Libsklog Documentation

Release 0.1

Paolo Smiraglia

May 17, 2012

CONTENTS

This is the documentation for Libsklog 0.1, last updated May 17, 2012.

ONE

INTRODUCTION

Libsklog is a C library which allows users to create logentries according to the scheme defined by B. Schneier and J. Kelsey in Secure Audit Logs to Support Computer Forensics. This document will illustrate you about how to install the library under Linux systems, how to configure the environment and finally how to use it.

To get more information, to notify a bug or more in general to contact me, please send an email to paolo.smiraglia@polito.it

CONTENTS

2.1 Installation

In this section is shown the procedure to install the library and to configure the environment. All steps are described assuming that the library installation prefix ($PREFIX) is:

```
/usr/local
```

2.1.1 Get Sources and Install Library

Before proceeding with the installation, several dependencies need to be resolved::

```
Libtool
Autoconf
OpenSSL >= 0.9.8
SQLite 3.x
libuuid
libconf
libjansson
```

Get the sources from GitHub repository:

```
mkdir ~/temp
cd ~/temp
git clone https://github.com/psmiraglia/Libsklog.git libsklog
```

Generate ./configure script (usually only the first time):

```
cd libsklog
autoreconf --install --force --verbose
```

Run ./configure script using the option –enable-debug (strongly recommended). Other options are available, to see them run:

```
./configure --help
```

Build and install the library:

```
./configure --enable-debug
make
make install (as root)
```

If you are Debian addicted, you can use "checkinstall" instead of "make install". In this way a .deb package will be created and installed.:

```
./configure --enable-debug
make
checkinstall (as root)
```

2.2 Configuration

2.3 API Reference

2.3.1 SKLOG_U APIs

```c
#include <stdio.h>

int main (void) {
        printf("Hello, world!!!");
        return 0;
}
```

2.3.2 SKLOG_T APIs

2.3.3 SKLOG_V APIs

2.4 Tutorial

INDICES AND TABLES

- *genindex*
- *modindex*
- *search*