Cyber Attack and Defense

It is well-known that attacks on industrial, government, and academic digital installations via the Internet threaten the security and economy of the United States. While most attacks are amateurish and can be detected fairly easily, the more serious attackers are continuously changing their tactics to be harder to defend against. They may be trying to steal Intellectual Property, or trying to damage an organization's infrastructure and/or data, or they may just be interested in stealing currency. These attackers are the dangerous ones.

A number of technological devices have been developed over the years to ensure confidentiality, data integrity, and authenticated communications. Notable examples include various public key cryptosystems such as RSA, Diffie-Hellman key exchange and elliptic curve versions of these, secure symmetric key cryptosystems such as AES-256, and hash-based systems for checking the integrity of data. Unfortunately, attackers have developed ways to side-step the security of these cryptosystems with side-channel attacks using timing or differential power analysis, or social engineering, or weaknesses in Operating System design and implementation, or by exploiting vulnerabilities that inadvertently exist in code due to bugs introduced by coders or incomplete testing against requirements. Attacks have become so successful that many people wonder whether it is possible to secure the Internet at all.

This project aims to shed some light on why it seems so difficult to protect the Internet. Using tools for attack, participants will see how an attack is planned and launched. Participants will see that effective attacks do not happen instantaneously but occur over a long period of time in phases that are characterized as a cyber kill chain. In the first, reconnaissance phase, the attacker gets some idea of the victim's network topology and potential vulnerabilities. In the 2nd, weaponization phase the attacker has crafted a tool for attack based on the information gathered in the first phase. Later stages involve delivery of the attack to the victim, resulting in the installation of the attacker's software, and finally execution of the attack. What has people really worried is that in some cases the execution is delayed indefinitely, possibly until the moment that a massively destructive cyber event is initiated, possibly by a foreign government. Unfortunately, it is often very difficult to detect a dormant attack payload as it generally does not give any indications of being active. What can be done, if anything?

For one thing, breaking the chain before execution will prevent or at least mitigate damage. There are numerous tools for doing this and project participants will experiment with some of them. But, detection and prevention tools cannot be static because sophisticated attackers will modify how they do reconnaissance so they look like benign traffic, for example. So, existing defensive tools eventually have to be modified or replaced. How is this done?

Research: offensive tools and defensive tools - understand what these accomplish and how they do it
run both kinds of tools to develop an appreciation of the power and limitations of each

Big Idea: for an attack that appears to be impervious to existing tools, can a new tool be designed to break the kill chain?