DESCRIPTION OF THE RESEARCH PROJECT FOR THE 2018 SUMMER RET SITE

Project 5: Secure Cyberspace

Area Coordinator:
Dr. John Franco
Geier Professor, Computer Science
Department of Electrical Engineering and Computing Science
College of Engineering and Applied Science
PO Box 210030
University of Cincinnati
Cincinnati, OH 45221-0030
Office: 831 Rhodes Hall
E-Mail: franco@gauss.ececs.uc.edu
Phone: 513-556-1817

Sub-Area Coordinator:
Dr. Raj Bhatnagar
Professor, Computer Science
Department of Electrical Engineering and Computer Science
College of Engineering and Applied Science
P.O Box 210030
University of Cincinnati
Cincinnati, OH 45221-0030
Office: 829 Rhodes Hall
E-Mail: raj.bhatnagar@uc.edu
Phone: 513-556-4932

Graduate Research Assistant:
Mr. Shaunak Kapoor
M.Eng. Student in Computer Science/Cyber Track
E-Mail: kapoorsk@mail.uc.edu; kapoor.shaunak37@gmail.com
Phone: 513-206-4906

Project Summary

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?

Challenge: Pick out at least one phase and one defensive action of the cyber kill chain and improve the ability of an existing tool to perform its intended task.

Guiding Questions:

How is a network configured to limit damage should an attack occur?
What devices are used to sense unusual traffic and behavior?
How do those devices work?
What software (types) is (are) used to detect and prevent intrusion and generate alerts for analysts?
Can humans successfully analyze the enormous amount of alert data that is generated by this software?
Can sensor software be designed to minimize the number of false positive alerts generated?
Can alerts be analyzed automatically to determine attacker intrusion, damage, command and control?
How did some well known attacks, such as Heartbleed, proceed?
What attacks are extremely difficult to detect or follow and why is that the case?
Can software be developed to examine code for vulnerabilities and correct them?

Facilities and Equipment to be Used

The entire development environment for this project will be placed on an 8 GB USB flash drive with Ubuntu 14.0.4 LTS installed at about $10 each. The environment includes the development tools necessary for an advanced classroom including *Eclipse, Emacs, VIM, OpenJDK, gcc, g++, Google-Chrome* or *Firefox,* and *Octave*. The devices can connect to the Internet via NetworkManager. In addition, a project website will be hosted on the *apache server* at http://gauss.ececs.uc.edu/ProjectX where X will be determined just before the RET period. The USB drives will be able to boot on any PC at the university or at the RET participant’s schools. At the university, labs in Old Chemistry 805, 825, and 614, together housing approximately 100 PCs, are available for the project.

Field Trip to Northrop Grumman Mission Systems

The field trip will be hosted at Northrop Grumman Mission Systems (NGMS) in Springdale. The primary instruction will be via presentations to inform teachers of the real world products that are created with the skills and knowledge gained in the cyber realm. This will include an introduction to NGMS and the cyber technologies used at NGMS plus a presentation to about NGMS experiences in penetration testing (or performing cyber assessments) for internal Northrop Grumman business units to test the integrity of corporate Northrop Grumman cyber systems and what results were discovered. Teachers are likely to learn more about real world products and career opportunities that are created by cyber operations.

Industrial Advisor for the Project

In addition to coordinating the field trip, an industrial advisor, Mr. Justin Spencer from Northrop Grumman

Mission Systems, Springdale, Ohio will work with RET participants during the summer he will participate in an *Industrial Advisors Panel Session* during the 2018 Summer RET Site to plan and schedule activities for teachers' students during the school year.

Possible Ideas for Classroom Implementation

A cyber competition can be designed and implemented. The particular class of competition will be up to the teachers. They may wish to design a Cyber Defense Exercise where students are given a VM to defend against an attack by a teacher or other students known as the red team. The VM runs services such as Wordpress and the red team tries to knock those services out. Scoring is based on the amount of time services are up. Or they may wish to modify one of the competitions that are part of the cyber curriculum such as the I-Wars® competition where teams defend their systems as well as attack other team systems. In all cases, authentication, integrity, and encryption protocols will be used.

A classroom *mathematics, computer science, or engineering* unit building on the research in this project could possibly discover vulnerabilities in protocols and software supporting the competition and perhaps protocols used in practice. Activities arising from the teachers' experience with research will expose students to issues in defending against malicious attacks as well as detecting anomalies in software designed by well-intentioned engineers.