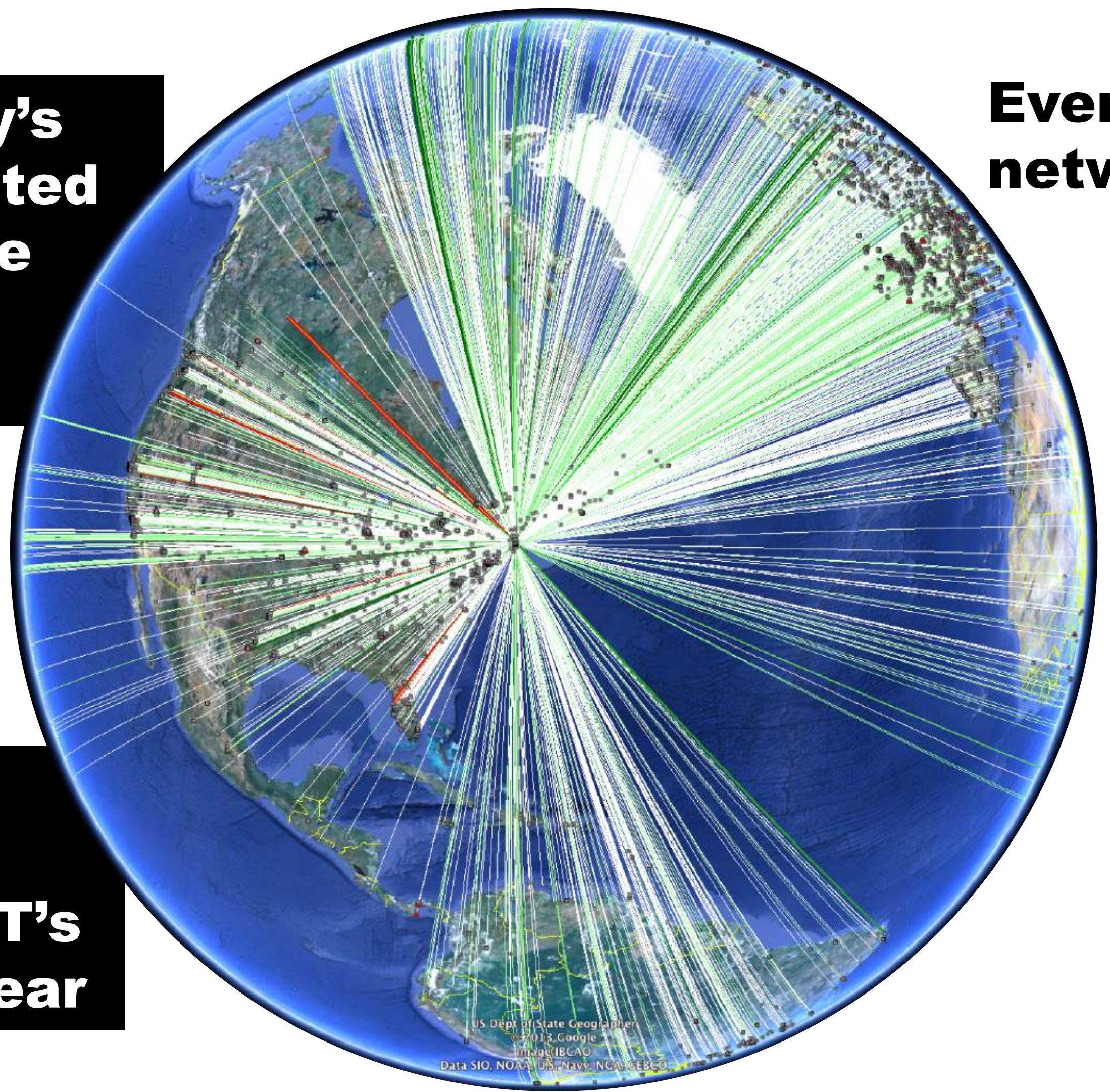
- **MIT Information Services & Technology (IS&T) security queue of more than 15,000 incidents**



Preliminary Results

Network Security at MIT

A map of one day's worth of unsolicited probes of a single host on MIT's network:



Graphic courtesy of MIT IS&T.

There are about 120,000 devices connected to MIT's network every year

Every day MIT's network sees roughly:

- **35,000 probes per host**
- **60 new hosts infected by malware**
- **2 million password crack attempts**
- **12 security contacts**
- **20 DMCA takedown notices**

Defenses

	Description	Implemented	Purpose
Restricted access to DNS servers	Recursive access to MIT DNS servers restricted to clients on MIT's network	Spring 2013	Makes MIT's DNS servers less vulnerable to being used for amplification attacks
Added resiliency for website & external DNS	Akamai contracted to provide access to mit.edu from off-campus	Spring 2013	Makes MIT's homepage less vulnerable to DDoS attacks
VPN required for off-campus access to admin. systems	MIT administrative applications (SAP, Data Warehouse, MITSIS) will require connecting from MIT's network, either from on-campus or via MIT's VPN	Spring 2013	Makes it more difficult for intruders to access sensitive information stored in MIT's administrative systems
Password policy	Kerberos passwords must be changed yearly and meet stricter complexity requirements	July 2013	Makes it harder for attackers to compromise MIT accounts via brute force attacks; also allows for updating encryption
Firewall	By default, incoming traffic originating from outside MIT's network destined for clients on IS&T-operated networks will be blocked	Rolling (2014)	Makes it more difficult for intruders to scan hosts on MIT's network; reduces "noise" in incoming traffic enabling (potentially) better detection
Secure wireless network	Required use of the MIT SECURE wireless network which uses the WPA2 protocol (and requires authentication)	The non-secure wireless network will be retired in 2014	Makes it more difficult for non-MIT affiliates to use the wireless network and easier to link activity to individual users

Ongoing Work

The impact of these new defenses is a central focus of this research. It aims to answer questions such as:

- **Does MIT's new password policy reduce the number of compromised accounts reported?**
- **Does its firewall diminish malware infection rates?**
- **Do network monitoring tools enable earlier detection of security breaches, or detection of new types of threats?**
- **What, if any, unintended consequences for non-malicious users arise from these new defenses?**
- **What, if any, emergent defensive properties arise from the combination of these protections?**

Existing research on the effectiveness of defenses tends to focus on the impact of specific tools and products, rather than trying to assess the role of individual defense technologies in the context of a broader defense strategy.

Extending Results Beyond MIT

In theory, the notion of combining multiple layers of defense to improve security has much to recommend it, but in practice it is often unclear how to design, implement, and assess these multi-layered systems effectively. Beyond exploring security issues specific to MIT, or even research universities, this analysis of the interplay between and combination of multiple different defense mechanisms on campus may provide insights relevant to all organizations seeking to design a comprehensive defense strategy for complex computer systems.

Acknowledgment

This work is funded by the Office of Naval Research under award number N00014- 09-1-0597. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the Office of Naval Research.