Open source laptop tracking and recovery

ADEONA

If you use a laptop, you have a good chance of having it lost or stolen. Learn about Adeona, a reliable open source system that can help you locate your lost or stolen laptop.

BY RUSS MCREE

If you search on the term "laptop" at the DATALOSS db site [1], you'll see announcements such as "160,000 notified that personal information is on stolen laptop" or "Social Security numbers and names of about 60,000 on stolen laptops."

This same search at The Data Breach Blog [2] will produce additional shock thanks to headlines like "Laptops stolen from TSA contractor contain personal information of 3,930" or "Stolen laptop contains personal data of 800,000 Gap job applicants."

Other recent news headlines have included the loss of PII (Personally Identifiable Information) for 190,000 employees on stolen Anheuser-Busch laptops, or a Stanford laptop containing data concerning 72,000 current or former employees.

Ponemon Institute conducted a study in July 2008 on behalf of Dell that determined that 800,000 laptop are misplaced by users each year as they pass through airports [3], a number that used to describe all laptop thefts globally. Even more significant is the fact that approximately half of the professionals surveyed for the Ponemon study admitted that they carry confidential company information.

Ultimately, this study indicates that approximately 63-million laptops were purchased worldwide in 2008. If we use the commonly assumed estimate that one in ten laptops are stolen each year, and 20 percent are lost or misplaced, then no fewer than 6,300,000 laptops ended up in the wrong hands last year.

Consider these statistics and then think about this: If you use a laptop, you stand a very good chance of losing it or having it stolen. Furthermore, FBI statistics indicate that as few as 2 percent of lost or stolen laptops will ever be recovered.

Adeona

Adeona [4] is the private, reliable, open source system for tracking the location of your lost or stolen laptop. With no dependency on a proprietary, central service, Adeona only needs to be installed on your laptop to help increase your sense of mobile device safekeeping. Additionally, Adeona ensures your privacy via advanced cryptographic methodology, allowing only the owner – or the owner's agent – to use the system to track a lost or stolen laptop.

Adiona [5], the Roman goddess of safe returns, lends her name to this remarkable open source offering. If you treat your laptop as your child, you'll appreciate knowing that Adiona is believed to watch over children and bring them home safely, and also to protect travelers.

Adeona utilizes the open source OpenDHT [6] (distributed hash table) distributed storage service to store location updates sent from the Adeona client you install on your laptop, which continually monitors the current location of your laptop and gathers data such as IP addresses and local network topology that is used to identify its current location. Again, keep in mind that the Adeona client then uses strong cryptographic methodology to encrypt the location data and ensure that the ciphertexts stored with the OpenDHT service are anonymous and unlinkable, while also making it is easy for a laptop owner to retrieve location information.

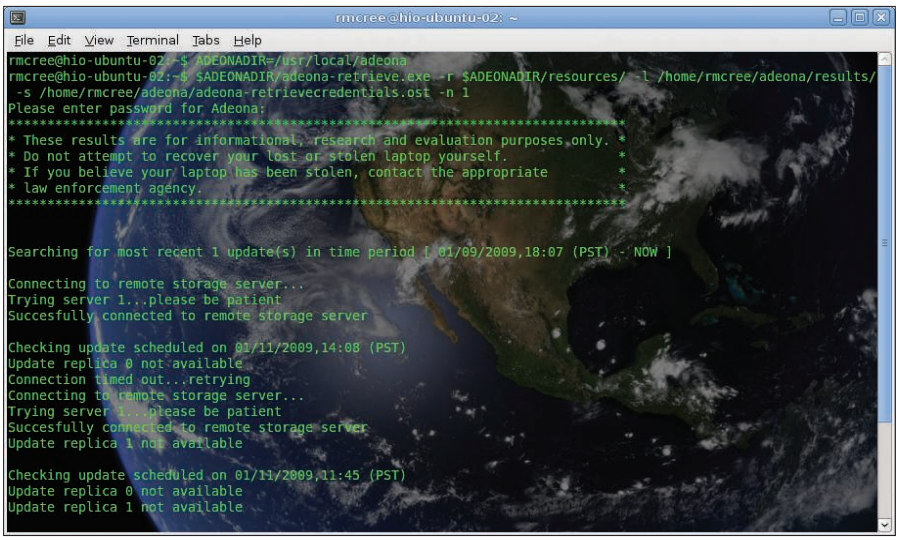

Figure 1: Retrieve your data from the remote storage server.

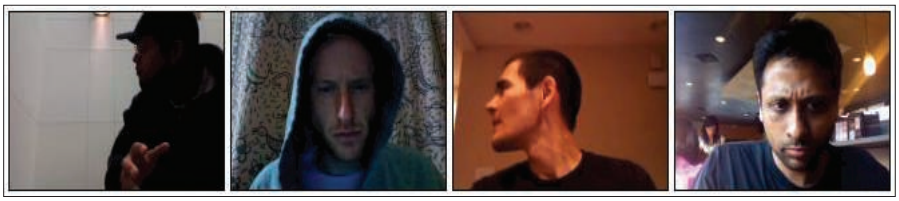

Figure 2: Actual Mac bandits as captured by Adeona (image from the Adeona Project homepage).

In this article, I'll start with Adeona installation and retrieval, and then I'll look at the science behind the system.

Installation

Regardless of your operating system, Adeona installation is straightforward. According to the online Adeona installation notes, it has been built and tested on multiple Linux flavors including Ubuntu, Fedora, Gentoo, and even the XO laptop (One Laptop per Child). I conducted installations on Ubuntu systems; be sure to check for dependencies: OpenSSL, traceroute, cron, and the optional iwconfig. To install Adeona, run:

```
$ tar xzf adeona-0.2.1.tar.gz
$ cd adeona/
$ ./configure
$ sudo make install
```

By default, the installer script will install Adeona in /usr/local/adeona. To make sure it runs during system startup, the Adeona client program relies on cron:

```
$ sudo crontab -e
```

This command will open root's crontab file so you can add the entry for the Adeona client. Note that the install script will print out the necessary crontab entry so you can just copy and paste it. Be sure you add this crontab entry for Adeona, otherwise the client will not run the next time you reboot.

The crontab entry for Adeona is comprised of:

```
@reboot $INSTALLDIR/adeona-client ➥
.exe -s $INSTALLDIR/adeona-➥
clientstate.cst -r $INSTALLDIR/ ➥
resources/ -l $INSTALLDIR/logs/ &
```

The trailing ampersand (&) is necessary to prevent the parent /bin/sh from lingering while the client is running. Although I did not test an installation on a 64-bit system, there are some compatibility issues that are resolved by compiling with the *-m32* flag, which is easily achieved by locating the *CFLAGS* variable in the *Makefile* and adding the *-m32* flag to it.

On some Debian-based systems, you might need 32-bit versions of the required libraries via getlibs (for example, *getlibs -l libcrypto.a*). Errors you might encounter could result from an absence of the C libraries or OpenSSL routines and headers. Resolve these via:

```
$ sudo apt-get ➥
install build-essential
```

or:

```
$ sudo apt-get ➥
install libssl-dev
```

After agreeing to the terms of the GPL (and assuming all dependencies are met), you'll be prompted for a password. To protect your location-finding credentials, please pick a password for Adeona; it does not need to be the same as your login password. Remember to add the Adeona crontab entry after committing your password.

Don't forget to make a backup copy of your location-finding credentials:

```
adeona-retrievecredentials.ost
```

The installer drops a copy of *adeona-retrievecredentials.ost* on your Desktop. Next, email it to yourself, or better yet, put it on a portable memory device (USB, SD, etc.). If you must, write down the contents given that they are protected by the password you established during the installation process.

To help prevent timing attacks, Adeona utilizes pseudo-randomly scheduled updates. Thus, you might not be able to retrieve any location information as stored in OpenDHT until at least one hour after installation.

Warning

Do not attempt to recover your lost or stolen laptop yourself. If you think your laptop has been stolen, contact the appropriate law enforcement agency.

Retrieval

Because the necessary binaries are included in client installation packages,

Listing 1: Retrieval example

```
01 info: ======== start location data
   =========
02 update time: 01/03/2009,23:48 (PST)
03 internal ip: 192.168.248.101
04 external ip: 67.40.1.228
05 access point: <NOT TELLING>
06 Nearby routers:
07 no routers found
08 info: ========= end location data
   ==========
```

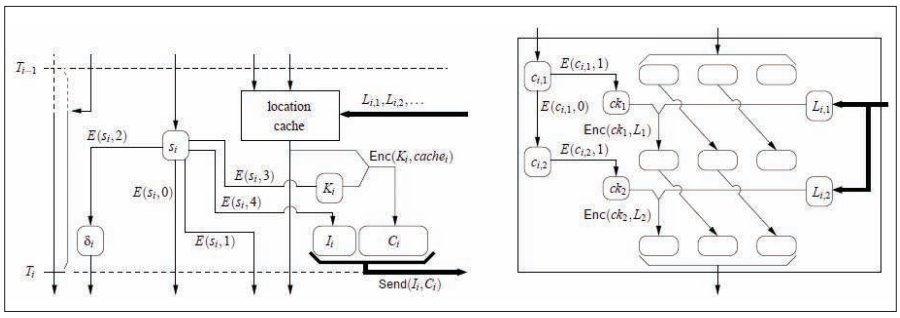

Figure 3: (Left) The Adeona core, where E is a block cipher (e.g., AES) instantiating the FSPRG and Enc is a standard encryption scheme. (Right) Close-up of the core's forward-private location caching.

retrieval is very simple on all systems. Logic dictates, however, that you'll be conducting retrieval from a different system than the one on which you installed your original client.

After installation, retrieval is achieved via the following commands:

```
ADEONADIR=/usr/local/Adeona
```

The command

```
$ADEONADIR/adeona-retrieve.exe ➥
-r $ADEONADIR/resources/ ➥
-l /path/to/results/ ➥
-s /path/to/your/➥
adeona-retrievecredentials.ost -n 1
```

retrieves the most recent location given the encrypted location-finding credential file. Figure 1 shows retrieval on my test system. Had I not attempted retrieval so soon after installation on this particular system, I might have received results like Listing 1.

If I were a thief using this laptop at a coffee shop or a library, the laptop owner would likely retrieve a specific access point – an IP address that can be geo-located by law enforcement – and additional router data.

Adeona offers an additional feature for Mac users that takes advantage of the built-in iSight camera [7]. With isight-capture incorporated, the Mac OS X version of Adeona gives you the option to capture pictures of the laptop user or thief. Rest assured that images are also privacy-protected; only the laptop owner (or the owner's agent) can access them (Figure 2).

Science Behind Adeona

According to the project lead's paper from 17th USENIX Security Symposium [8], the client consists of two modules: a location-finding module and a cryptographic core.

The paper says, "With a small amount of state, the core utilizes a forward-secure pseudorandom generator (FSPRG) to efficiently and deterministically encapsulate updates.

The core ensures forward-privacy: a thief, after determining all of the internal states of the client and even with access to all data on the remote storage, cannot use Adeona to reveal past locations of the device. The owner, with a copy of the initial state of the client, can efficiently search the remote storage for the updates.

The cryptographic core uses only a sparing number of calls to AES per update." Figure 3 details forward-secure pseudorandom generator (FSPRG) methodology.

Future Development

I can't think of a single reason why you shouldn't install Adeona on your laptop. For that matter, you might want to install it on your desktop PCs and your servers. Although they're less likely to walk off than your laptop, they could be stolen. Be sure to store the unique .ost file for each device safely, somewhere other than the device to which it belongs. Future development might even lead to Adeona clients for mobile devices such as iPhones.

The project leads have also indicated the prospect of adding functionality to send authenticated commands back to the laptop (for example, delete sensitive data). OpenDHT, the remote storage service, would act as a private, anonymous intermediary for relaying communication between the laptop and its owner. Further engineering might include hardening the Adeona client via kernel-level support or even hardware support,to be significantly more resistant to thieves attempting to disable it.

Conclusion

You'll want to keep a close eye on this project – the benefits for enhancing laptop security are obvious, and the roadmap toward support for other devices looks promising. May your laptop remain in your possession at all times but, should that fail, may Adeona bless it with many safe returns. ■

INFO

[1] DATALOSS db: *http://datalossdb.org/*

[2] The Data Breach Blog: *http://breach.scmagazineblogs.com/?s=laptop*

[3] "Study: 800,000 laptops lost each year in airports," by Stevie Smith: *http://www.thetechherald.com/article.php/200831/1604/Study-800-000-laptops-lost-each-year-in-airports*

[4] Adeona: *http://adeona.cs.washington.edu/index.html*

[5] Adiona: *http://www.thaliatook.com/OGOD/adiona.html*

[6] OpenDHT: *http://www.opendht.org/*

[7] iSight CLI image capture: *http://www.intergalactic.de/pages/iSight.html*

[8] "Privacy-Preserving Location Tracking of Lost or Stolen Devices: Cryptographic Techniques and Replacing Trusted Third Parties with DHTs": *http://adeona.cs.washington.edu/papers/adeona-usenixsecurity08.pdf*

THE AUTHOR

Russ McRee, GCIH, GCFA, CISSP, is a security analyst, researcher, and founder of holisticinfosec.org, where he advocates a holistic approach to the practice of information assurance. Russ conducts constant vulnerability and malware research and currently works for Microsoft Online Service's Security Incident Management team. A frequent speaker at industry events, Russ also writes *toolsmith*, a monthly column for the ISSA Journal, and has written for numerous other publications, including *Information Security*, *(IN)SECURE*, *Sys Admin*, and *OWASP*. Russ thanks Tadayoshi Kohno and Tom Ristenpart, Adeona project leads, for their contributions to this article.