Good Advice that Just Doesn’t Help

Andrew Dingman, Gianpaolo Russo, Tyler Uffelman & George Osterholt

Indiana University Bloomington

“Alexa, turn on the furnace”
“I’m sorry, Dave, that will be 10 bitcoins”

From light bulbs to cars and refrigerators to children’s toys, consumer devices are increasingly connected to home networks and the Internet. This trend, often called the “Internet of Things”, enables many desirable features for the end user. Connected sensors and remote control let you save on heating bills while always coming home to a warm house, even when you break your routine; turn off that burner you left on from the office; unlock the door for your pet sitter from state. However, poor device security and unanticipated interactions also bring new opportunities for malicious actors.

What makes secure “things”?

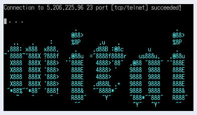
Guidelines exist for designing less vulnerable “things”. Sources include both industry groups such as OWASP and the Online Trust Alliance and government agencies such as the National Highway Traffic Safety Administration, Federal Trade Comission, and even the FBI.

OK, but does that help?

Recommendations
- Six sources of “Best Practices”
- 131 total practices
- 56 unique recommendations

IoT Events
- 3 high profile IoT security events
- Millions of devices
- Variety of devices - cars to cameras

Large-scale, live exploits provide better insight than counting exploits



```
Connection to 5.206.225.96 23 port [tcp/telnet] succeeded!

█. . .
                  .                                  .
                 @88>                               @88>
   ..    .    :  %8P      .u    .                   %8P
 .888: x888  x888.  .    .d88B :@8c        u         .
~`8888~'888X ?888f  .@88u  =~8888f8888r   us888u.   .@88u
  X888  888X '888> ''888E   4888>'88~  .@88 ~8888~ ''888E
  X888  888X '888>   888E   4888> '    9888  9888    888E
  X888  888X '888>   888E   4888>      9888  9888    888E
  X888  888X '888>   888E  .d888L .+   9888  9888    888E
 ~*88%~~~*88~ '888!  888&  ^~8888*~    9888  9888    888&
   ~     ~     ~    R888~    ~Y~       ~888*~~~888~  R888~
                     ~~                  ^Y~    ^Y'    ~~
```

Mirai Botnet
- DDoS botnet of vulnerable IoT devices, mostly ameras
- Best known for ~620 Gbps attack against KrebsOnSecurity
- Variants still in use

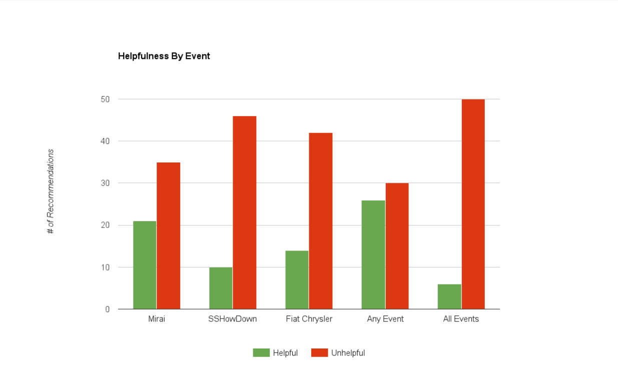
Miller & Valasek car hack
- Complete remote vehicle control over the Internet
- Resulted in 1.4 million vehicle recall

Akamai SSHowDown
- Local privilege on remote devices
- Common vulnerability across multiple devices
- Uses “secure” protocol

Evaluation

Guidance from six sources was simplified to 56 unique recommendations. Each of these 56 recommended practices was then evaluated in light of three recent large-scale events involving security of connected devices.

- **Helpful:** Had it been followed, this practice would have either
  - Prevented the event
  - Reduced the impact of the event, or
  - Eased recovery from the event
- **Unhelpful:** Either the practice
  - Was in fact followed, or
  - Would not have mitigated event impact



Observations

Over half of recommendations (30 out of 56) **would not have helped** in any examined event had they been followed

- Many **good ideas** were **unhelpful**.
  - **Exemplar: Transport encryption is a Good Idea**
    Practice documents consistently recommended TLS or other transport-layer encryption. This practice would protect against data leaks and theft of credentials,
    - **Mirai:** Attacker already knew default credentials. No theft was necessary
    - **SSHowDown:** No need to steal credentials. Used defaults and/or lack of authentication. *In fact, transport encryption was used!*
    - **Vehicle Hack:** Establishing a control channel required no leaked data or authentication
- **Low-hanging fruit**
  Until trivial problems are addressed, attackers won’t use more sophisticated attacks.
- **Economic Incentives**
  Security by design requires skilled personnel and training. Insecurity cost is an externality for many cheap devices.