Backdooring X11 with class

Matias Katz
@matiaskatz
matias@matiaskatz.com

Andsec Security Conference

End of November 2015

Buenos Aires, Argentina

www.andsec.org

An idea back in 1995...

Locking a computer
using hardware

An idea back in 1995...

mkit | IT & Security Solutions

2 steps:

1) Find a way to read a device

2) Find a way to lock a computer

An idea back in 1995...

mkit IT & Security Solutions

Step 1

Filesystem? NO

UUID? YES

Reading the device

mkit IT & Security Solutions

2 steps:

1) “/dev/disk/by-id/” enrollment

2) Check if present each 0.1s

Locking the computer

mkit IT & Security Solutions

Step 2

DBUS

Locking the computer

mkit | IT & Security Solutions

DBUS:

- IPC software
- Apps communication
- SW and HW interruptions

Locking the computer

mkit IT & Security Solutions

DBUS:

- Runs with privileges
- Speaks directly to the kernel
- Available in most X Display Managers

Demo “locker.py”

What else to do

- Sound alarm
- Email certain data
- Power off
- Delete private keys
- Encrypt certain files
- Shred entire disk

And then I thought...

Mkit | IT & Security Solutions

Can I unlock a computer using the same method?

Generating a Backdoor

Unlocking a computer

mkit IT & Security Solutions

2 steps:

1) Find a way to unlock a computer

2) Trigger the unlock

A good backdoor

mkit IT & Security Solutions

2 main features:

1) Leave small traces

2) Have a stealth trigger

Unlocking a computer

Unlocking computer leaving small traces:

Binaries? NO

Rootkits? NO

OS features? YES

Unlocking a computer

mkit IT & Security Solutions

Unlocking computer leaving small traces:

DBUS :)

Unlocking a computer

Mkit | IT & Security Solutions

Stealth trigger to unlock:

- Not checked by AVs

- Execution without suspicion

- Available in all computers

Unlocking a computer

Mkit IT & Security Solutions

Stealth trigger to unlock:

Keystrokes? NO

Open port? NO

Hardware? YES

Hardware change

Stealth hardware trigger:

- Respond while locked
- OS must not interfere
- Cannot be disruptive

Hardware change

mkit IT & Security Solutions

Network Connection? NO

Screen brightness? NO

Power input? NO

So?

Audio Jack :)

Playing with audio jack

mkit IT & Security Solutions

- Mechanic detection

- Notifies the OS

- Who checks that?

Playing with audio jack

mkit IT & Security Solutions

2 steps:

1) Read “/proc/asound/card0/codec#0”

2) Check for changes

Playing with audio jack

Demo “jack.py”

(Warning: Playing with the audio jack could damage it)

Playing with audio jack

mkit IT & Security Solutions

Small problem:

What if the victim wants to use the headphones?

Playing with audio jack

Simple solution:

Create a pattern

Playing with audio jack

mkit IT & Security Solutions

2 steps:

1) Set checks each 1s, like “01110”

2) Replicate that with the headphones

Unlocking the computer

Demo “back2.2.py”

The aftertaste

How to mitigate it?

- Remove Dbus (nope)
- Disable screen lock (ugly but ok)
- Switch to a minimal XDM (ok)

The aftertaste

Do you have to run it beforehand?

YES

(that's why it's called a “backdoor” :D)

The aftertaste

Mkit IT & Security Solutions

Can it be persistent?

YES (rc.local)

The aftertaste

How big is it?

20 lines (dirty)

1 line (nice)

The aftertaste

mkit IT & Security Solutions

What's so good about it?

- NO Opcodes

- Undetectable

The aftertaste

```
>>> import
dbus
>>>
```

```
>>> import dbus
Traceback (most recent call last):
  File "<stdin>", line 1, in <module>
ImportError: No module named dbus
>>>
```

The aftertaste

Can you do it to 'root' ?

YES (but...)

The aftertaste

Can you do it on Windows ?

YES

- WinDBus
- COM / RPC / DDE

The aftertaste

Can you *Shellshock* it ?

HELL YEAH (however..)

(Thanks *Chino* for the idea and *Nutrix* for the help implementing)

Backdooring X11 with class

Matias Katz
@matiaskatz
matias@matiaskatz.com