Securing Network Audit Logs on Untrusted Machines

Bruce Schneier

schneier@counterpane.com

Counterpane Systems

101 East Minnehaha Parkway, Minneapolis, MN 55419

(612) 823-1098

Fax: (612) 823-1590

RAID

Louvain-la-Neuve

15 September 1998

WHAT'S THE PROBLEM?

- **Audit logs are essential for forensics.**
- **Audit logs often must be kept on untrusted machines.**
- **We would like to make these audit files secure:**
  - **unalterable**
  - **unreadable**

WHAT'S THE SOLUTION?

- **Use hash chains to detect modifications of audit logs.**
- **Use encryption to keep audit logs confidential.**
- **Use cross-logging to prevent single points of failure.**

MORE INVOLVED STATEMENT OF THE PROBLEM

- **We have an untrusted machine, U:**
  - **Which is not physically secure or sufficiently tamper-resistant to guarantee that it cannot be taken over by some attacker.**
  - **Which needs to be able to build and maintain a file of audit log entries.**
- **We have a trusted machine, T:**
  - **Which interacts minimally with U.**
- **Note that while U is "untrusted," it isn't generally expected to be compromised. However, it is a possibility.**

WHAT WE WANT

- **To make the strongest security guarantees possible about the authenticity of the logs on U.**
- **In particular, we do not want an attacker who gains control of U at time t to:**
  - **Be able to read log entries made before time t.**
  - **Be able to undetectably alter or delete log entries made before time t.**

APPLICATIONS

- **U is an electronic wallet; T is a trusted computer at a bank.**
- **U is a firewall; T is a more-trusted computer on the network.**
- **U is an intrusion-detection system; T is a more-trusted computer on the network.**
- **U is a digital camera; T is a secure evidence-gathering facility.**
- **U is a portable computer; T is a trusted central computer.**
- **U is a set-top box; T is a trusted content provider.**

LIMITS ON THE USEFUL SOLUTIONS

- **No secuity measure can protect audit log entries written after an attacker has gained control of U.**
- **If there is a reliable, high-bandwidth channel between T and U, then there is no problem.**
- **No cryptographic method can prevent the deletion of log entries.**
  - **Physical methods are beyond the scope of this research.**
- **In a sense, this technique is an engineering trade-off between how "offline" U is and how often we expect U to be compromised.**

A Description of Our Method

- **U and T initially share a secret key. This key is used to create the logfile.**
- **Four basic security ideas:**
  - **1. The log's authentication key is hashed after each log entry is written. The new authentication key overwrites and irretrievably deletes the previous key.**
  - **2. Each log entry's encryption key is derived, using a one way function, from the authentication key.**

- **3. Each log entry contains an element in a hash chain that serves to authenticate the values of the previous log entries.**
- **4. Each log entry contains its own permission mask. This allows partially trusted users to view only some kinds of entries.**

Protocols in the Paper

- **Startup: Creating the Logfile**
  - **Requires interaction between T and U.**
- **Creating a New Log Entry**
- **Closing the Logfile**
- **Validating the Logfile**
- **Verification and Querying of Entries by Partially-Trusted Verifiers**

Cross Peer Linkages: Building a Hash Lattice

- **If there are multiple instances of U, they can cross-link their audit logs with each other.**
- **In applications where there are many instances of T and with different instances of U authenticating their log files with different instances of T, this cross-linking can make back-alteration to audit logs impractical.**
- **Details are in the paper.**

Replacing T with a Network of Insecure Peers

- **It is possible to run this scheme with multiple instances of U taking the place of a trusted T.**
- **Probabilistic security.**
- **Details are in the paper.**

Conclusions

- **It is much harder to prevent attacks than to detect them.**
- **Detecting attacks is not enough, you need to gather enough forensic evidence to convince a neutral third party.**
- **Secure and trusted audit logs are key to forensics.**

Full paper can be found at:
http://www.counterpane.com/secure-logs.html

CRYPTO-GRAM is a free monthly e-mail newsletter. Subscribe at:

http://www.counterpane.com