Security Forum Presentation and Presenter Bio

"Coming Detractions: Crossfire DDOS Attack", by Min Suk Kang, PhD student in Electrical and Computing Engineering and CyLab at Carnegie Mellon University.

The Crossfire Distributed Denial of Service (DDOS) attack can effectively cut off the Internet connections of a targeted enterprise (e.g., a university campus, a military base, a corporate web servers, a set of energy distribution stations); it can also disable up to 53% of the total number of Internet connections of some US states, and up to about 33% of all the connections of the West Coast of the US. The attack has the hallmarks of Internet terrorism: it is low cost using legitimate-looking means (e.g., low-intensity, protocol conforming traffic); its locus cannot be anticipated and it cannot be detected until substantial, persistent damage is done; and most importantly, it is indirect: the immediate target of the attack (i.e., selected Internet links) is not necessarily the intended victim (i.e., an end-point enterprise, state, region, or small country). The low cost of the attack, would also enable a perpetrator to blackmail the victim.

Min Suk Kang

Min Suk Kang is a third-year PhD student in Electrical and Computer Engineering at Carnegie Mellon University. He is advised by Virgil Gligor in CyLab. Before he joined CMU, he received the M.Sc and B.Sc degrees in Electrical Engineering at KAIST in 2008 and 2006, respectively. He is supported by funding from the Korean Government Scholarship Program and Carnegie Mellon University.

Security Forum Presentation and Presenter Bio

"PicoCTF: Inspiring Tomorrow's Cyber Security Workforce and Leaders", by Jonathan Burket, PhD student in Electrical and Computing Engineering and CyLab at Carnegie Mellon University.

Prof. David Brumley, the Plaid Parliament of Pwning (PPP), and the CMU Entertainment Technology Center are hosting the second annual PicoCTF competition, a nation-wide high school computer security contest with the primary goal of encouraging computer security and computer science education. In the fall of 2014, PicoCTF (picoctf.com) will feature high school students competing in realistic security challenges woven into a fun storyline. Participating students, anywhere from the somewhat computer savvy to experienced programmers, will learn how to identify security vulnerabilities and perform real-world attacks. The competition covers computer forensics, cryptography, web exploitation, reverse engineering, and binary exploitation.

2014 is the second year we will be hosting the PicoCTF competition. In 2013, PicoCTF attracted 10,000 students from over 900 schools in 48 states. Students in the competition played for an average of 12 hours, and in doing so learned to forge an HTTP cookie, read a control flow diagram, and brute force a hashed password. Every instructor surveyed after the competition reported that they would encourage their students to participate in PicoCTF again.

Jonathan Burket

Jonathan Burket is a first-year PhD student in Electrical and Computer Engineering at Carnegie Mellon University. He is advised by David Brumley in CyLab. Before he joined CMU, he graduated from University of Virginia in 2013 with BAs in Physics and Computer Science. His research focuses on web security and binary analysis in embedded systems. In 2012, he worked at Udacity (an online MOOC) to help develop an online introductory physics course taken by thousands of students worldwide. He is supported by funding from Carnegie Mellon University and a Frank J. Marshall Graduate Fellowship.