Adaptive Host and Network Security: (Diagnosing, Reacting, Evading And Maneuvering)

Scott Alexander (Applied Communication Sciences, USA)
Paul Robertson (DOLL, Inc. USA)
Greg Sullivan (Draper Labs)

`http://www.dollabs.com/saso2015ahansdreamworkshop`

Over the past decade the threat of cyber attacks on critical commercial and government infrastructure has been growing at an alarming rate to a point where it is now considered to be a major threat in the world. Current approaches to cyber security involve building fast-growing multi-million line systems that attempt to detect and remove attacking software. Meanwhile, cyber exploits continue to multiply in number, but their size continues to be a couple of hundred lines of code. Related factors are that the defenders have to defend the entire system where attackers only have to find a single hole. These disparities of effort means that the current defensive approaches to cyber security can at best fight a holding action. The workshop is intended to explore game-changing approaches to cyber security that focus on adaptation. There is a clear need to develop systems at both the host level and the network level to actively adapt to cyber attacks and to provide greater protection for networked computation at all levels. Adaptation provides the ability to dodge an attack but certain reactions can result in self denial-of-service attacks. Maneuvering can lead the attacker astray, even into a trap. For example reconfiguration of the network to move computation out of the line-of-fire while making the original configuration appear live to the attacker can not only lead the attacker away from important assets but also allow the attackers actions to be monitored. How can we diagnose the nature of an attack and how can such diagnoses help in surviving an attack?

We seek papers that demonstrate early results in addressing adaptive approaches to surviving cyber-attacks.