# Network Security

# Project Proposal

## CHANG LIU

## chang.liu@jhu.edu

# Mar. 2, 2012

**Develop a tool that can protect a system from hacking**

1. **Background of the Problem**

The Coordination Centre of the Computer Emergency Response Team at Carnegie-Mellon University has recorded a doubling of both software vulnerabilities and reported security incidents every year since 1999. Since the rates of intrusions and security incidents have increased dramatically in the last few years, there is an increasing demand for Intrusion Detection System for a network or system administrator to monitor and maintain the security of the network. In addition, the IDS system should not only be able to detect the malicious attempt from the attacker, but should also be able to prevent such attacks.

An Intrusion Detection and Prevention System (IPS) is a software application that monitors the malicious networks and/or system activities or policy violations, furthermore, the application will log the said activities, attempt to block/stop activity, and report activity. Our goal in this project is to develop an Intrusion Detection and Prevention System that could monitor and handle some well-known malicious activities in the real network environment.

1. **Citation of the Paper**
2. **Description of the project**

Our project goal is to develop an integrated tool that could identify some well-known security vulnerabilities of a website and propose solutions to those vulnerabilities. Our tool should have some individual modules that could detect different kinds of vulnerabilities. The user only need to enter the URL of a particular website then the tool will call each module that had been integrated into it to detect the certain kinds of potential vulnerabilities.

For example, when we enter the URL “http://www.test.com”, the tool itself will look up and analyze the home page to see if there are any SQL injection entries that are available to hack. Then the SQL injection module of the tool will automatically test the entry to see whether such an entry is vulnerable to SQL injection by making attempt to hack it. We may also need to analyze the result returned by the server of the hacking attempt and then determine whether the page is SQL injectable. If the module failed to make the injection attempt, we may say the site is not vulnerable at least to our test case. If the module successfully performed the attack, we know that the site is vulnerable to the SQL injection, and thus the tool will provide the solution guideline to SQL injection (like what it is, how it happened, and how to avoid such kind of vulnerability).

So in this way, a user who may not have knowledge in the security area could know the potential security risk of their site and learn how to fix it.

1. **Description of the deliverables**

The deliverables will be a software application that could detect and measure the potential security vulnerabilities of a given website, and provide solutions to fix the vulnerabilities found as well.

1. **Description of approach to produce deliverables**

As we are not familiar with the techniques that are used to detect the intrusion attack attempts, we may first need to learn something about that, and develop our application while learning all the techniques we need.

We plan to develop our program in a phases manner, for the first phase we want develop some basic functions / modules that could be easier to implement with simple output. For instance, the phase one product should be able to detect the Denial of Service attack and output/log the attacker’s IP address. The goal of phase 1 is to make our application basically functional, more features will be added to the program in the phase 2.

In phase 2, while we becoming more and more familiar with the procedure and techniques to detect some well-known intrusion activities and the way to prevent them, we will start to add more features that could detect and analyze some more complex intrusion attempts like ARP attack. In addition, we will polish the products from both phase 1 and phase 2, all the output from each module/function will be in report format along with graphical display that will be easy for system/network administrators who have no experience in security to read and understand.

For phase 3, we will test all the modules/functions we developed during the phase 1 and phase 2, fix any bugs we may find during the test.

1. **What will be novel/new in your project as compared to the chosen paper(s)? Describe the** **differences clearly**
2. **Required resources**

*Snort* Open Source Platform