




Tripwire: an Introduction

Dan Bunker - @ejsuncy 

BYU yHack

11 Feb 2015

How I stole my first client

Client's old webhost's email to me (don't do this):

Here is the login for <http://academic.willulead.com>

folder: /var/www/vhosts/willulead.com/academic

username: willulead

password: OYdNm3ayWsJQunK7Wg34!

Me, on the road home after break, with a hotspot:

```
ejsuncy$ ssh willulead@academic.willulead.com
ejsuncy$ screen
ejsuncy$ cat /etc/passwd
```

I just wanted to upload my public rsa key to the .ssh/authorized_keys file in my home folder!

/etc/passwd identifies each user's home folder

The next day...

Someone has been doing illegal stuff on the server. It was compermized. [REDACTED]

For now I won't be able to give you access until I can find out more.

FYI, Someone tried to gain root access to the server using the willulead login.

There is a list of files [REDACTED]

that have to go through that have been determined suspicious [REDACTED]

by the Rackspace team. I just don't have the time at the moment to go through them.



← **‘the website guy’**

“he wants to create a whole new website on a new server. And if you are interested he would like you to take over and be his website guy.”

Raised Questions

How could `ejsuncy$ cat /etc/passwd` trigger a security alert?

How does it automagically generate a list of “suspicious files”?

How can I tell which files have been compromised?

Tripwire

“Systems intruders will often use trojan binaries for login, su, ps, and ls, etc. to cover their tracks and keep a low profile on the system.”

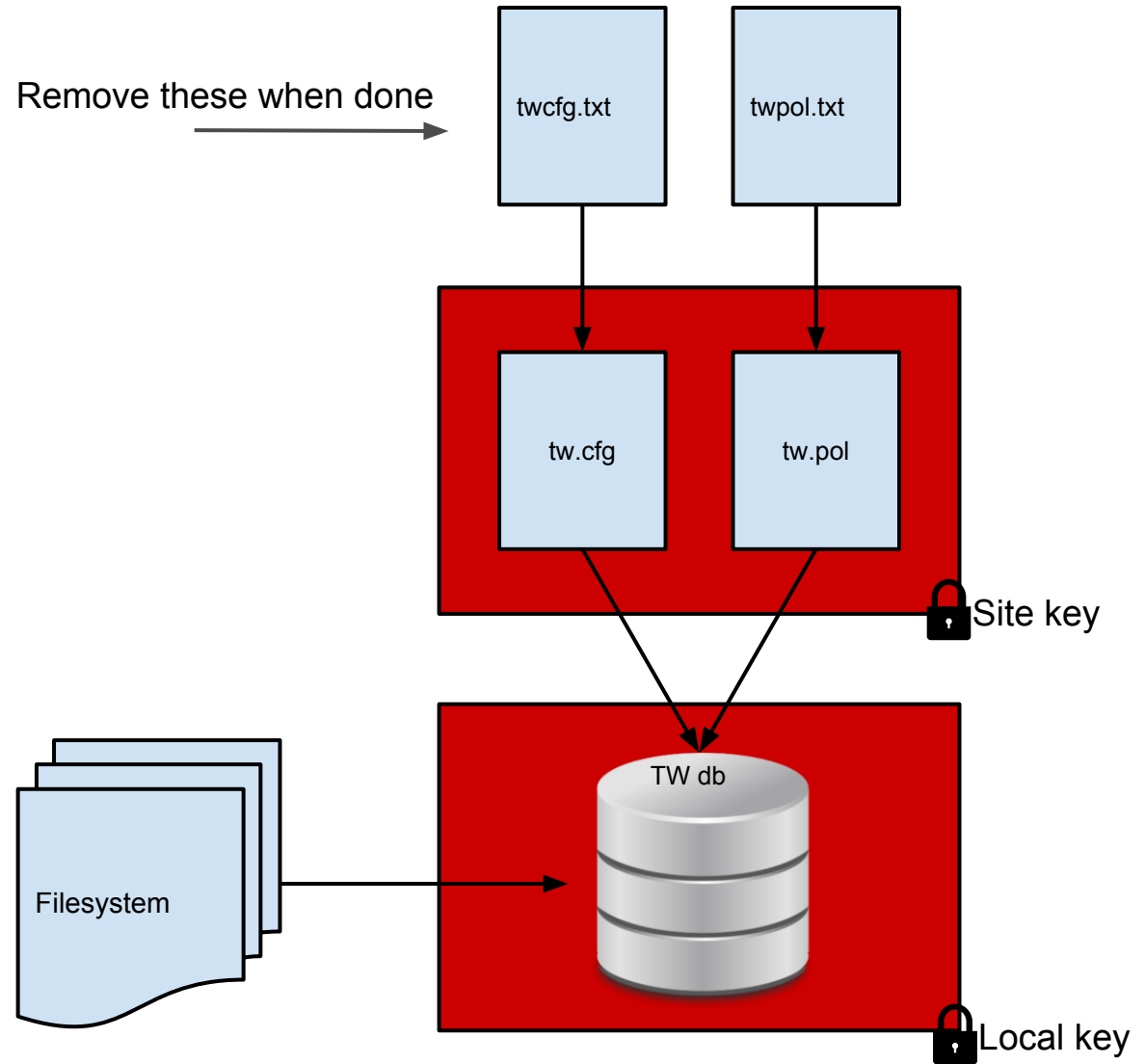
Tripwire

- uses strong checksum method similar to MD5
- should be installed ASAP after OS installation! (but after setting hostname, FQDN, etc)

Tripwire

- periodically verifies the integrity of a server's file systems
- keeps a database of checksums on the file stats of critical system files

Overview



Tripwire Setup on Ubuntu

- Download fresh copy of Ubuntu
- apt-get update && apt-get upgrade
 - start with a clean, updated system
- Set hostname, FQDN if applicable
 - tripwire uses these and might need to be reinstalled if these are changed
- apt-get install tripwire
 - sudo

Tripwire Installation

- Configure postfix for your needs
 - Internet Site worked for me
 - Email notifications

Package configuration

Postfix Configuration

Please select the mail server configuration type that best meets your needs.

No configuration:
Should be chosen to leave the current configuration unchanged.

Internet site:
Mail is sent and received directly using SMTP.

Internet with smarthost:
Mail is received directly using SMTP or by running a utility such as fetchmail. Outgoing mail is sent using a smarthost.

Satellite system:
All mail is sent to another machine, called a 'smarthost', for delivery.

Local only:
The only delivered mail is the mail for local users. There is no network.

General type of mail configuration:

No configuration
Internet Site
Internet with smarthost
Satellite system
Local only

<Ok> <Cancel>

Tripwire Installation

- Again, make sure hostname/FQDN is correct

Package configuration

Postfix Configuration

The "mail name" is the domain name used to "qualify" _ALL_ mail addresses without a domain name. This includes mail to and from <root>: please do not make your machine send out mail from root@example.org unless root@example.org has told you to.

This name will also be used by other programs. It should be the single, fully qualified domain name (FQDN).

Thus, if a mail address on the local host is foo@example.org, the correct value for this option would be example.org.

System mail name:

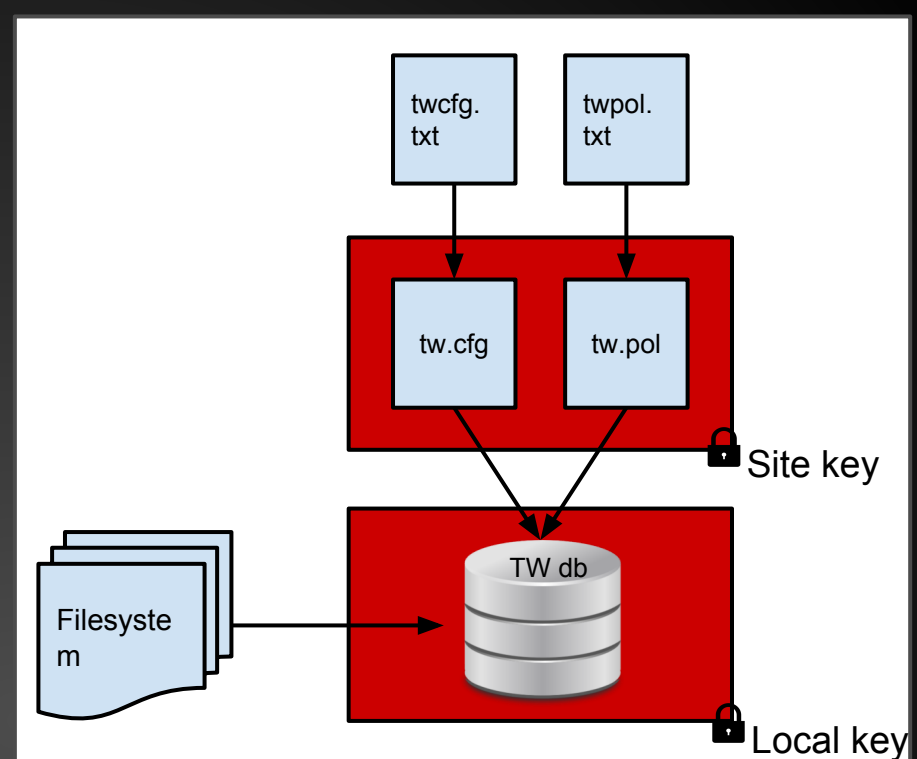
twdemo

<Ok>

<Cancel>

Tripwire Installation

- Site key
 - signs config files
 - signs policy files
 - used across many systems
- Local key
 - signs tripwire db
 - used on one system



Package configuration

Tripwire Configuration

Tripwire uses a pair of keys to sign various files, thus ensuring their unaltered state. By accepting here, you will be prompted for the passphrase for the first of those keys, the site key, during the installation. You are also agreeing to create a site key if one doesn't exist already. Tripwire uses the site key to sign files that may be common to multiple systems, e.g. the configuration & policy files. See `twfiles(5)` for more information.

Unfortunately, due to the Debian installation process, there is a period of time where this passphrase exists in a unencrypted format. Were an attacker to have access to your machine during this period, he could possibly retrieve your passphrase and use it at some later point.

If you would rather not have this exposure, decline here. You will then need to create a site key, configuration file & policy file by hand. See `twadmin(8)` for more information.

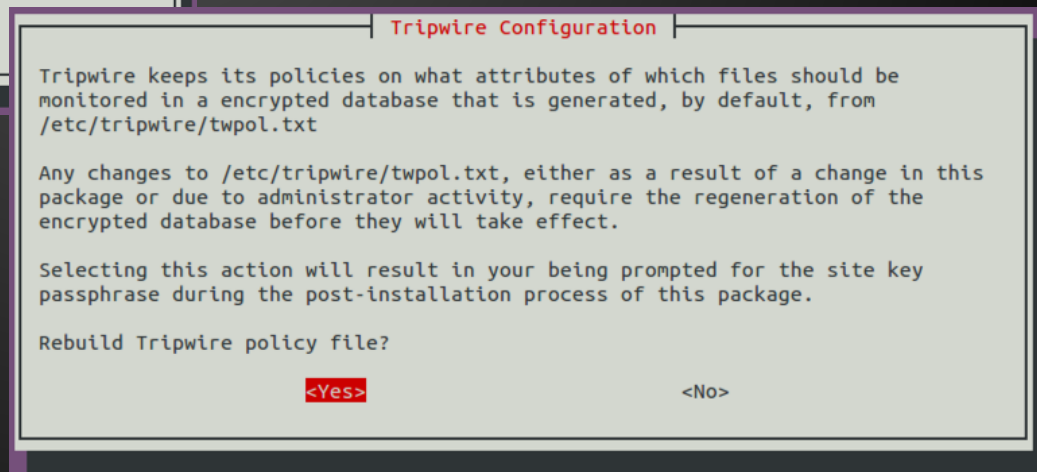
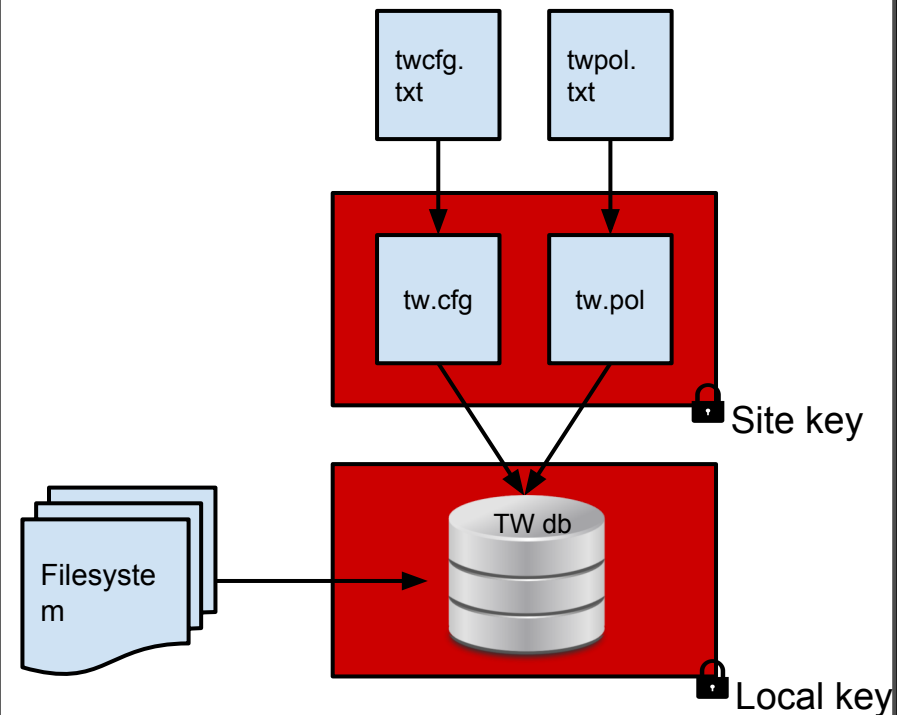
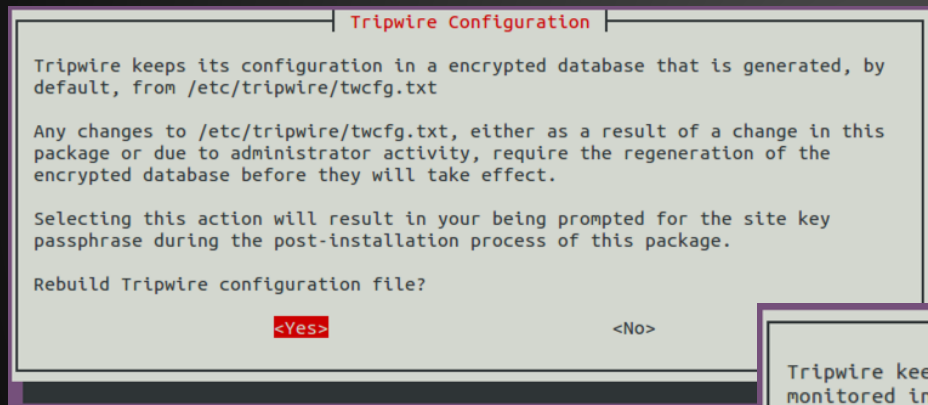
Do you wish to create/use your site key passphrase during installation?

<Yes>

<No>

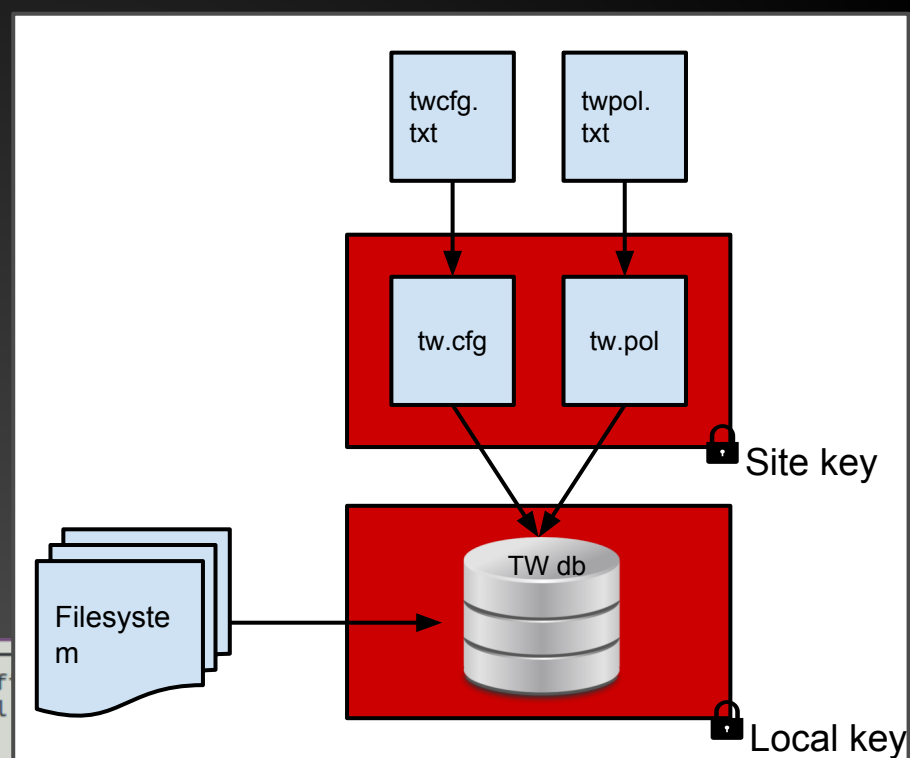
Tripwire Installation

- generate twcfg.txt
- generate twpol.txt



Tripwire Installation

- Set site & local key passphrases



Get site passphrase

Tripwire uses two different keys for authentication and encryption of files. The site key is used to protect files that could be used across several machines. This includes the policy and configuration files.

You are being prompted for this passphrase either because no site key exists at this time or because you have requested the rebuilding of the policy or configuration files.

Remember this passphrase; it is not stored anywhere!

Enter site-key passphrase:

<Ok>

Get local passphrase

Tripwire uses two different keys for authentication and encryption of files. The local key is used to protect files specific to the local machine, such as the Tripwire database. The local key may also be used for signing integrity check reports.

You are being prompted for this passphrase because no local key file currently exists.

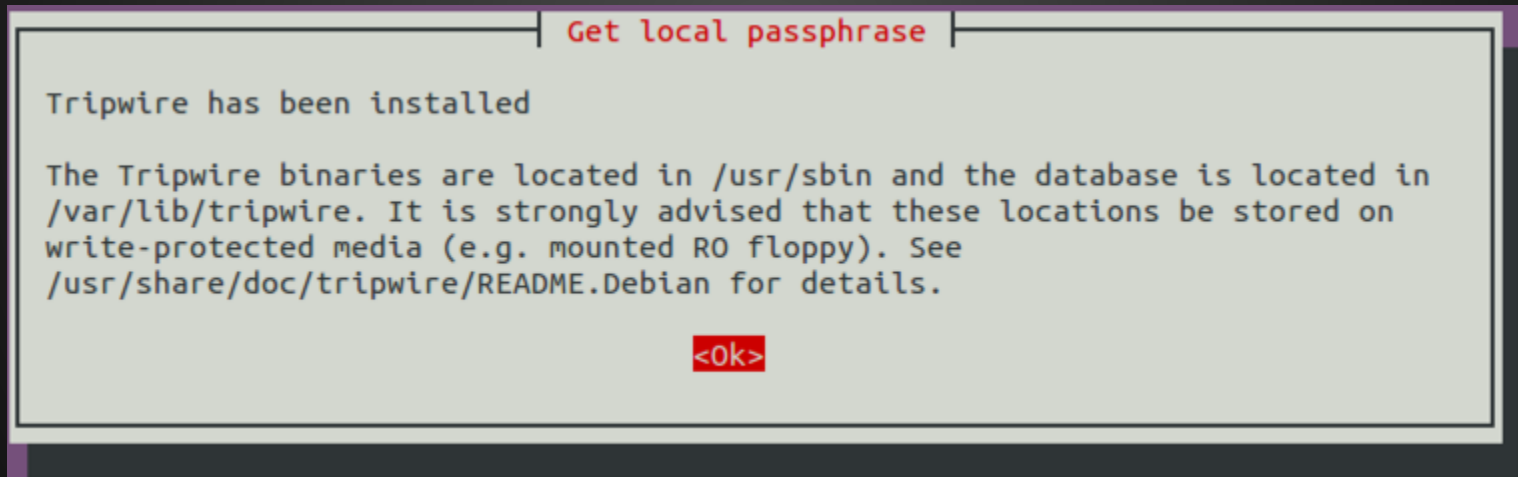
Remember this passphrase; it is not stored anywhere!

Enter local key passphrase:

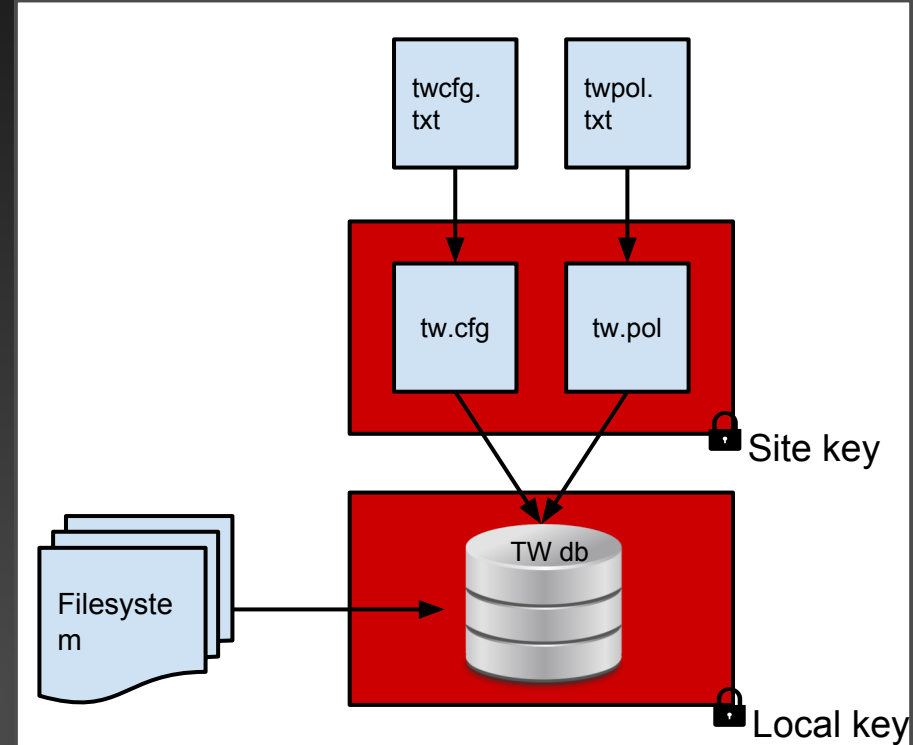
<Ok>

Tripwire Installation

- Done!



Tripwire Initialize & Configure



- `sudo -i`
- `twadmin -m P /etc/tripwire/twpol.txt`
 - encrypt/install the default policy file
- `tripwire -m i`
 - encrypt/initialize the db
 - `-m i`: initialization mode
 - `-m c`: check mode (will be used later)
- Lots of false positives!

Tripwire Customize (remove false positives)

- `tripwire -m c | grep Filename >> twtest.txt`
- `edit /etc/tripwire/twpol.txt`
 - comment out files that appear in `twtest.txt`

```
(
  rulename = "Root config files",
  severity = 100
)
{
    /root                                -> $(SEC_CRIT) ; # Catch all additions
    #/root/mail                          -> $(SEC_CONFIG) ;
    #/root/Mail                          -> $(SEC_CONFIG) ;
    #/root/.xsession-errors              -> $(SEC_CONFIG) ;
    #/root/.xauth                        -> $(SEC_CONFIG) ;
    #/root/.tcshrc                       -> $(SEC_CONFIG) ;
    #/root/.sawfish                      -> $(SEC_CONFIG) ;
    #/root/.pinerc                       -> $(SEC_CONFIG) ;
    #/root/.mc                           -> $(SEC_CONFIG) ;
    #/root/.gnome_private                 -> $(SEC_CONFIG) ;
    #/root/.gnome-desktop                 -> $(SEC_CONFIG) ;
    #/root/.gnome                        -> $(SEC_CONFIG) ;
    #/root/.esd_auth                     -> $(SEC_CONFIG) ;
    #/root/.elm                          -> $(SEC_CONFIG) ;
    #/root/.cshrc                        -> $(SEC_CONFIG) ;
    /root/.bashrc                        -> $(SEC_CONFIG) ;
    #/root/.bash_profile                 -> $(SEC_CONFIG) ;
    #/root/.bash_logout                  -> $(SEC_CONFIG) ;
    /root/.bash_history                  -> $(SEC_CONFIG) ;
```

Tripwire Customize (remove false positives)

- Also remove lock files (everything under /var/lock/subsys), pid files (/var/run)
- Optional:
 - /var/log files, depending on log rotation configuration
 - /dev/pts/0 for remote shell

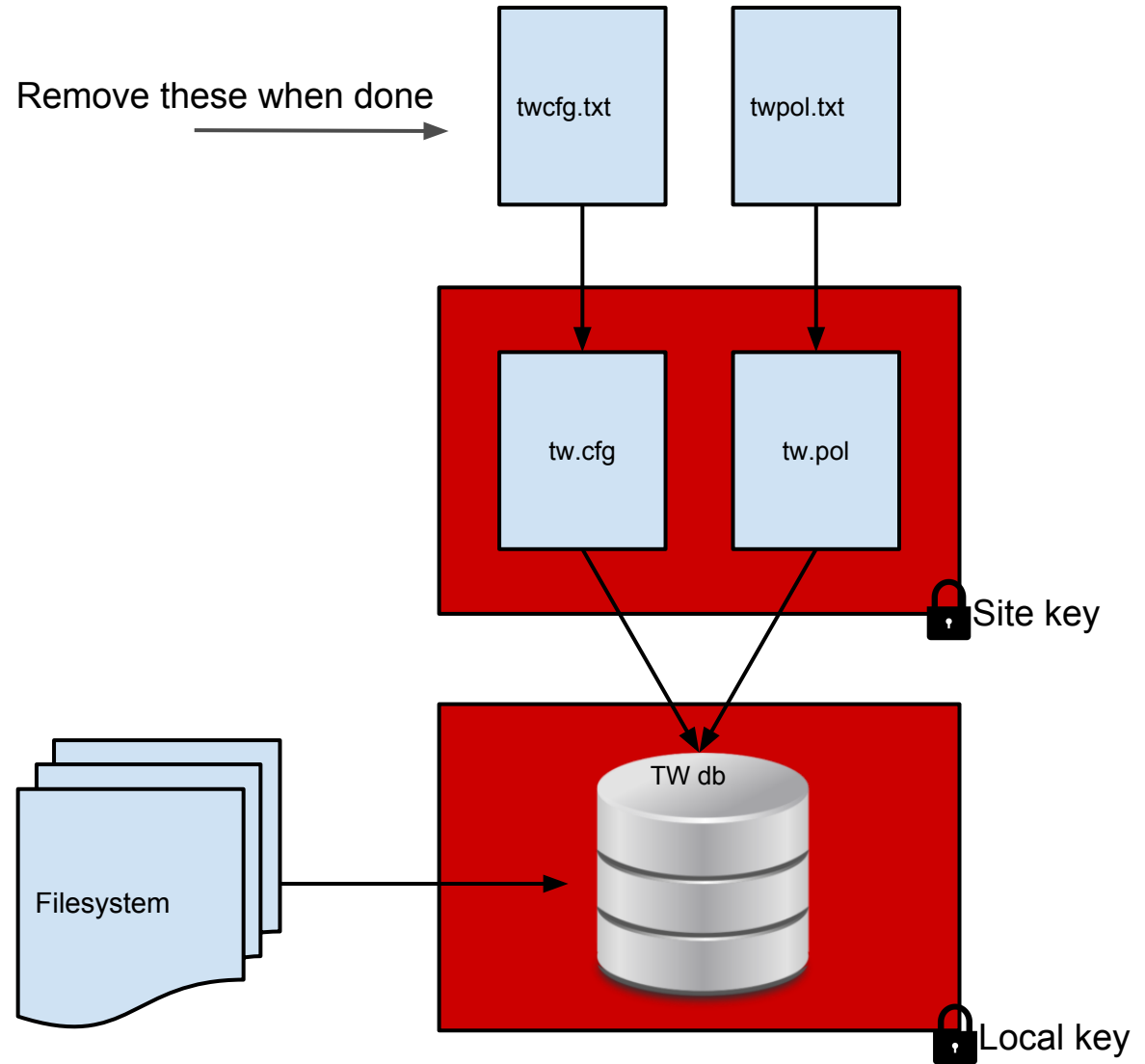
Tripwire Finalization

- Double check:
 - `tripwire -m c | grep Filename >> twtest.txt`
- Install edited policy:
 - `twadmin -m P /etc/tripwire/twpol.txt`
- Recreate database:
 - `tripwire -m i`
- DELETE cleartext policy and config files!
 - `rm /etc/tripwire/twcfg.txt /etc/tripwire/twpol.txt`
 - you can always get them back with a passphrase
 - `twadmin -m p > /etc/tripwire/twpol.txt`

Using Tripwire

- `tripwire --check`
 - produces report
- `tripwire --check --interactive`
 - place an 'x' next to each fs change you made
 - provide local password
 - updates database
- try installing mailutils
 - `sudo apt-get install mailutils`
 - run a tripwire interactive check and update database
- setup cron job to email your report (3:30am)
 - `sudo crontab -e`
 - `30 3 * * * /usr/sbin/tripwire --check | mail -s "Tripwire report for `uname -n`" your_name@email.com`

Recap



Discussion

- Pros

- catches bugged binaries/trojans
- catches file & dir access time changes

- Cons

- doesn't catch
 - cat /etc/shadow (cat doesn't update unix atime)
- but does catch
 - vi /etc/shadow (vi writes a .swp file to /etc while editing file, changing access time of /etc)

Modified:
[x] "/etc"

Object Detail:

Section: Unix File System

Rule Name: Other configuration files (/etc)
Severity Level: 66

Modified Objects: 1

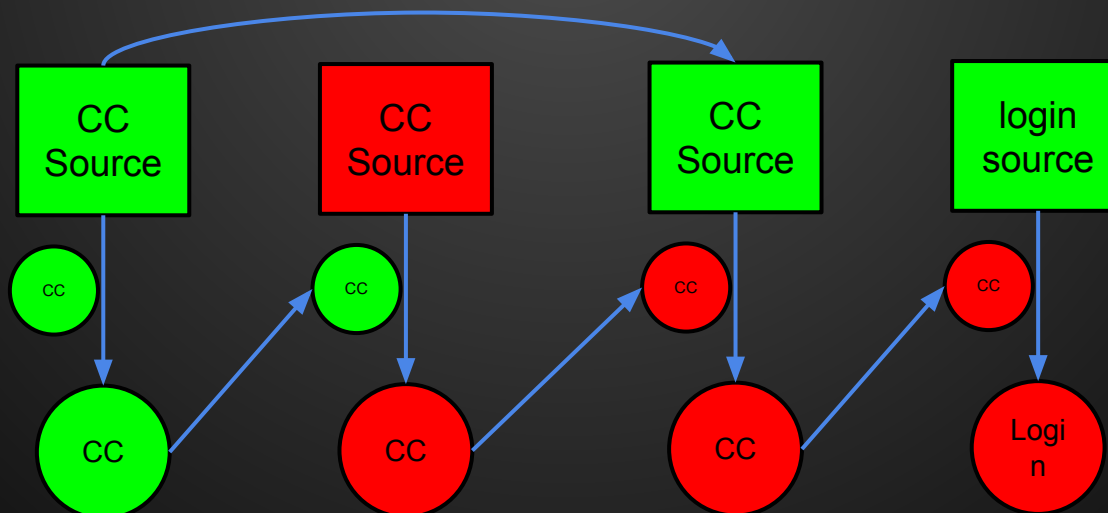
Modified object name: /etc

Property:	Expected	Observed
Object Type	Directory	Directory
Device Number	51713	51713
Inode Number	393218	393218
Mode	drwxr-xr-x	drwxr-xr-x
Num Links	97	97
UID	root (0)	root (0)
GID	root (0)	root (0)
Size	4096	4096
* Modify Time	Wed Feb 11 12:03:12 2015	Wed Feb 11 12:14:52 2015
Blocks	8	8

Usage Example

Ken Thompson gave an ACM Turing Award lecture when he received it, and he described a C Compiler hack:

“First we compile the modified source with the normal C compiler to produce a bugged binary. We install this binary as the official C. We can now remove the bugs from the source of the compiler and the new binary will reinsert the bugs whenever it is compiled. Of course, the login command will remain bugged with no trace in source anywhere.”



(Re) Sources

- [Introductory article](#)
 - (if that doesn't work) [cached version](#)
- [Basic Tutorial and Configuration](#)
- [Installation & Advanced Configuration Tutorial](#)
- [Sourcecode \(sourceforge.net\)](#)
- Ken Thompson's lecture
 - [*Reflections on Trusting Trust*](#)