

# Attack Graphs for Proactive Digital Forensics

Tara L. McQueen

Delaware State University

Research Alliance in Math and Science

Computational Sciences and Engineering Division

Mentor: Louis P. Wilder

[http://wiki.ornl.gov/sites/rams09/t\\_mcqueen/Pages/default.aspx](http://wiki.ornl.gov/sites/rams09/t_mcqueen/Pages/default.aspx)

## Purpose

- Increase cyber security and protection
- Identify possible cyber attacks as they occur
- Examine Universal Serial Bus (USB) exploits
- Create attack graph of USB exploit
- Explore event logs and registry data
- Investigate theoretical proactive design

## Cyber Security

- Maintaining confidentiality, availability and access of information
- Identifying legitimate
  - Users
  - Requests
  - Tasks
- Preserving information integrity
- Mending network vulnerabilities



## Cyber Protection

- Growing need as fraudulent activity increases
- Affecting industries dependent on
  - Networks
  - Computer Systems
  - Internet

## Hacking

- Gaining unauthorized
  - Access
  - Control
  - Data
- Using technical knowledge and exposed information
- Cleaning tracks
- Preventing is difficult and expensive



## Proactive Digital Forensics

- Anticipating hacker/exploit path
- Detecting hacker/exploit in progress
- Collecting proper data immediately for judicial efforts
- Enhancing security

## Attack Graphs

- Communicate information about threats
- Display combinations of vulnerabilities
- Show vulnerabilities as vertices
- Express hierarchical constraints via edges

## USB Exploits

- Take milliseconds to initiate (in and out)
- Collect confidential documents
- Send worm through network
- Execute applications automatically
- Easy to develop, retrieve and unleash
- Occur unknowingly



## USB Exploit Attack Graph

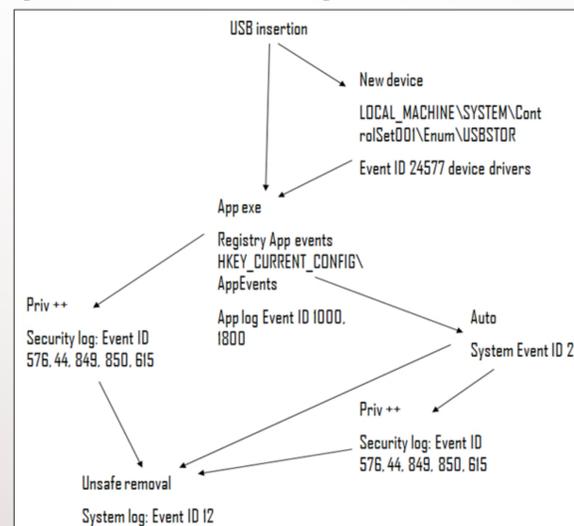


Fig. 1. USB exploit attack graph

## Event logs and Registry

- Standard on Windows
- Monitors events
  - Application
  - Security
  - System
- Identifies operations and information
- Essential for Attack Graph



Fig. 2 Windows XP Event Viewer

## Splunk

- Analyzes/monitors IT infrastructure
- Records and indexes data
  - Logs
  - Configurations
  - Scripts
  - Alerts
  - Messages
- Operates in real-time
- Search, navigate, graph and report data



Fig. 3. Splunk

## Theoretical Proactive Design

- All computers/nodes on network use Splunk
- Splunk's additional behavior configurations stem from attack graphs
- Attack graphs designed for all known exploits
- Plug-in device triggered
- Real-time alerts sent after trigger
- Instant in depth recording of "suspicious" activity

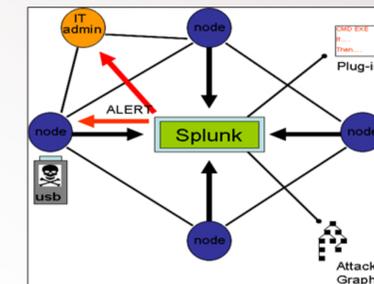


Fig. 4. Proactive Digital Forensic Design

## Splunk with Attack Graphs

- Targets specific attacks paths
- Allows unlimited attack types
- Provides systematic and proactive approach



## Future work

- Create plug-in
- Implement design on test network
- Run trial exploit
- Research and prepare other exploits/attacks