Protecting Organizations with Practical Data-Driven Methods

Sophisticated attackers routinely compromise enterprise and government networks, allowing adversaries to steal sensitive data, extort businesses for millions of dollars, engage in political espionage, and disrupt critical infrastructure. To address these threats, many organizations collect extensive amounts of data about their networks and employ teams of security analysts to detect and stop attacks. Unfortunately, security teams struggle to use this data to protect their organizations because conventional techniques are ill-suited to find stealthy and targeted (unlabeled and rare) attacks in vast, noisy datasets.

My research addresses this problem by developing new data-driven methods that leverage insights from large, real-world datasets, security domain knowledge, and collaborations with a variety of commercial and academic organizations. This talk will explore two systems I’ve built that enable enterprise security teams to uncover and thwart attacks against their network. First, I’ll describe a set of methods that organizations can use to detect spearphishing attacks, mitigating the predominant way that attackers break into an enterprise’s network. Second, I’ll discuss a system that can help stop attackers from spreading within an enterprise’s internal environment, allowing organizations to minimize the damage incurred by successful breaches. Organizations such as the Lawrence Berkeley National Laboratory, Facebook, and Barracuda Networks have used the ideas from my research to detect real-world attacks against their networks and improve the security of millions of users.

Bio: Grant Ho is a CSE Postdoctoral Fellow at UC San Diego, where he works with Geoff Voelker and Stefan Savage. Previously he received his Ph.D. from UC Berkeley, advised by David Wagner and Vern Paxson. Grant’s research explores how we can effectively use large-scale data to improve computer security. He is the recipient of an NSF Graduate Research Fellowship and a Facebook PhD Fellowship; and his work has been recognized with three distinguished paper awards across the top security conferences, such as Usenix Security and IEEE Security and Privacy, and the 2017 Internet Defense Prize.

Host: Nick Feamster