Security Issues for Embedded Devices

Jake Edge
LWN.net
jake@lwn.net
Slides: http://lwn.net/talks/elc2009

Overview

Examples – embedded devices gone wrong

Attack surface

Attacks and attackers

Similarities and differences with “regular” security

Specific security ideas to keep in mind

It's a thinking process

Examples

- Airtel DSL modem – multiple problems
- 3Com OfficeConnect wireless modem/router – authentication bypass password disclosure
- Nokia N95 smartphone – JPEG crashed phone
- Ralinktech wireless drivers – malformed 802.11 probe allowed remote code execution
- SonyEricsson smartphones – malformed WAP Push message crashed the phone
- ...

Attack Surface

The attack surface of a system is the “sum” of the inputs that can be controlled or influenced by untrusted users

It “measures” the system vulnerability potential

Reducing the attack surface is one important way to increase the security of a system

Inputs

“Inputs” includes obvious things like the network and the services provided over the network

It also includes less obvious things: serial ports, USB, flash devices, ...

The least obvious are in some ways the most dangerous

Devices and their attack surface

- Print server – user/admin interface, print jobs
- NAS – network, admin interface
- Voting machine – user interface, data storage, maintenance port
- Home router – admin interface, wifi, WAN
- Television – video inputs?, network?, remote control
- ...

Android ADP1

Obvious inputs – wifi, bluetooth

Less obvious – Cell, GPS receiver

Requires physical access – touchscreen, SD slot, USB, accelerometer?

Attacks

Successful attacks can do different things depending on the device:

- router – capture traffic, reroute DNS queries
- print server – grab sensitive print jobs (budget?)
- voting machine – steal elections
- TV – show more ads, record viewing habits
- phone – steal pictures, contacts, credentials

Attackers

The kinds of attackers will vary based on the kinds of results an attack could bring

Phishing and other money-making schemes likely to attract sophisticated, funded attackers

Also true for targeted attacks (against an individual or company)

Attackers II

Attackers are not necessarily “external” (employees for example), firewall ineffective

The internet is obviously a major source of attacks

Wireless (of all sorts) is particularly dangerous – no access required, hard to detect

Consider the attack surface

It may not be practical or sensible to try to secure all inputs – they should at least be considered

Creating a “threat model” will help you decide

Some threats (physical access, rogue administrator, etc.) may well fall outside of the threat model

What's different about embedded

- Often have attack surfaces other systems don't
- Code is “fixed”, hard to upgrade
- People don't treat them like computers
- Monocultures

What's the same about embedded

- Same programs, protocols, etc. as desktops and servers
- Thus the same vulnerabilities/exploits
- All of the same rules for securing systems

Specific things to look at

- Default and/or easily guessed passwords for admin accounts should be eliminated
- Be especially careful with programs that allow user interaction (web, command line, ssh)
- In-house code may need more scrutiny than code that is already running on many systems
- Need to keep an eye on security alerts and have a strategy for field upgrades

Remove unneeded things

- Protocols – IPv6, SMB, NFS, ...
- Services – telnet, NTP, sshd, SMTP, ...
- User accounts
- Software packages – Perl, C compiler, wget, sendmail, ...
- Minimize kernel configuration
- Minimize the abilities of the inputs to only those that are needed by the application

It's a thinking process

Think beyond the “rules”

Think of how things can be broken, rather than how they will work

Consider attack surface, threat model, and sensitivity of the data or device to make security tradeoffs

Questions?