How Do You Know? Using an integrity checker to verify system binaries.

John F. Rovert

9 December, 2000

How do you know if any of the system binaries supplied for your Operating System has not been modified due to an attack or other intrusion? This paper will describe a "Best practices" plan to setup and use Tripwire as a host-based "early warning detection" system.

Assumptions

1. That the vendor did not make any errors during the creation of the installation media
2. The binaries on the media are correct.

If these assumptions can be made; then you have a baseline to compare the sizes and computed checksums of the operating system binaries. That is, if you have the original binary checksums. Surveying the major vendors of Unix operating systems, Compaq (Digital Electronic Corp), IBM, Hewitt-Packard, Silicon Graphics/Cray and Sun Microsystems, note Linux vendors where not surveyed, only Sun has system checksums available for public query.

Installing Tripwire

Tripwire developed by now Gene H. Kim and Gene H.Spafford will be used to track any changes in the size or the computed checksums of the Operating System binaries. The Academic Release Version 1.3.1 of Tripwire is used as a baseline for this paper. The source code was obtained from Purdue University.

Once the source code has been obtained and unpacked it is ready to be compiled. First you should edit the ~/include/config.h file to set values specific to your site. These include the following lines:

```
#include "../configs/<your specific OS configuration header file>

#define CONFIG_PATH <path to the tripwire binary file>

#define DATABASE _PATH <path to the tripwire datafile to be created>
```

Before you compile the Tripwire source code you must be logged in as root, this is so the necessary files can be written to system areas.

To compile Tripwire once you are at root just enter the command "make". This will compiled the Tripwire source code for your specific system (assuming you have made the correct changes to the ~/include/config.h file).

Now enter the command "make test" to have Tripwire run its bulit-in test suite. If no errors were encountered during the compilation and running of the tests you are now ready to begin running Tripwire.

Running Tripwire

This is an excellent start, however, it is the opinion of this author that the configuration file that Tripwire uses should not be modified until all software has been installed.

The initial run of Tripwire should include all nine of the checksums that are supplied with Tripwire, this will give nine different checksums for each file on the system and if any file changes one or more of the computed checksums will differ from the original. The following command will execute the Tripwire program in initialization mode to create the initial database for the specific system.

```
<path to tripwire binary>/tripwire –init
```

Once this has been accomplished, if you are setting up a Sun system, you should extract the MD5 checksums from the database generated by Tripwire and compare these calculated values to the values supplied by The Solaris&trade; Fingerprint Database; the Sun database contains the MD5 checksums for the specific SunOS binary files. Any differences between the calculated values and the values returned from the The Solaris&trade; Fingerprint Database should be regarded, as suspicious and further investigation would be warranted.

If no differences werefound, installation of all of the recommended and security related patches supplied by the vendor may be installed. Once these have been installed, rerun Tripwire, using the below command, to track any changes made to any file on the system.

```
<path to tripwire binary>/tripwire
```

When Tripwire finishes review the log file for any changes and rerun Tripwire in update mode to recreate the specific checksums for any file that has changed via the installation of the recommended and security related patches. Make a copy of this database, label it and store it in a secured area for use in comparing at a later date.

```
for i in <list of files that changed>

do

<path to tripwire binary>/tripwire –update $i

done
```

where $i is the complete path and file name of the file(s) that have changed

Continue this cycle of installing software and rerunning Tripwire until all software packages have been installed. Once this has been completed and the intermediate log files reviewed and Tripwire run in update mode to recreate the checksums of modified files, then and only then should you modify the Tripwire configuration file to run and track changes to files.

Stephen Northcutt describes in his text "Network Intrusion Detection An Analyst's Handbook"

> *The best way to apply tripwire is to run it in initialize mode over the entire file system. Copy that database to removable media and store it in your desk drawer, leaving the original on the server. Next edit the file systems that you run tripwire in and restrict the run to core directories,/,/etc,/usr,/usr/sbin, and so on; these files should not change often!*

The Tripwire configuration file will list all files or directories of files to be checked for modification whenever is Tripwire run. Files that should be checked include:

- Any root (/) level "dot" files .rhosts, .profile etc.
- Any system start up files (rc.*)
- Any application binary that has been installed
- Any compiler, linker and associated libraries

- /etc/hosts
- /etc/aliases (mail aliases)
- /etc/services
- /etc/passwd and /etc/shadow files
- /opt (for any optional OS components installed)

It is upto the management to decide how often Tripwire should be run but it would be a good idea to run it at daily and make sure the log file is reviewed and any changes questioned.

The Tripwire log files will show not only the checksums of the files specified in the configuration file but also attributes of the files that may include

- permission and file mode bits
- inode number
- number of links
- user id of owner (UID)
- group id of the owner (GID)
- size of file
- access timestamp
- modification timestamp
- inode creation/modification timestamp
- nine fields of signatures

    1. null sig
    2. MD5
    3. Snefru
    4. CRC-32
    5. CRC-16
    6. MD4
    7. MD2
    8. SHA
    9. Haval
    10. reserved

These additional attributes may be turned off via command line options however it would be ill advised to do so since if something does change this information may be of use to track down the exact cause or who made the change.

References

Rivest, Ronald L. "Request for Comments: 1321" http://www.faqs.org/rfcs/rfc1321.html April 1992.

Kim, Gene H. "Sigfetch Manual Page" sigfetch(8) October 1992.

Kim, Gene H. and Spafford Gene H. "Tripwire Manual Page" tripwire(8) October1992.

Kim, Gene H. and Spafford Gene H. "Tripwire Configuration Manual Page" tw.config(5) October 1992.

Kim, Gene H. and Spafford Gene H. "The Design of a System Integrity Monitor: Tripwire" Department of Computer Sciences, Purdue University CSD-TR-93-071; COAST TR 93-01; 1993. https://www.cerias.purdue.edu/techreports-ssl/public/93-01.ps

Kim, Gene H. and Spafford Gene H. "Experiences with Tripwire: Using Integrity Checkers for Intrusion Detection" PROCEEDINGS OF THE SYSTEMS ADMINISTRATION, NETWORKING AND SECURITY CONFERENCE III (SANS); Washington DC COAST TR 94-03; 1994. https://www.cerias.purdue.edu/techreports-ssl/public/94-03.ps

Kim, Gene H. and Spafford Gene H. "Writing, Supporting, and Evaluating Tripwire: A Publically Available Security Tool" PROCEEDINGS OF THE USENIX UNIX APPLICATIONS DEVELOPMENT SYMPOSIUM; pp. 89-107; Toronto, ON; COAST TR 94-04; 1994. https://www.cerias.purdue.edu/techreports-ssl/public/94-04.ps

Rivest, Ronald L. http://theory.lcs.mit.edu/~rivest/homepage.html

MD5 Homepage (unofficial). http://userpages.umbc.edu/~mabzug1/cs/md5/md5.html

Northcutt, Stephen. "Network Intrusion Detection An Analyst’s Handbook" 1999.

Tripwire Security Systems Inc. http://www.tripwiresecurity.com.