Appendix A

Developing the Tool Platforms to Test the Thesis

This is an appendix to:
author = {David Ross},
title = {{Securing IEEE 802.11 Wireless LANs}},
school = {Queensland University of Technology},
month = {dec},
year = {2008},
type = {{PhD} thesis},
address = {Information Security Institute and the School of Information Technology, QUT, Brisbane, QLD, Australia},
note = {Draft (unpublished)}

This author's choice of the *Red Hat / CentOS / Fedora* OS family is described in subsection 5.5.2 of Chapter 5. A reader wishing to replicate these experiments may well prefer a *Debian* distribution or a derivative, such as *Ubuntu*, or some other Unix-like OS, since command-line and basic GUI operations are the same on any distribution.

The following describes the set-up on a Fedora distribution and may not involve identical commands and configuration on other systems.

A.1 Preparation, Installation and Configuration of the Tools

On the 29th March 2008, the initial preparations were commenced for the development of the simulation tools. Once a stable platform has been prepared, originally *Fedora 7* in this case, the set up of *ns-2* proceeded as follows. Version *ns-2.32* was initially chosen, but was immediately replaced by *ns-2.33*, being the most current stable release, as at 31st March 2008. The "*ns-allinone-2.29.3*" version was not used as the *ns-2.3x* versions contained required wireless additions for this work.

A.1.1 Preparing the Environment

The first step was to check that the development environment was complete and install any missing tools.

```
rpm -q wget
rpm -q gcc-c++
rpm -q libX11-devel
rpm -q xorg-x11-proto-devel
rpm -q libXt-devel
rpm -q libXmu-devel
```

A.1.2 Download and Install Tcl/Tk

Next *Tcl* and *Tk* and Object-oriented-Tcl, *OTcl* were prepared. The latest releases of *Tcl* and *Tk* were 8.5.2 and the latest *OTcl* was 1.13. These were obtained, compiled and installed as follows.

```
cd /usr/src
wget http://prdownloads.sourceforge.net/tcl/tcl8.5.2-src.tar.gz
wget http://prdownloads.sourceforge.net/tcl/tk8.5.2-src.tar.gz
wget http://prdownloads.sourceforge.net/otcl-tclcl/otcl-src-1.13.tar.gz
tar xzvf tcl8.5.2-src.tar.gz
tar xzvf tk8.5.2-src.tar.gz
tar xzvf otcl-src-1.13.tar.gz
cd /usr/src/tcl8.5.2/unix
./configure
```

```
make
make install
cd /usr/src/tk8.5.2/unix
./configure
make
make install
cd /usr/src/otcl-1.13
```

A.1.3 Installation Issues

At this point configure repeatedly failed for *OTcl*, while trying to find the *Tcl* binaries. Both

```
./configure
```

and

```
./configure --with-tcl=/usr/local/bin/tclsh8.5
```

or any other permutation failed.

Version *otcl-1.13* was released 10th March 2007. All of these tools were downloaded and being prepared over a year later on 29th March 2008. The *Tcl/Tk* version 8.5.2 had only been released the day before, on 28th March 2008. It seemed likely that the year-old *OTcl* was incompatible with the new versions of *Tcl* and *Tk*.

It was decided to try reverting to *Tcl/Tk* version 8.4.14, from 19th October 2006 — a version verified to work for current *ns-2* sources. The reversion proceeded as follows.

```
cd /usr/src/tk8.5.2/unix
make distclean
cd /usr/src/tcl8.5.2/unix
make distclean
cd /usr/local/bin
rm -f tclsh* wish*
cd /usr/local/include
rm -f tcl* tk*
cd /usr/local/lib
rm -rf tcl* tk* libtcl* libtk*
cd /usr/local/man/man1
```

```
rm -f tclsh* wish*
cd /usr/local/man/man3
rm -f Tcl* Tk* TCL* Ttk*
```

Next, the version 8.4.14 sources for *Tcl* and *Tk* were obtained, compiled and installed, as follows.

```
cd /usr/src
wget http://prdownloads.sourceforge.net/tcl/tcl8.4.14-src.tar.gz
wget http://prdownloads.sourceforge.net/tcl/tk8.4.14-src.tar.gz
tar xzvf tcl8.4.14-src.tar.gz
tar xzvf tk8.4.14-src.tar.gz
cd /usr/src/tcl8.4.14/unix
./configure
make
make install
cd /usr/src/tk8.4.14/unix
./configure
make
make install
```

Then, *OTcl* version 1.13 was successfully compiled and installed as follows.

```
cd /usr/src/otcl-1.13
./configure
(NOT ./configure --with-tcl=/usr/share/tcl8.4.14/ as in some examples.)
vi Makefile
line 31 change
INST_OLIBSH=    NONE/lib
to
INST_OLIBSH=    /usr/local/lib
make install
```

A.1.4 Download and Install TclCl

Next, a *Tcl/C++* interface, called *TclCL*, for "Tcl with CLasses", was needed to provide the *Tcl/C++* interface for *ns-2* and *nam*. Version 1.18 was used.

```
cd /usr/src
```

```
wget http://downloads.sourceforge.net/otcl-tclcl/tclcl-src-1.18.tar.gz
tar xzvf tclcl-src-1.18.tar.gz
cd tclcl-1.18
./configure --with-tcl=/usr/src/tcl8.4.14/
make
make install
```

A.1.5 Download and Install ns-2, nam and xgraph

Finally, *ns-2* and *nam*, along with optional David Harrison's *xgraph*, were built as follows.

```
cd /usr/src
wget http://downloads.sourceforge.net/nsnam/ns-2.33.tar.gz
wget http://downloads.sourceforge.net/nsnam/nam-src-1.13.tar.gz
wget http://downloads.sourceforge.net/nsnam/xgraph-12.1.tar.gz
tar xzvf ns-2.33.tar.gz
tar xzvf nam-src-1.13.tar.gz
tar xzvf xgraph-12.1.tar.gz
cd ns-2.33
./configure
make
make install
echo 'export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/lib:' > /etc/p
rofile.d/ns.sh
chmod 0733 /etc/profile.d/ns.sh
```

After the installation, a clean boot with all the new libraries was performed and the simulator was tested as follows.

```
$ ns
% set ns [new Simulator]
_o4
% ^C
```

Then *nam* was built.

```
cd /usr/src/nam-1.13
./configure
make
make install
```

Then check the *nam* console starts.

```
nam
```

Lastly, *xgraph* was built.

```
cd /usr/src/xgraph-12.1
./configure
make
make install
```

Initially, the *Fedora 7* OS was chosen both for its currency over the very stable *CentOS* (a re-compiled community version of RHEL) and its stability over the latest release, at that time, of *Fedora 8* (a *Red Hat* sponsored community *Linux* project). As *ns-2* is compiled against the current running kernel, the frequency of kernel upgrades has considerable impact on research activity involving the simulator. By not being the latest release, at that time, *Fedora 7* was likely to have less frequent kernel upgrades and thus provide a longer mean time between full compilations of the software. However, as the research progressed, *Fedora 7* fell too far behind in development, presenting unsupported packages and a general security risk and so it was decided to move to *Fedora 9*.

A.2 Platform-Specific Issues

Soon after the move to *Fedora 9*, in late August 2008, the *Fedora* software repositories were penetrated and the *Fedora GPG*[1] software signing keys may have been compromised [125]. This prompted the issue of new keys and a new package repository for both *Fedora 8* and *Fedora 9*. *Fedora 7*, being no longer supported, was not included in this process. The possibly compromised keys are listed here.

- RPM-GPG-KEY-fedora (4F2A6FD2),
- RPM-GPG-KEY-fedora-test (30C9ECF8),
- RPM-GPG-KEY-fedora-extras (1AC70CE6), and
- RPM-GPG-KEY-legacy (731002FA).

The key change involved upgrades to the latest *PackageKit* (0.2.5-1.fc9 i386) and a new *fedora-release* (9-5.transition noarch) with new .repo files pointing to the new repositories, but signed with the old key, in the old *updates* repository.

[1] *GNU Privacy Guard* (*GnuPG* or *GPG*).

This update then loads the new .repo files pointing to the new repositories on old systems accepting the old key, such that any subsequent updates point to the new *updates-newkey* and *updates-testing-newkey* repositories.

```
================================================================================
 Package                 Arch       Version          Repository        Size
================================================================================
Updating:
 PackageKit              i386       0.2.5-1.fc9      updates           561 k
 PackageKit-libs         i386       0.2.5-1.fc9      updates           106 k
 fedora-release          noarch     9-5.transition   updates            34 k
 gnome-packagekit        i386       0.2.5-2.fc9      updates           1.1 M
 yum-packagekit          i386       0.2.5-1.fc9      updates            11 k

Transaction Summary
================================================================================
Install      0 Package(s)
Update       5 Package(s)
Remove       0 Package(s)
```

For any case where the original .repo files have been modified, this update leaves two rpmnew .repo files as follows:

```
warning: /etc/yum.repos.d/fedora-updates.repo created as /etc/yum.repos
.d/fedora-updates.repo.rpmnew
warning: /etc/yum.repos.d/fedora.repo created as /etc/yum.repos.d/fedor
a.repo.rpmnew
```

These can then be modified if desired and moved over the active files.

```
mv /etc/yum.repos.d/fedora-updates.repo.rpmnew /etc/yum.repos.d/fedora-
updates.repo
mv /etc/yum.repos.d/fedora.repo.rpmnew /etc/yum.repos.d/fedora.repo
```

However, as all future updates were to come from the *updates-newkey* and *updates-testing-newkey* repositories, this was not required.

The next update then points to the new repositories, signed with the new keys listed here:

- RPM-GPG-KEY-fedora-8-and-9-primary (6DF2196F) and
- RPM-GPG-KEY-fedora-test-8-and-9-primary (DF9B0AE9)

The new keys are then imported as required during the normal update process.

```
warning: rpmts_HdrFromFdno: Header V3 DSA signature: NOKEY, key ID 6df2
196f
Importing GPG key 0x6DF2196F "Fedora (8 and 9) <fedora@fedoraproject.or
g>" from /etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-8-and-9-i386
Is this ok [y/N]:
```