Wu-chang Feng

Email: wuchang@cs.pdx.edu
Telephone: 503.725.2409

Open Source

1. Forensix: Automated analysis and recovery of computing systems

(Project funded by NSF)

When intrusions occur and systems are compromised, one of the most time-consuming, error-prone, and expensive operations is the analysis and recovery of the system. Unfortunately, current forensic systems and techniques fail to efficiently provide the ability to perform reconstruction and recovery in a detailed manner. With the rapid increase in computing, networking, and storage capacity and the precipitous drop in their respective costs, the ability to do large-scale auditing, analysis, replay, and rollback of system activity is now technically and economically feasible. In this project, we are constructing the computer equivalent to ``TiVo" that will allow system administrators, law enforcement officials, and security experts to quickly track down sources of security incidents and undo the damage that has been caused.

Specifically, we are currently augmenting the SNARE and SELinux auditing frameworks to support complete system call auditing to a backend database. We are also developing database functionality that will allow the system to efficiently handle a set of queries that are essential for doing forensic reconstruction and system recovery. A proof-of-concept prototype is available at http://forensix.sourceforge.net

2. PuzzleNet: Automated network defense

(Project funded by an Intel Research Council award)

Whether it is spam, viruses, worms, or denial-of-service attacks, undesirable Internet communication is currently uncontrollable. One of the approaches for thwarting this activity is the use of client puzzles. The idea of client puzzles is to force a client to solve a hard puzzle before giving it service. Forcing a client to solve a puzzle slows it down, thus preventing it from quickly spreading malware and from overwhelming servers. One of the disadvantages of current puzzle mechanisms is that they do not operate at a layer common to all Internet activity: the IP layer. Because of this, they cannot be used to thwart arbitrary network attacks. In this project, we are building a client puzzle mechanism directly into the fundamental Internet protocol layer.

An IP layer puzzle mechanism forces hackers and spammers to expend an arbitrary amount of resources and money to continue their activities. In order to effectively realize the potential of IP puzzles, we are also examining ways to dynamically and automatically issue them based on network information collected from a distributed set of sources. When coordinated widely, IP layer puzzles can be used to support a cyber-equivalent to the Emergency Response System, instantly slowing down communication activity that threatens to overwhelm the

Internet. A proof of concept prototype is available upon request. The project's web page is at http://syn.cs.pdx.edu/projects/puzzles

3. Infrastructure for On-line Game Services

(Project funded by an IBM Faculty Partnership Award)

On-line gaming is quickly becoming the next killer Internet application, rapidly blossoming into a multi-billion dollar industry. Due to the unpredictability of game popularity and the large fluctuations in game usage, on-line games are an ideal candidate for on-demand computing and network infrastructure such as those provided by IBM. The idea behind on-demand infrastructure is to treat computing and network resources in the same manner as the power grid treats energy resources.

To this end, this project is examining how best to multiplex a diverse set of applications onto this "computing grid" with the goal of driving down the costs for both game providers and hosting providers. With our partners at IBM, we are currently working on several open-source game services including a geographic redirection service and a cheat prevention service. We are also developing provisioning strategies for allocating cluster resources for games using IBM's Tivoli Intelligent ThinkDynamic Orchestrator.