# Intelligent Security Systems
# Project - Intrusion Detection System

Sameera Desai, Appurv Jain, Sagar Parab

March 31, 2013

**Executive Summary:**

As the technology is ameliorating, the number of hacking and intrusions are augmenting. The motive behind the attack can be personal or professional. Intrusion Detection Systems are like alarms that alerts the user of the attack. Intrusion Detection Systems monitors the networks or the system behaviors for malicious activities or behaviors. It generates reports based on these activities. They detect unauthorized accesses.

We will be implementing the Intrusion Detection System using R, a popular scripting language for statistical computing. R is open source and provides us with the flexibility and potency of a scripting language and has many freely available packages that implement many artificial intelligence and machine learning algorithms, statistical modeling techniques and various other useful tools. Being a scripting language, R enables us to write our own rules for misuse detection and can implement artificial neural networks using the Neural Networks package. Additionally, R provides a lot of functionality for data manipulation and visualization, which will enable us to clean and prepare the data for analysis.

**Specification:**

Our decision to select R as our tool of choice was preceded by a significant amount of research on popular Intrusion detection systems such as Snort, Bro, etc. However, those tools inhibit flexibility in terms of the techniques used for anomaly and misuse detection. Alternatively, we could have decided to use a data mining tool such as Weka, but the GUI interface is not as flexible and powerful as a scripting language. Therefore we decided to use R.

Some of the advantages of building an IDS using R are :

- Since R is written in C and Fortran, it is very fast. This is a string positive since many techniques used in misuse and anomaly detection are computations intensive
- R is open source
- R programs can be developed as a command line utility or have a GUI
- R contains a vast collection of packages that support a wide variety of data processing and modeling techniques.
- Hence all the tools and abilities required to build an efficient Intrusion Detection System is present in R itself

**Methods and Techniques:**

In order to prepare the data for the next phase, we compiled the various data sets into two distinct data sets, one for Misuse Detection and the other for Anomaly Detection.

The data set for anomaly detection will contain normal usage classified as 'normal' and all the attacks, regardless of type will be classified as 'attack'. This helps us classify pattern other than normal behavior as an attack.

For misuse detection, we used the 'normal' classification for normal usage and named the other attacks by their specific types.

**Implementation:**

We used R for data manipulation. The attack we took into consideration were as follows:

1. Neptune
2. Satan
3. Smurf
4. PortSweep
5. Nmap

We converted the given files to csv so that they were compatible with read functions in R. Then using R, we added columns according to the attack type and finally combined the various tables to form our master datasets for anomaly and misuse detection.