Smart Devices Need Smart People: Learn How to Be Smart!

ELIZABETH A EVANS, DUKE DIGITAL INITIATIVE
ALYSE ZAVALA, DUKE IT SECURITY OFFICE
INTERNET OF THINGS (IoT)

- The network of physical devices, smart appliances, vehicles, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data (aka "connected devices" or "smart devices")
- Experts estimate that the IoT will consist of about 30 billion objects by 2020.
Botnets?

- **Botnet**: a group of computing devices infected with malicious software that are centrally controlled without the owners' knowledge. This “zombie” army can be used to send spam emails, launch distributed denial of service (DDoS) attacks, etc.

- Recent IoT Botnet Examples: **Mirai, Bashlight, Hajime, Persirai**
  - **Mirai** identifies vulnerable IoT devices using a list of more than 60 common factory default usernames and passwords (admin:admin, root: admin, etc.) At its peak, Mirai infected 4000 IoT devices per hour.
An Army of Million Hacked IoT Devices Almost Broke the Internet Today

A massive Distributed Denial of Service (DDoS) attack against Dyn, a major domain name system (DNS) provider, broke large portions of the Internet on Friday, causing a significant outage to a ton of websites and services, including Twitter, GitHub, PayPal, Amazon, Reddit, Netflix, and Spotify.

Security

Dishwasher has directory traversal bug

Thanks a Miele-on for making everything dangerous, Internet of Things firmware slackers

By Richard Chirgwin 26 Mar 2017 at 23:08

Don’t say you weren’t warned. Miele went full Internet-of-Things with a network-connected dishwasher, gave it a web server, and now finds itself on the wrong end of a security bug report – and it’s accused of ignoring the warning.

Boy, 11, hacks cyber-security audience to give lesson on ‘weaponisation’ of toys

Reuben Paul, 11, tells conference that smart cars, fridges, lights and even teddy bears can be used to spy on or harm people.
IoT Hack Demo

Bluetooth Smart Lightbulb
Model: Colorific BC090
IOS and Android
THINK BIGGER...

Blocked!
IoT Security Tips

- Always change weak default passwords to strong/unique passwords
  - See https://security.duke.edu/passwords for password tips
- Always update with security patches when available
  - Fill out Warranty Card for vendor communication
- Disable/restrict all ports and services on IoT devices which are not used
- Setup a Network Firewall
  - Disable Universal Plug and Play (UPnP) on routers if applicable
  - Home IOT firewalls (CUJO, RATtrap, Dojo, SENSE, Luma, Core, etc)
- Email security@duke.edu if you have any questions

*Note: If you are on the Duke Network, please register your device on https://dukereg.duke.edu/ or CMDB, and consider Network segmentation (VRFs) if it will be many IoT devices