Cyber Grand Challenge - A Response - Andrew Dudley - 1001149051

It's difficult to do much criticizing of either the host or the players of the Cyber Grand Challenge, primarily due to the fact that a fully automated CTF event of this sort has never been done before. From that perspective, everything appears to have been very well thought out, with seemingly few hiccups considering the complexity of the systems at play. In this review, I'll attempt to point out some of the aspects of the CGC in general, and possibly the techniques used by shellphish, which appear to be areas where further exciting development could be found.

These kinds of events are very structured. There are a lot of rules, a lot of predetermined information available, and the hacking teams spend a year+ developing a system that is optimized against these constraints. There is one major issue with this, which is that this isn't how cyber security and hacking actually works in the real world. There are no rules. There are no hard constraints. It's a game of cat and mouse where everything is changing.

Speaking of rules and games, one of the greatest downfalls of Shellphish seems to have been their game strategy (or lack there of.). They pointed out that it's possible that by waiting to patch their binaries until first deploying the exploit - all other things held equal - they would have placed in second. While there are no explicit rules in the real world, it is certainly still a game, and to win any game, the player must not only be able to understand lower level moves (which equates to finding valid actions), but also be able to formulate intelligent, adaptive plans. Hack the game. The mechanical Phish was in dire need of a higher-order planning module that could learn the unknown aspects of the game and act accordingly to maximize their points. It could still locate vulnerabilities, develop POV, and create patches (which probably looks better for Shellphish once the tournament has ended), but only play them when doing so promises maximum points.

All who participated agree that a lot was learned from the Cyber Grand Challenge, and it goes without saying that we still have a *lot* more to learn. It would be interesting to see a system developed that converts this type of challenge from a one day event into a more persistent form. Teams working over years to improve their automated systems, scheduled and unscheduled battles against other autonomous systems, a changing set of rules that force the developers to adapt and discover more. From where we stand, it seems like an impossible task to evolve from these toy challenges to something a bit more real. Maybe the implementation of a ceaseless war of semi-autonomous systems is just the catalyst needed to bring forth the next generation of autonomous cyber security platforms.