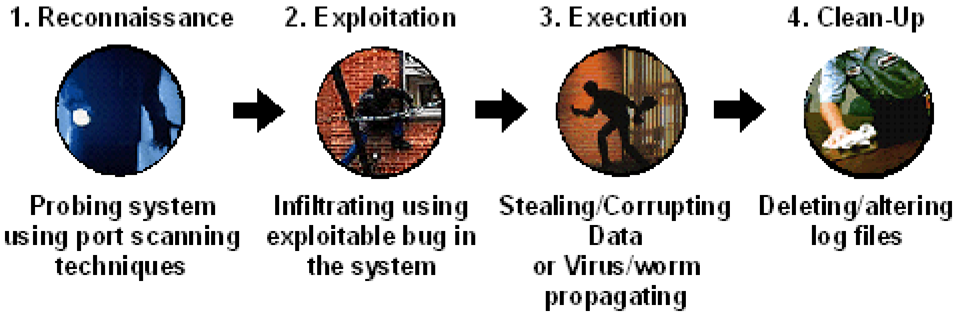
HOW'S THE TRAFFIC?

ABSTRACT

Network security is still at its infancy. Existing intrusion detection and prevention solutions lack accuracy, broad attack coverage, speed, performance, and scalability. They do not provide reliable protection to today's vital networks. Random Knowledge's approach to intrusion detection is to apply Mathematically Optimal Detection that outperforms other methods, including pattern matching, neural networks and statistical techniques. Our mathematical algorithms detect and localize traffic patterns consistent with possibly-stealthy forms of attacks from within hoards of legitimate traffic. Basic to this approach is the need for a high fidelity model of the *normal traffic*.

PREVENTING INTRUSIONS

External hackers use a four step process for intrusions: reconnaissance, exploitation, execution and clean up.


1. Reconnaissance
2. Exploitation
3. Execution
4. Clean-Up
Probing system using port scanning techniques
Infiltrating using exploitable bug in the system
Stealing/Corrupting Data or Virus/worm propagating
Deleting/altering log files

Stages to hacker attacks

Reconnaissance involves a method called port scanning, which determines what computer ports are open as well as what programs or services are running on a particular system by sending a sequence of probing packets to the target network and observing its responses. Inevitably, programs have exploitable weaknesses. Once a system's weakness has been found, an intruder exploits this flaw to enter the system. Next the intruder executes his attack, which can range from propagating a worm to stealing valuable company information. According to Abtrusion Security AB, "to steal or somehow modify information is probably the primary goal of the hacker"[1]. Lastly, intruders typically 'cover their tracks', especially when the chance of being closely monitored by sophisticated software is high.

In reconnaissance, a hacker tries to find an exploitable computer bug or website hole through which he/she can gain access/control of the network or launch a worm attack. He/she often scans the target network's ports by employing stealthy techniques such as:

1) spreading his probe packets out over a long period of time,
2) launching his scan through a multitude of other compromised computers, and
3) sending extra non-probing packets with spoofed source information.

[1] Torbjörn Hovmark, "Anatomy of a Hacker Attack", Abtrusion Security AB, 2002

Once a hacker is inside a network he/she will often slowly execute his/her ultimate goal by masquerading as legitimate users. This reconnaissance may take up to weeks but a huge payoff apparently makes the wait worthwhile.

Random Knowledge Inc. (Random Knowledge) has developed a sophisticated, scalable real-time Portscan Detection System (PDS) that will estimate the likelihood of various malicious activities on a computer network. Random Knowledge's PDS includes: 1) a highly sophisticated, patented detection and tracking algorithms to detect stealthy hacker espionage, 2) a proprietary anomaly detector for less expensive solutions, 3) a sophisticated, patented localization technology to provide estimates about the source and destination of malicious packets, and 4) an automatic response system that either gives the hacker incorrect information for trapping him/her in a virtual "fish bowl" or eliminates his/her ability to gain access via a dynamic firewall.

PROBLEM AREA 1

Random Knowledge's detection systems relies on high fidelity models for normal traffic[2] from which it can critically judge the legitimacy of any substream of packet traffic. The input to the PDS is the network's packet traffic stream. In our first problem area, we will try to characterize normal traffic which involves:

a) defining all the different types of connection sessions,
b) verification of a Poisson measure model for the incoming connection sessions, i.e. if the connection session types are labelled 1,…,n, determining if $N(A\times(0,t])$ is Poisson distributed for any subset A of {1,…,n}, where N is the Poisson measure,
c) determining the rates for $N(A\times(0,t])$ or equivalently its mean measure if the session generation indeed conform reasonably to the Poisson measure model, otherwise suggesting other suitable models, and
d) verification for self-similar processes and heavy tailed distributions within connection sessions (for example the transmission time), and the estimation of its parameters.

Hitherto, there has been much study of traffic characterization that focuses on the implications for improved network performance. Random Knowledge's approach is the study of traffic characterization for the implications of detecting malicious hacker activity.

PROBLEM AREA 2

The PDS's anomaly detector component uses a combination of simple statistical tests. The purpose of these tests are solely to determine when to throw out the null hypothesis that all the traffic observed is legitimate. In our second problem area, we will use the results of the first problem area to fine-tune the hypothesis tests to maximize a weighted cost between missing portscans (false negatives) and producing too many false alarms (false positives).

[2] We define normal traffic as the traffic generated by legitimate users.