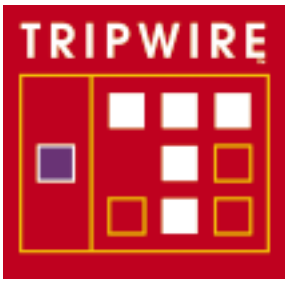

Intrusion Detection System 1.3 for UNIX®

"Used world wide by government agencies, as well as small companies to many Fortune 500 corporations, Tripwire®, is the most widely deployed intrusion detection security tool for the Unix® market."

Tripwire® Intrusion Detection System 1.3 for UNIX® (IDSU/1.3) is a system integrity checker, a utility that compares properties of designated files and directories against information stored in a previously generated database. Any changes to these files are flagged and logged, including those that were added or deleted. When run against system files on a regular basis, any changes to a critical system file will be detected, and appropriate damage control measures can be taken immediately. With Tripwire IDS, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes.

Tripwire IDS 1.3 for UNIX

Features	Benefits
Proven Secure	• An industry standard, Tripwire has been used since 1992 • Officially recommended by CERT and CIAC
Thorough	• Can inspect every file on your system • Built-in high and low speed modes can allow high frequency checking
Compliments perimeter security	• Defense-in-Depth security coverage by working seamlessly with firewalls and other perimeter solutions.
Diverse operating system support	• Including Sun, HP, Linux
Year 2000 compliant	• Will not incur errors caused by wrapping the century date
Easy to read reports	• Easy to read saving valuable time
Analyzes all objects on OS	• Provides complete and accurate inventory changes - Forensic and post mortem analysis - Validation during system restoration process • Detects errors from malfunctioning hardware, virus activity, internal interfaces malicious and even accidental changes • Detects misuse and abuse of privilege
One way signatures	• Detects changes without compromising data confidentiality • Industry standard signatures(MD5, SHA)
Easily scalable	• From one, to tens of thousands of computers

Why You Need an Intrusion Detection Policy

As a system administrator, lets say you run a network of 50 networked UNIX computers from nearly a dozen vendors — including Sun workstations running Solaris and SunOS, PCs running Linux, and a Cray running Unicos . This morning, you were a bit surprised when the lastlog message indicated that root had logged into the system at 3AM. Especially since you thought you were the only one with the root password!

You are faced with one of the most tedious and frustrating jobs a system administrator can have — determining which, if any, files and programs have been altered without authorization. File modifications may occur in a number of ways: an intruder, an authorized user violating local policy or controls, or even the rare piece of malicious code altering system executables as others are run. It might even be the case that some system hardware or software is silently corrupting vital system data.

In each of these situations, the problem is not so much knowing that things might have been changed; rather, the problem is verifying exactly which files — out of tens of thousands of files in dozens of gigabytes of disk on dozens of different architectures — might have been changed. Not only is it necessary to examine every one of these files, but it is also necessary to examine directory information as well.

The Tripwire IDS System

The Tripwire IDS integrity checking scheme has a high level of automation — both in generating the output and the input list of files. If the scheme is difficult to use, it may not be used often enough — or worse, turned off. Tripwire IDS includes a simple way to describe portions of the filesystem to be traversed.

Additionally, in cases where files are likely to be added, changed, or deleted, Tripwire IDS makes it easy to update the checklist database. Some files may change daily or weekly. It should not be necessary to regenerate the entire database every time a single file changes to maintain database accuracy.

Tripwire IDS' integrity checking program can be run regularly to enable detection of file changes in a timely manner. It also is possible to run the program manually to check a smaller set of files for changes. Tripwire IDS is easy to invoke and use, as the administrator is likely to compare the differences between the base checklist and the current file list frequently.

Tripwire IDS generates output that is easy to scan. A checker generating three hundred lines of output from each machine for the system administrator to analyze daily would be self-defeating — this is far too much to ask of even the most amazingly dedicated system administrator! The program allows the specification of filesystem exceptions that can change without being reported, and hence reduce noise. For example, changes in system log file sizes are expected, but a change in inode number, ownership, or file modes is cause for alarm. Properly specified, Tripwire IDS operates unobtrusively, notifying you when a file changes outside the specified bounds, and otherwise running quietly.

Tripwire Support

E-mail support is available for customers who have purchased Tripwire IDS, as per their license agreement. To purchase the latest release of Tripwire IDS, contact the VCC offices at (503) 223-0280.

System Requirements

The following are required to run Tripwire IDS:

- C compiler, lex, yacc, make (for source release distributions)

The following operating systems are supported:

- Sun Solaris (SPARC)
- Sun Solaris (Intel)
- Sun SunOS
- HP HP/UX
- IBM AIX
- DEC OSF/1
- FreeBSD
- NetBSD
- BSDI BSD/386
- Linux
- SGI Irix
- Sequent Dynix
- Sequent Ptx
- Convex
- Cray UNICOS
- Mach
- DEC Ultrix
- SCO

Distributed By

visual computing corporation

The Berg Building
615 SW Broadway
Second Floor
Portland, OR 97205

Tel: 503.223.0280
Fax: 503.223.0182

www.visualcomputing.com/tripwire/