

Data Forensics

"Analyzing the
Tracks of an Intruder"

or

"Analyzing Administrative
Responses to Log Anomalies"

Tye Stallard

Outline

- Motivation
 - Administration of applications is important
- Background
- Issues
- Approach
- Further research

Approaches

- Audit trail examination
 - Aggregation of low level data into higher level abstractions
 - Difficult to convincingly subvert
- Application log examination
 - Similar to debugging
 - Given anomalous behavior, find cause
- "In theory there is no difference between theory and practice. In practice there is."

Formal auditing model

- Bishop
 - A computer is in one of many states.
 - Some states are within the security policy
 - Some states are outside the security policy
 - Others are indeterminate
 - Audit records document state transitions

Application level logging

- A large amount of state information is summarized
- Interpretation of "standard log entries" depends on implementation
- Information recorded depends on application
- Configurability depends on application

Administration Issues

- Aggravating
 - Logging integrity unreliable
 - Too much unimportant data
 - Authenticity poor
 - "I didn't put that there!"
 - Various levels of granularity
- Mitigating
 - Demonstrated policy violation exists

Assumption

- Consistent system administration practices are a predictor of a secure system
 - Consistent host administration over time
 - Consistent network administration over many hosts
 - Administrative process
 - Documented
 - Repeatable
 - Measurable

Why web servers?

- HTTP is dominate
 - Most IP is TCP and most TCP is HTTP
- HTTP is becoming a common transport platform for applications
 - Because TCP:80 is open on firewalls!
 - Handy GUI
- Apache
 - a common application
 - sophisticated logging capabilities

Web services

- Web protocols
 - IETF: WEBDAV(deltav)
 - W3C: WEBI, WDDX, XMI, Jabber
 - See salcentral.com
- Standards
 - UDDI - Universal Description Discovery & Integration
 - WSDL - Web Services Description Language
 - SOAP - Simple Object Access Protocol
 - XML - Extensible Markup Language

Trust over the network

- Systems used to be closed/static
- Web client/server trust variable
 - Anonymous, remote, transient
 - Strongly authenticated, standalone system
- "Web services" are highly integrated into applications
- More of the application is subject to hostile environment
 - Unknown clients have access to details of internal data structures

Apache logging configuration

- Modules
 - mod_log_config
 - mod_status
 - mod_info
 - mod_usertrack
- Directives
 - CustomLog
 - TransferLog
 - ScriptLog (CGI)

Common Sources of Application Information

- Apache logs
 - error.log
 - access.log
 - rewrite.log
 - ssl.log
- Operating system
 - Syslogd
 - Filesystem (MAC)

Apache Phases

1. URI -> Filename translation
2. Auth ID checking
3. Auth access checking
4. Access checking other than auth
5. Determining MIME type of the object requested
6. Future use
7. Actually sending a response back to the client.
8. Logging the request

Administrator's actions

- Logs are admin's input
- Actions are admin's output
- Identify problems before the system is r00t3d!
- What is reasonable admin practice to react to anomalies?
- What evidence exists that admin is finding cause of anomalies?

Problem

- Locate evidence of admin actions
- What are examples of actions?
 - Update software
 - Removal of unused software
 - Log rotation
 - Log analysis
 - Adjusting log levels
- Derived from Saltzer's and Schroeder's Design Principles

Example

- User downloads and saves a web page
- User changes value of HIDDEN variable
- User submits form (uploads data)
- Module handles that form fails
- Apache records status code 500
- Apache admin disables module or page

Sanctum's web vulnerabilities

- hidden manipulation
- cookie poisoning
- application buffer overflow
- stealth commanding
 - (shell escape)
- parameter tampering
- cross site scripting
- forceful browsing
- backdoor and debug options
- third party misconfigurations and known vulnerabilities

WeBDAV

- Apache module (mod_dav)
- One operating system account (apache)
 - All web files are readable and writeable
- Many WeBDAV accounts
 - ACLs managed by application
 - SDBM stores all properties

Server errors

- "500" Internal Server Error
- "501" Not Implemented
- "502" Bad Gateway
- "503" Service Unavailable
- "504" Gateway Time-out
- "505" HTTP Version not supported

access.log

- 192.168.50.4 - -
[01/Jun/1997:05:28:50 -0700]
"GET /cgi-bin/phf?Qalias=x%0a
cat+/etc/shadow HTTP/1.0" 200
87

error.log

```
1. Jun  1 00:29:13 localhost  
httpd[19665]: [error]  
[client 192.168.50.2]  
attempt to invoke directory  
as script: /var/www/cgi-bin
```