The Industry:
Protection from the Outsider Threat

AntiVirus

A virus is a self-replicating, usually malicious, computer program. Anti-virus software actively protects by identifying known viruses by their digital 'signature'.

2007 anti-virus market leaders:
Symantec, **McAfee**, **Trend Micro**

AntiSpyware

Spyware collects personal information about users without their informed consent. Its purpose ranges from data mining to password theft.

2007 anti-spyware market leaders:
Symantec, **LavaSoft**, **Spybot**

Intrusion Detection (in general)

In Information Security, intrusion detection is the act of detecting actions from an outside attacker that attempt to compromise the confidentiality, integrity or availability of system resources.

Intrusion detection tools include:

- Firewalls
- VPNs
- Audit Tools
- Physical Access Control

Insider Threat Prevention

No tools exist. With billions of dollars being spent on the outsider threat, it's surprising that the industry has not made a stronger push to protect against insider attacks.

BACKGROUND INFORMATION

References & Resources

References

[1] National Survey on Managing the Insider Threat
09/12/2006 – by the Ponemon Institute and ArcSight

[2] CSI/FBI Computer Crime and Security Survey
2003 – by Robert Richardson

[3] Survey on Identity Compliance
03/01/2007– by the Ponemon Institute and SailPoint Technologies

[4] Internet misuse costs businesses $178 billion annually
07/19/2005 - By Peter Saalfield, IDG News Service

IPRO 311 Spring 07 Contacts

Alana Platt – Project Leader - platala@iit.edu
Dr. David Grossman – Faculty Advisor - grossman@iit.edu
Dr. Nazli Goharian – Faculty Advisor - nazli@ir.iit.edu

IIT Center for Information Security

Web: http://iitcis.iit.edu
Email: info@iitcis.iit.edu

Department Information

Illinois Institute of Technology
Department of Computer Science
10 West 31st Street
Chicago, IL 60616
Phone : (312) 567-4496
Web: www.cs.iit.edu

IPRO311
The Misuse Problem

Helping Fight Computer Crime

The Growing Insider Threat

With almost every aspect of our daily lives depending on digital data transmission and verification, the need to protect these channels is paramount. Most attention has been given to the outsider threat (hackers, viruses, etc.), yet these threats make up the minority of computer crime. The real danger lies in what the Defense Personnel Security Research Center has called the "Peopleware Problem".

[2]

There's software for this, right?

Not quite. It's surprising that the market has not yet capitalized on this threat, but this problem is a bit more complicated than you might expect:

- There is an insufficient amount of user-activity data available for product testing
- A computer-generated dataset can be used, but many question its validity
- A true (real world) dataset is ideal, but companies are reluctant to disclose private user

78

: the percentage of respondents that reported one or more insider-related security breaches within their company [1]

Objectives of this Project

- Bridge the gap between threat and solution.
- Create a "true" dataset for future use in misuse prevention.
- Test the validity of the data by developing detection software.

The Solution:
Developing a Real Dataset

The Spring 2007 IPRO 311 team will be working to develop a dataset of real user activity and habits. To test the validity of our data, we will create misuse detection software for preliminary analysis of our results.

Why is this Important?

- American organizations lost more than **$178 billion** to insider misuse [4].
- All existing utilities are reactive which *cannot* fix the problem. We need to facilitate a "smart" detection system.

Tackling the Problem

To effectively begin development, the team had to analyze our members' skill sets and create several distinct and specialized subteams:

Project Management
Alana Platt [Project Leader]
Yacin Nadji [IPRO311 Team Leader]

Software Development Team
Jason Soo [SubTeam Leader]
Yacin Nadji
William Alton
Matt Holmes

Query Processing Team
Jong Min Lim [SubTeam Leader]
Young Cho
Peter Niedzinski
Gerardo Sanchez

Design Team
Justin Choriki [SubTeam Leader]
Mark Malanowski
Daniel Hyc
Hee Yeol Jeong

60

: the percentage of US-based businesses and government agencies that admit inability to effectively assess "insider threat" risks within their organizations. [3]

Our Progress:
From Concept through Creation

Key Tasks

- survey current security tools
- develop data recording tool
- queries / dataset creation
- build misuse detection prototype
- analyze results

Critical Barriers

- coming together as a team
- software compatibility issues
- metric logging anomalies

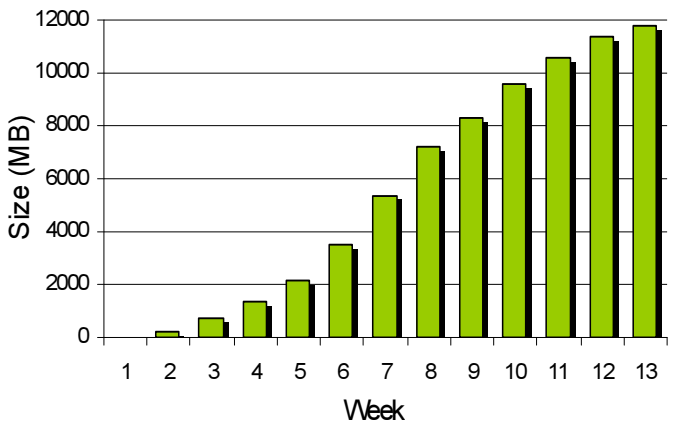
Data Collection

The logging system is built and installed on a modified version of Knoppix, a bootable Linux distribution. The "distro" is loaded from a CD-R and can be run on nearly any hardware. Data is collected both from the operating system and through a controlled web search engine. The collected data is regularly synced to multiple remote data servers.

System-Level Metrics:
- CPU Usage
- Memory Usage
- Keystrokes
- Processes (Current, Old)
- Network Usage
- Files (New, Open, Modify)

Query-Level Metrics:
- Query String
- Documents Retrieved
- Time Spent on Page
- Document Relevancy
- Number of Clicks

Weekly Dataset Growth



Results:
A "True" Misuse Dataset

76 *Man hours* *of user activity*

13 *Hundred* *queries issued*

95 *Thousand* *keystrokes recorded*

12 *Distinct* *user profiles*

12 *Gigabytes* *of collected data*

Validity of the Dataset

During testing of the dataset using our in-house detection software, we were able to accurately discriminate misuse from normal use with only one recorded "false positive", which is excellent. Further development of the detection software should bring about even better results.

Conclusion

During the past 14 weeks, we have logged a wealth of user activity data which was eventually manipulated to create 12 distinct user profiles. These profiles, in conjunction with an in-house-developed misuse detection prototype, were used to analyze our final dataset and verify its validity.

Plans for the Future

We believe that the direction in which this project is moving has the potential to produce important advances for the information security community. We plan to:

- Continue development of a misuse detection prototype.
- Make the dataset available for other researchers.