LogStitch

Graduate Student: Wajih Ul Hassan
Assistants: Jackson DeDobbeleare & Jerry Chen
Concept Introduction

- **System Data Provenance**
  - Lineage of all the activities that happened on the system
  - Can be used for forensics/reconstruct attack

- **Trustworthy Whole-System Provenance for Linux Machine**
  - Linux Provenance Module (Usenix Security Conference 2015) runs inside kernel to collect data provenance
  - Tamper Proof Monitor - Impervious to disabling or manipulation in user space
  - Complete System Awareness - Observation of all data that pass through controlled data types.
Research Objectives

- Instead of using Linux Provenance module which is running inside the kernel we will use application logs to reconstruct attack.
- Understand whether or not applications have enough logging information to analyze malware/attack entry.
- Stitch various logging information together to form a thread of information for traceability.
- With enough logging information, we can reconstruct the attack and uncover the system vulnerabilities.
Research Steps

1. Install various application source files (ex. Firefox, Chrome, Transmission, Nano, Vim, Tar, PostGreSQL, MySQL, xpdf, W3M, Bash, OpenSSH, Pine, ...).
2. Configure settings to allow logging then run applications to generate and collect logging data.
3. Analyze logging data and draw a conclusion for each application.
4. Install Malware on the system
5. Analyze logs to find out how malware is infecting the system
Research Status

- Installed source files for applications
- Configured Applications for logging capabilities
- Ran applications with some elementary tasks
  - Firefox (i.e. open tab, click on link, go to another tab, etc.)
- Collect the Logging Files
Log Entry Example

1095243584[7f1c3ff7e4a8]: http request [GET / HTTP/1.1]
1095243584[7f1c3ff7e4a8]: Host: google.com
1095243584[7f1c3ff7e4a8]: User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:42.0) Gecko/20100101 Firefox/42.0
1095243584[7f1c3ff7e4a8]: Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
1095243584[7f1c3ff7e4a8]: Accept-Language: en-US,en;q=0.5
1095243584[7f1c3ff7e4a8]: Accept-Encoding: gzip, deflate
1095243584[7f1c3ff7e4a8]: Cookie: _P_JAR=2017-10-23-19; NID=114=gIPhw6MV6XhmVhpLt5EpclUrzoSizRptr2gmTB8nWMTyXn_ig33_TmXAh2fKw1pXr1liYSWJLglNYhct2-315E6Kp1gnmPn29wMrzt7mpjUbjNgSu2vKx6mbG; OOPc=5061451-3:
1095243584[7f1c3ff7e4a8]: Connection: keep-alive
1095243584[7f1c3ff7e4a8]:
725608192[7f1c3ff7eda0]: HTTP/1.1 200 OK
725608192[7f1c3ff7eda0]: Content-Type: application/octet-stream
725608192[7f1c3ff7eda0]: Date: Mon, 23 Oct 2017 22:07:46 GMT
725608192[7f1c3ff7eda0]: Expires: Fri, 27 Oct 2017 22:07:46 GMT
725608192[7f1c3ff7eda0]: Cache-Control: public, max-age=345600
725608192[7f1c3ff7eda0]: Server: ocsp_responder
725608192[7f1c3ff7eda0]: Content-Length: 463
725608192[7f1c3ff7eda0]: X-XSS-Protection: 1; mode=block
725608192[7f1c3ff7eda0]: X-Frame-Options: SAMEORIGIN
725608192[7f1c3ff7eda0]:
725608192[7f1c3ff7eda0]: