Embedded Systems Security

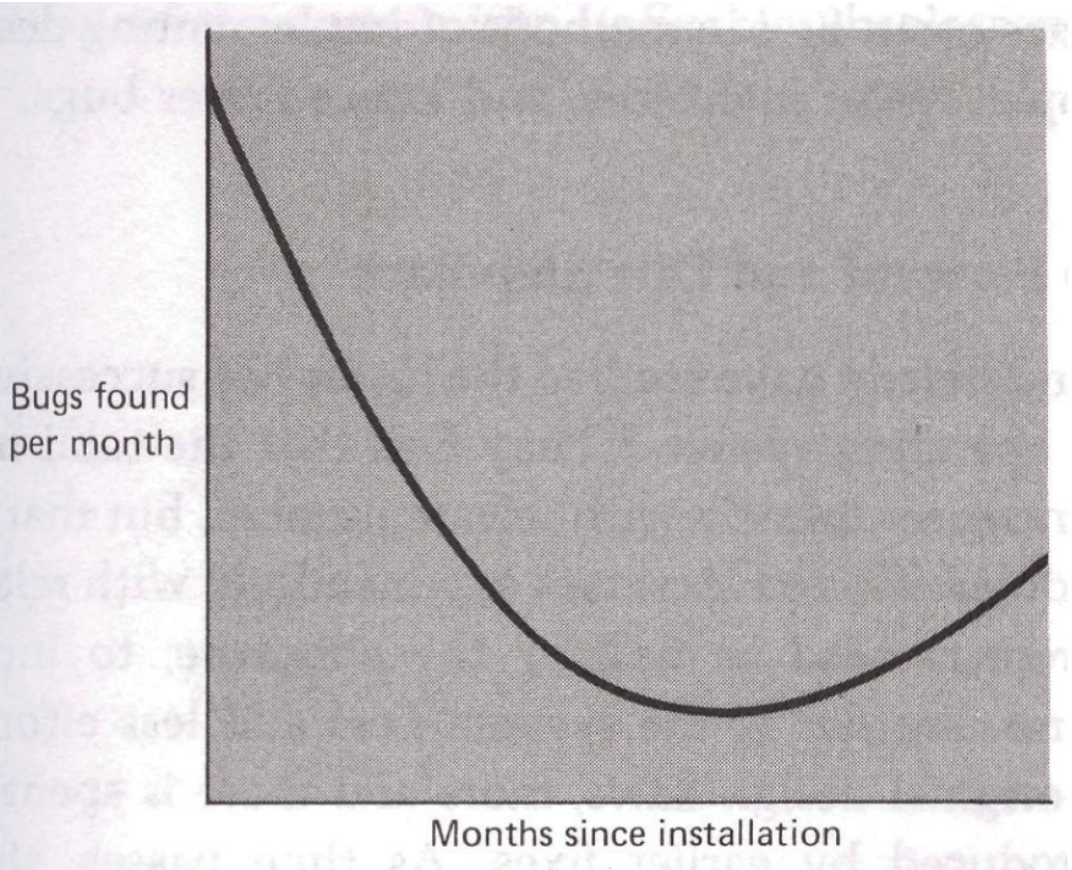
Jim Gettys
Bell Labs
February 22, 2014

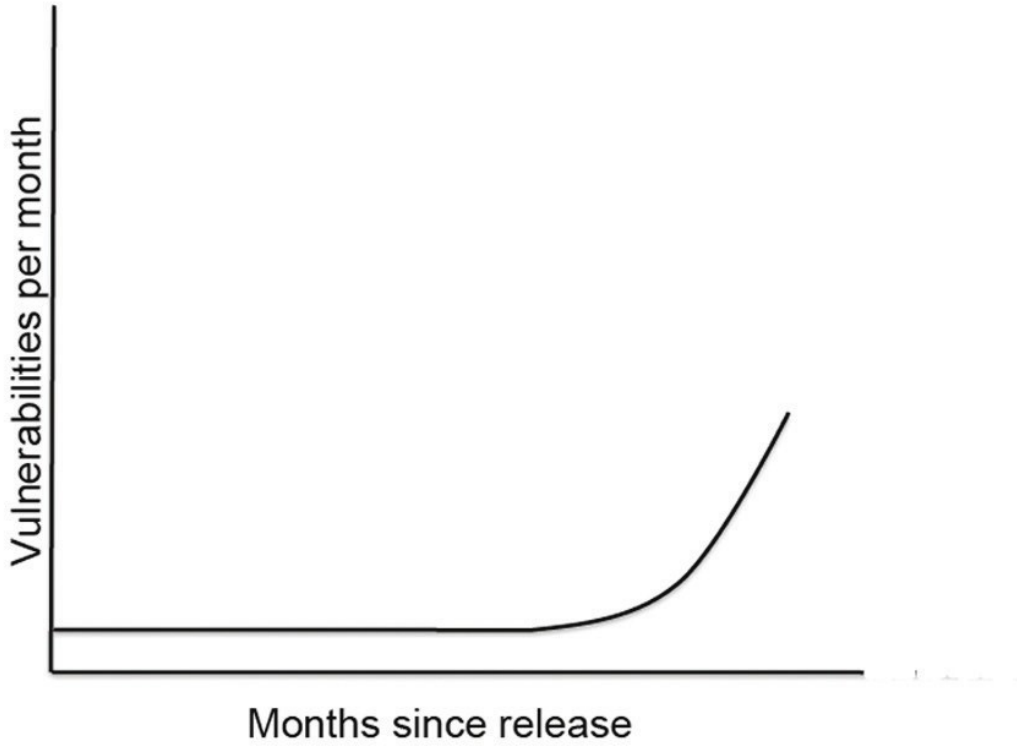
The Internet of Things Is Wildly Insecure — And Often Unpatchable

- Wired, January, 2014, By Bruce Schneier
  - I instigated this article, and helped Bruce with the information in it, and concur with it
  - As with anything, there are nits I'd change
  - The situation is worse than the article presents
- Almost simultaneously, the TAO catalog from the Snowden documents was published
  - I believe this was not a coincidence!

Familiarity Breeds Contempt:
the honeymoon effect and the role of legacy code in zero-day vulnerabilities

- By Sandy Clark, Stefan Frei, Matt Blaze, Jonathan Smith, ACSAC '10





Take Aways

- You cannot leave software and devices “unmaintained”: continuous update is essential, for the life of the device
- Products **MUST** have **SECURE** update stream for the life of the device! (Remember Windows XP!)
  - You **must** select components that **CAN** be maintained
  - You **must** select products that **CAN** be maintained
- Who do you trust? Today? Tomorrow? In 10 years?
  - Long term, only community maintenance *might* possibly succeed
  - Binary blobs leave you helpless and vulnerable, forever
- The owner **must** have ultimate control! You must have the ultimate problem when the device/network/system fails.....

Surprising Result

- RMS was right about Tivoization!
  - Says me, who helped define the MIT License
- But for only one of the three real reasons:
  - *Life*
  - Liberty
  - *The Pursuit of Happiness*
- Whether enforceable by software license is orthogonal to the basic principle....

Home Routers, Modems, etc.

- Usually unmaintained and unpatched: all commercial products I am aware of are simple to Pown.
- Firmware is usually not updated after ~1 year after sale by vendor, after the crash rate diminishes
- Only important related to other embedded devices (e.g. your Nest thermostats) in that they are on your path to the rest of the world and have radios too...
- We now depend on our Internet service: fundamental change is well underway
  - e.g. POTS is doomed: you'd like basic things like your phone to work in an emergency

What can you do?

- Install OpenWrt/CeroWrt today and come help
  - Gets you mesh networking, IPv6, Bufferbloat fixes, etc...
  - CeroWrt gets you routing, rather than bridging
- Build in basic firmware security in your devices: cost is between 26 cents and zero cents
- Become aware of basic building blocks such as OpenFirmware, etc., etc...
- Security is difficult to impossible to retrofit!
  - THINK!

I'll leave you with a meme to spread

“Friends Don't let Friends Run Home Routers with Factory Firmware”