Internet of Things (IoT) - Research

Addy Moran

GENERAL INFORMATION

What is a SmartHome?

A SmartHome utilizes the Internet of Things ideal in a home environment, by connecting everyday technologies to the internet to increase automation and cost/energy efficiency.

Popular SmartHome products include:

- SmartTV – can connect to the internet, download apps/widgets, stream videos
- Smart Fridge – keeps track of amount of food, sends notifications when a food item is gone, grocery lists
- Smart Bed – monitors sleep, tracks data, automatically changes bed pressure
- Garage Door Openers – opens garage door automatically once your car enters the drive way
- Security System – tracks doors opening/closing/locking, keeps video feed of certain rooms
- Thermostat – automatically changes temperature levels based of schedule (wake up, go to work, go to bed)
- Water Management – notifies you if you have a water leak

Advantages

1. Control appliances, AC, TV, etc. with an app
2. Safety
3. Accessibility (could help elderly/disabled stay in their house but stay safe)
4. Energy Efficiency
5. Cost Effectiveness (after purchase)

Disadvantages

1. If technology is compromised, both personal security and information security are put at risk
2. Technology can be moody
3. Technology based on Wi-Fi and electricity, so power outages and Wi-Fi glitches can cause problems
4. Expensive to buy

SECURITY

Top 5 Security Concerns

1. Hacking connected thermostats (i.e. Nest)
    a. can show family schedules, when family members are home (and when awake/asleep)
    b. Hackers can adjust temperature in gas stations and blow it up if gets hot enough. Can also adjust "fullness" of gas (when sensor goes off/on) - can cause overflowing
2. Hacking Smart TV's
    a. many have web cams (so someone could watch you watch TV (or even if it's off)). Can lock you out of Smart TV

3. Compromise Security Systems
    a. interconnected (garage, door locks, cams, etc.) - can do anything if your Wi-Fi is hacked
    b. determine if family on vacation, open garage doors, steal, etc.
4. Eavesdropping on Communication Systems (video conferencing, printers, etc.)
    a. Can steal information, gain access, monitor email messages, listen to Amazon Echo reading your email, how people interact w/ devices, eavesdropping on telephone/video conversations.
    b. If someone hacked a Nest Cam and could communicate through 2-way audio?
5. Changing Lighting Systems
    a. if lighting systems are hacked can control lights (on/off) and amount of electricity used. Could increase electricity bill.

App Security

Operating Systems

- IOS - use Swift (replaced Object-C)
    - problems w/ Objective-C
        - Integer Overflow (Medium level likelihood of exploitation, severe problem)
            - caused by - user entering too large of an integer data type. If the user enters a negative number when an unsigned number is expected the program may allocate a buffer of that size causing a heap overflow.
            - no longer vulnerable with Swift - Swift, causes a runtime error so an attacker can't use this vulnerability
        - Buffer overflow (Very High Severity and Likelihood of Exploitation level).
            - caused by - incorrect pointer manipulations.
            - Swift still vulnerable - Swift can call C functions, however Swift is at lower risk then Objective C
- Android - uses Java
    - C standard (std) library vulnerabilities can cause application/runtime errors
    - Sandboxing Mechanism (allows the execution of untested/untrusted programs/code) - is this a virtualization? Can this be used as an exploitation?

General App Vulnerabilities

- C/C++ Vulnerabilities
    - Stack Overflow
    - Heap Overflow
    - Integer Overflow
    - printf (is java vulnerable to this as well?)
    - Array indexing
    - Unicode bug
    - File I/O - Directory Traversal Vulnerability, Symbolic Link Vulnerability
- Cross Site Scripting & Request Forgery

- SQL Injection
- LDAP Injection
- Insecure Cryptographic Storage

Pin Number Security

- 2 digits random (given by lock (i.e. 1 and 5)) first then 4-digit code after
- 4-digit code = 10^4 options = 10,000

- brute force
    - if each code took 2 second to check, it would take 5.5 hours to go through 10,000 options
    - average time 2.75 hours

Wi-Fi Hacking

- Average Wi-Fi password lengths:
    - WPA/WPA-PSK/WPA2-PSK: 8 characters
    - WPA - PSK (secret string of characters) - have an exhaustive search of likely passwords
    - average cracking time (in years) = combos / 100PSKPerSecond / # Cracking PCs / 60 sec/min / 60 min/hour /24 hors/day / 365/24 /days/year/2
        - time = combos/100/#PCs/60/60/24/365.24/2
        - list of common default router login passwords: http://mywifipro.net/support/solutions/articles/1000052636-common-default-router-login-passwords

Smart Home Product Security

- Samsung Smart TV
    - Hacked Miracast enabled Wi-Fi network (and accessed domestic LAN)
        - were able to browse/download any files on USB drives plugged into Smart TV
        - stole browser cookies with sensitive information (for authentication purposes, for example Gmail account access)
        - found out that the TV sends unencrypted voice recognition data and text
        - surveillance activities
- Smart Meters
    - Poor passwords allow hackers to:
        - take full control of any device
        - modify a unique ID to impersonate a customer
        - could shut down power supplies
        - could access/transfer meter readings and inject worms that cause problems to entire network
        - used AES-128 encryption which is still vulnerable to brute force attacks
- Wi-Fi LED Light Bulbs (LIFX)
    - Only one light bulb needs to be connected to the Wi-Fi at a time. A hacker was able to:

- control every other light bulb in the house and see network configurations
- able to analyze network traffic and identify packets on an encrypted network configuration among the light bulbs. Analysts injected packets into network that interferes with bulbs
- Only the 802.15.4 6LoWPAN wireless is vulnerable, so hacker must be within 30 meters of the network

- Baby Monitor & Other IP Cameras
  - Hardcoded backdoor credentials, authentication bypass flaw, direct browsing flaw, information leakage flaw, cross-site scripting bug (XSS), Shodan leaks these devices online
  - hacker can:
    - access and open a video stream

Other Security Concerns

- Lose security for comfort/accessibility (for example, only asking for a password once)
- If you have a guest over and they used their Wi-Fi could they get access to this information (in relation to BYOD)?

TRUST ZONES & SCALING

Trust Zones: Devices in a trust zone can only interact with other devices in that trust zone.
Kitchen – Fridge, Microwave, Slow Cooker
Entertainment – Smart TV, Speaker/Sound System
Security – Locks, Garage Door, Video Cameras, Alarm System
Utilities – Water Management, Thermostat/Humidity, Smoke/C02 detectors, Light Bulbs

Scaling (0 – 4):
0 – doesn't need any security (Kitchen)
1 – doesn't need much security
2 – want some security (Utilities)
3 – want more security (Entertainment)
4 – must have security (Security and Document Cloud Storage (medical records, SSN, Birth Certificates))

POSSIBLE IMPLEMENTATIONS

Software-Defined Networking (SDN):

Purpose

- Allows software to run separately from the hardware (virtualization). Separates the network traffic and decides where the traffic is sent.

Basic Structure

- Application Layer – switch/network virtualization, firewalls, flow balancers
- SND controller – removes the control plane from network hardware and runs it as software, integrates all physical and virtual devices on the network. Makes it easier to integrate and administer applications
- Physical Network Layer

- Note: Could also use Application Programming Interfaces (APIs)
  - provide a channel for instructions to be sent to a device to program. APIs could work “northbound” and with the controller, or they could work “southbound” work with the network (like Switches)
- Note: Could also use a Network Overlay, created using virtual switches, these set up tunnels that make use of a physical network, don’t need to configure hardware to send traffic to it’s destination.
  - Emerging protocols: VXLAN, STT, NVGRE

How it works

- “This is done by decoupling or dissociating the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane)” – Wikipedia
- Commonly used with OpenFlow protocol

Pros

- Directly Programmable
- Agile – allows administrators to dynamically adjust network traffic flow
- Centrally Managed – centralized in software based SDN controllers
- Programmatically configured allows network managers configure, secure, manage, optimize network resources quickly

Security

- controller can change data plane at any time
- DDoS (Distributed Denial of Service) detection and mitigation, botnet (using someone’s computer without the user’s knowledge) and worm (replicates malicious software to spread to other devices often through a network) propagation
- Collects network statistics from forwarding plane (using OpenFlow) and them applies classification algorithms to detect any anomalies, if detected controller reprograms data plane to mitigate
- Implements Moving Target Defense (MTD) Algorithms – hides/changes key components of a system/network
- Open standards-based & vendor-neutral – simplifies network design and operation instead of using multiple vendor-specific devices & protocols.

Personal Firewalls

Purpose

- Control network traffic
- Difference between personal firewalls and firewalls:
  - Personal firewalls usually only protect the computer that the software is installed, where a conventional firewall protects the network using an interface such as a router or proxy server.

How it works

- Usually works as an application layer firewall

Pros

- Allows more flexibility for a computer/hub based on the circumstances (different hubs have different Firewall policies)
- Each personal firewall can control what programs can access internet/network, can prevent unwanted network traffic
- Can protect against malware sent as an executable program
- Can help protect network and computers better from hackers

Cons

- If network is hacked, hacker can shut down firewalls
- Using an operating systems or other firewalls can increase security vulnerability

Li-Fi

History

- Idea came around in 2011 from Harald Haas, a professor at University of Edinburgh
- Prototype finished in 2015
- University of Edinburgh LiFi R&D Centre and pureLifi Ltd (a university company) are collaborators

Expectations & How it Works

- Homes are solar powered
  - LED light source with a solar panel can form a transmitter and receiver system
- For internet to work you must be in the room with the LED and Li-Fi router
- Data is transmitted through undetectable flicker of an LED light

Pros

- Strangers/Hackers can't access your information unless they are in that room

IDEAL SITUATION

Goals

- All devices connected in safe/un-hackable way

Problems that may occur

- In order for Li-Fi to work homes would need to be powered by solar power.
- For secure connectability (multiple LANs, etc.) professionals would have to install the devices and set up the networks (no self-installation).
- Some of the devices/software haven't been developed yet

What technology would be needed for the ideal to be successful?

- Safer Wi-Fi or a different SmartHome connectability option (like Li-Fi)
- Software to split/monitor which device can access which LAN (Software-Defined Networking would probably be implemented)

RESOURCES

http://www.cheatsheet.com/gear-style/when-will-the-smart-home-finally-become-popular.html/
http://www.cheatsheet.com/gear-style/smart-homes-4-potential-problems-you-may-run-into.html/?a=viewall
https://en.wikipedia.org/wiki/Bring_your_own_device#Advantages
http://www.cnet.com/ - for product reviews
http://www.tomsguide.com/us/best-smart-home-gadgets,review-2008.html - most popular brands
http://www.makeuseof.com/tag/5-security-concerns-consider-creating-smart-home/ - top 5 security concerns
http://tech.co/smart-home-tools-smarter-office-2015-12
https://www.directenergy.com/learning-center/modern-home/advantages-smart-home
https://en.wikipedia.org/wiki/Sandbox_(computer_security)
https://en.wikipedia.org/wiki/Java_security#Potential_sources_of_security_vulnerabilities_in_Java_applications
http://www.drdobbs.com/security/security-issues-in-swift-what-the-new-la/240168882
http://www.securecodingacademy.com/documents/10192/14602/RT-CVL
http://www.veracode.com/security/application-vulnerability
http://www.kwikset.com/electronics/homeowners/keylessentry.aspx
https://www.reddit.com/r/WhatsInThisThing/comments/2njl7u/how_long_will_it_take_to_try_all_10000_4_digit/
http://mywifipro.net/support/solutions/articles/1000052636-common-default-router-login-passwords
http://www.hackingtutorials.org/wifi-hacking-tutorials/top-10-wifi-hacking-tools-in-kali-linux/
http://www.hgtv.com/remodel/mechanical-systems/11-smart-apps-for-your-home
https://en.wikipedia.org/wiki/Software-defined_networking
https://en.wikipedia.org/wiki/Computer_worm
https://www.opennetworking.org/sdn-resources/sdn-definition
http://www.networkcomputing.com/cloud-infrastructure/7-essentials-software-defined-networking/1672824201
http://www.veritas.com/community/articles/network-security-and-ways-protect-system
http://resources.infosecinstitute.com/how-hackers-violate-privacy-and-security-of-the-smart-home/
http://uk.businessinsider.com/how-smart-homes-can-be-hacked-2015-7?r=US&IR=T
http://www.digitaltrends.com/cool-tech/li-fi-wireless-internet-led-light-solar-cell/
https://en.wikipedia.org/wiki/Personal_firewall