Project/Paper Ideas for COE449

Dr. Ahmad Almulhem
spring 2008 - 072

1 Design Projects

- **Hospital Network**
  Design a network for a hypothetical general hospital. The design has to enumerate different types of users, such as doctors, patients, etc. Also, it should consider different resources such as patients' records, employees' records, etc. Identify potential threats and perform risk analysis. Design a suitable security policy and choose suitable mechanisms to enforce the policy.

- **University Network**
  Design a network for a hypothetical university. The design has to enumerate different types of users, such as students, faculty, etc. Also, it should consider different resources such as students' records, employees records, etc. Identify potential threats and perform risk analysis. Design a suitable security policy and choose suitable mechanisms to enforce the policy.

- **Honeypot**
  A honeypot is a computer system on the Internet that is intentionally set up to attract and "trap" attackers who attempt to penetrate other people's computer systems. It can provide a valuable surveillance tool [see honeynet project]. Design and deploy a honeypot in an environment of your choice. Present a complete study and statistics of the seen attacks.

2 Programming Projects

- **Email spams**
  E-mail spam ("bulk e-mail" or "junk e-mail") is an abuse of the Internet by sending nearly identical messages to numerous recipients by e-mail. Design and implement a tool to detect spam emails. One possible way to detect spams is to search for common spamming words.

- **Phishing**
  Phishing is an attempt to illegally acquiring sensitive information, such as user-names, passwords and credit card details, by masquerading as a trustworthy entity (for example, as a bank). Design and implement a tool to detect phishing emails/websites.

- **Steganography**
  Steganography refers to hiding a message in such a way that only the sender and intended recipient know about the hidden message. Examples of steganography techniques include embedding the desired message in a jpeg image or a pdf document, etc. Design and implement a steganography technique of your choice.

- **Chaffing**
  Chaffing is a cryptographic technique to achieve confidentiality without using encryption. It can also be viewed as a steganography technique (see above). Design and implement a chaffing tool.

- **Port Knocking**
  Port knocking is a method used for dynamically modifying firewall rules. In this method, a user is only granted access when she/he perform a correct sequence of connection attempt to a set of prespecified closed ports. Design and implement a port knocking daemon and analyze its security and possible attacks.

- **Firewall**
  A firewall is a dedicated appliance, or software, which inspects network traffic for the purpose of denying or allowing passage based on a set of rules. Design and implement a firewall with specific features and properties.

- **Graphical passwords**
  Text-based passwords can be difficult to remember. Graphical passwords provide an alternative, where images are used instead. Design and implement an authentication system that uses graphical passwords.

- **Security Policy**
  Design and implement a GUI tool to design security policies. The tool should automate the routine tasks in designing and deploying a security policy.

- **Security Visualization**
  In a protected network, there are many sources of data, which include traffic, firewalls logs, IDS alerts, etc. Security visualization refers to graphically presenting security-related data in a way that provide useful and actionable insight. Design and implement a security visualization tool.

3 Analysis Projects

Analysis projects can be viewed as a complement of design projects. In this case, an existing system need to be systemically analyzed for possible vulnerabilities. The goal is to identify security threats and propose a plan to improve the existing system.

4 Papers

Writing a term paper requires choosing a topic related to network security, and researching it. You should at least survey 4 papers under the selected topic. The paper's organization and content has to be comparable to published papers (see next section). Most of the ideas under "Project Ideas" are also applicable for writing a term paper. The following list provides additional topics:

- Secure communication protocols
- Honeypots
- DOS/DDOS Attacks
- Buffer-Overflows

- malwares types and classifications
- Network forensics
- Intrusion Detection Systems

5 More ideas

More interesting ideas can be found in the computer security literature. The following is a list of some representative publications:

Journals & Magazines

- IEEE Security and Privacy Magazine (http://computer.org/security/)
- ACM Transactions on Information and System Security (http://www.acm.org/tissec)
- IEEE Transactions on Dependable and Secure Computing (http://www.computer.org/tdsc/)
- Journal of Computer Security (http://www.mitre.org/jcs)
- Computers & Security (http://www.elsevier.com/locate/issn/01674048)
- International Journal of Network Security (http://ijns.nchu.edu.tw/)
- Journal of Privacy Technology (JOPT) (http://www.jopt.org/)

Conferences

- The ACM Conference on Computer and Communications Security (CCS) (http://www.sigsac.org/ccs.html)
- Digital Forensic Research Workshop (http://www.dfrws.org/)
- Recent Advances in Intrusion Detection (RAID)(http://www.raid-symposium.org/)
- USENIX (http://www.usenix.org/)