Understanding Threat Models for Embedded Devices

Jake Edge
LWN.net
jake@lwn.net

Embedded Linux Conference
April 13, 2010

Introduction

- Analyzing threats to a device should be done during the product design phase
- Initial analysis is not based on the software installed on the device
- Potential threats are based on the planned functionality of the device
- Some thought should be given to other uses

Threat model

- Based on the possible threats to a system
- Threats are based on several aspects of the device's intended use
- Once the threats are identified, a subset is targeted to defend
- Impossible to defend against all threats
- Narrowing down the threats to be defended allows developers to prioritize their efforts

What is being protected?

- What data is being protected by or stored on the device?
- Alternatively: what are the consequences for the user if the device is compromised?
- Proper functioning of the device is the most basic – denial of service
- As the value of a compromise increases for an attacker, the attacks get more sophisticated

What is being protected?

- A television or microwave probably has little data of interest to an attacker
- Network router/firewall or storage server either have or protect fairly high-value data
  - Snoop on internet traffic/phone calls/...
  - Drain a bank account through phishing
  - Delete the family photo album
- Basic security tenet: Make the cost of an attack more than the data is worth to an attacker

Inputs

- Inputs are the device's connections to the external world
- Network/wireless are obvious – Bluetooth, cellular voice/data, GPS a bit less obvious
- Remote controls, front panel buttons are still inputs – still vulnerable depending on location
- Weirder stuff: cameras, microphones, USB ...
- The only way into the system is via inputs

Inputs

- All inputs should at least be considered
- May reject attacks against some
  - Require physical access
  - Implausible attack scenarios
  - Implies targeted attack at individual/organization
  - Inputs “walled off” from the rest of the system

Installation location

- Embedded devices may be “installed” in unfriendly environments
  - Often can't assume physical security
  - Even “home” devices can be installed elsewhere
- Internet router/firewall used in coffee shop
- TVs/DVRs installed in bars/restaurants
- Unexpected uses may lead to increased exposure to threats

Users

- Based on the target market, the technical knowledge of the users should be considered
- Non-technical users may use the device in highly insecure ways
  - Connecting devices directly to the internet
  - Sharing much more data than they realize
- Are security updates planned?
  - How are users supposed to find out?
  - Without easy update, more hardening needed

Example: Television

- Low-value data (if any at all)
- Few inputs (HDMI, remote control, front panel)
- Non-technical users
- Installed “everywhere”
- Relatively few security concerns
  - Denial of service via crash
  - Annoying folks with universal remotes (not really an issue that TV makers can be expected to fix)

Example: Home NAS server

- Data is high-value to user, probably low value to attacker (except possibly targeted attacks)
- Network is the only real input (on/off switch)
- Non-technical users
- Generally installed behind router/firewall
  - Could be attacked from inside the network (browser-based or other malware)
  - Might be installed/configured insecurely

Example: Home NAS server

- Attacker could deny access, get ransom
  - Encrypt the contents
  - Disable the device
- Has enough compute power to be used in a botnet
- Could be used to store attacker data
- Common flaw: default admin password
  - Doesn't require the user to change it

Other devices

- A similar analysis can be done *early* in the product development cycle
- Explicitly deciding not to defend against certain kinds of attacks allows developers to focus
  - Customer expectations should be set correctly
  - Security is always about tradeoffs

Conclusion

- Seen as a PR problem, but it is really a customer relations issue
  - Customers that get burned (or hear of others that got burned) won't return
  - Once a reputation for lax security is established, it can be very hard to break (ask Microsoft)
- Starting early allows you to “bake security in” and not try to bolt in on later