DSci529: Security and Privacy In Informatics

Internet of Things

Prof. Clifford Neuman

Lecture 8
5 March 2021
Online

Course Outline

- Overview of Security and Privacy
- What data is out there and how is it used
- Technical means of protection
- Identification, Authentication, Audit
- Reasonable expectation of privacy
- Big Data – Technology and Privacy
- AI and Bias
- **The Internet of Things and Security and Privacy**
- Social Networks and the use of our Data
- Access to Data by Governments - Privacy in a Pandemic
- Privacy Regulation - GDPR, CCPA, CPRA
- Influence of Social Media – Free Speech – Disinformation
- CryptoCurrency - TOR - Privacy Preserving Technologies

No Lecture on Friday 12 March

- Friday March 12th is the first of the university “wellness days”
  - There will be no lecture
  - Do not submit current events for the 12th of March
  - The next lecture will be Friday March 19th

- Mid-term exam results
  - Will be posted by March 12th (even though no lecture on that day)

Today's Agenda

- 12:00 – 12:15 Introduction and Announcements
- 12:15 – 13:50 Student Presentations – Internet of Things
  - 10 minutes for each presentations followed by approx. 5 minutes of open class discussion (smart home as 10 minutes following the 2 pres)
  - Pratheek Athreya – Introduction and Wearables
  - Arzu Karaer - Cybersecurity in the Automotive Industry
  - Bolong Pan - Social Engineering, Methodologies and Threats
  - Danielle Sim - Digital Assistant Devices
  - Jinyu Zhao - Smart Homes Part 1
  - Pu (Rosy) Zhao - Smart Homes Part 2
  - Junbo S – Security and Privacy
- 13:50 – 14:00 Break
- 14:00 – 14:45 Internet of Things Discussion – Dr. Neuman
- 14:45 – 15:20 Current Event Discussion

Upcoming Presentations
Social Media – March 19th

- Addison Allred
- Yixiang Cao
- Lei Gao
- Brianna Hefferin
- Mingliao Xu
- Shengwang Zhang
- Zixin Zheng
- Hehan Xie
- Chengyuan Zhou
- Hehan Xie

- This group will have 100 minutes to present.

Upcomming Presentations Pandemic/Govt Data Use – March 26th

Pandemic (40 minutes)

- Yuemeng Gao
- Tanmay Ghai – Privacy Preserving Contact Tracing
- Yi Lin – Big Data in China related to the COVID Pandemic
- Gan Xin – Health QR Code in China

Other government use of data (50 min)

- Yi Jin – How US and China collect and use personal data
- Congrui Li
- Michelle Muldoon – Law Enforcement and Privacy w.r.t. Data Brokers
- Griffin Weinhold – Decentralized Search and Search Histories in Court
- Xihao Zhou – Use of Data by Governments
- Jinglun Chen – Use of location data
- Jiemin Tang – Security and Privacy regulation for food delivery services

Upcoming Presentations
Privacy&Security Regulation – April 2nd

- Jia Yu Lee
- Yansong Wang
- Kaifan Lu – Assessing China's Cybersecurity Law

- 30 minutes for this group to present

Upcoming Presentations Healthcare – April 2nd

- Vartan Batmazyan
- Phuong Ngo
- Sharad Sharma (DNA Databases)
- Ye Zheng - Fitness apps

- This group will have 40 minutes to present.

Upcoming Presentations – April 9th Free Expression - Disinformation

- Adriana Nana – Deep Fakes and Privacy
- Resherle Verna – Should Social Media company's have right of censorship

  – This group will have 20 minutes to present.

Upcoming Presentations Privacy and Finance – April 16th

- Jonathan De Leon – Privacy in Finance
- Sidong Wang – History and Technologies for Cryptocurrencies
- Saurabh Jain – Privacy of Credit Card/Payment card information
- Yifeng Shi -Financial value of data gathered through free services

- 40 minutes

Secure Communication – Privacy Preserving Technologies – April 16th

- Zihuan Ran – Privacy Preserving Database Technologies
- Aziza Saulebay – 5G and Data Privacy
- Carol Varkey – Messaging Application Privacy
- Francisco Ventura – Encryption Technologies and implications

- 40 minutes

Upcoming Presentations
Other Security Topics – April 23rd

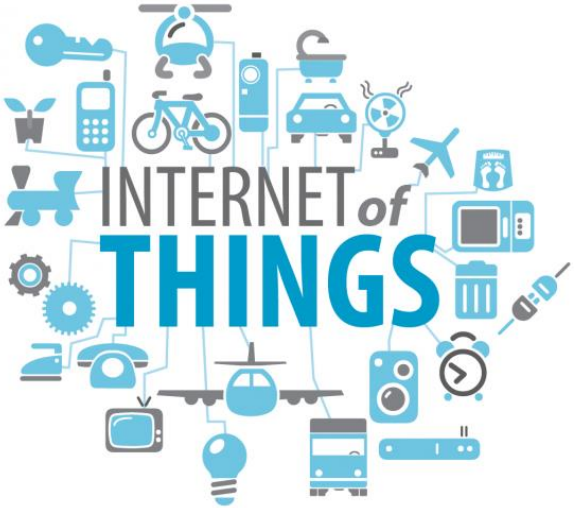
- Yo-Shuan Liu – User experience and Multi-Factor Authentication
- Philana Williams – Security for Web App Development
- Haonan Xu – Privacy issues in Cloud Computing
- Pratishtha Singh – Card privacy Concerns in India

What are “Things”

- IoT Includes devices and software embedded with sensors, and network connectivity for integration and to enable data collection/exchange.
- Network connected “smart” objects can be sensed and controlled remotely.
- In some cases a hub serves as a “master” device, but more and more frequently, this hub resides in the cloud.
- There are more than 500 million internet connected devices in U.S. homes alone and it is estimated that approximately 50 billion objects will have IoT capability by 2020.

Some Issues

- Devices
  - We carry
  - At our home
  - At work and “on the road”
  - In our vehicles
- Privacy
  - What data they collect or possess
- Security
  - How that data is protected
- Attacks enabled
  - Further implications



IoT on our Person

- On our person
  - Smartphone
  - Laptop/Tablets
  - FitBit or activity Tracker
  - Smart Watch
  - Insulin Pumps
  - Pacemakers
  - Google Glass

- Or in our homes

Issues

- How we connect
  - And how we authenticate/authorize
- Data Collection or Manipulation
  - Sensor or PLC (programmable Logic Controller)
- General Purpose Computing or Specialized
- How to Update / Reprogram
- Risks and Consequences

Readings for This Week (read these after today's lecture)

Carsten Maple, Security and privacy in the internet of things, 5/4/2017, Journal of Cyber Policy.

The internet of things (IoT) is a technology that has the capacity to revolutionise the way that we live, in sectors ranging from transport to health, from entertainment to our interactions with government. This fantastic opportunity also presents a number of significant challenges. The growth in the number of devices and the speed of that growth presents challenges to our security and freedoms as we battle to develop policies, standards, and governance that shape this development without stifling innovation. This paper discusses the evolution of the IoT, its various definitions, and some of its key application areas. Security and privacy considerations and challenges that lie ahead are discussed both generally and in the context of these applications.

Readings for This Week (read these after today's lecture)

Smart TVs, smart-home devices found to be leaking sensitive user data, researchers find. NBC News, September 18, 2019.

Smart-home devices, such as televisions and streaming boxes, are collecting reams of data — including sensitive information such as device locations — that is then being sent to third parties like advertisers and major tech companies, researchers said Tuesday.

"Nearly all TV devices in our testbeds contacts Netflix even though we never configured any TV with a Netflix account," the researchers wrote.

Readings for This Week (read these after today's lecture)

Our Privacy Nightmare and What Can Be Done About It

- By Adam Piore On 10/24/19 at 12:39 PM EDT Newsweek

The Internet of Things (IoT) is not just a security problem. It's also a privacy nightmare. Few people in Washington know more about the issue than Marc Rotenberg, a Georgetown Law Professor who serves as president and executive director of the Electronic Privacy Information Center (EPIC). In 1994, he founded the Washington D.C.-based organization to fight to protect individual privacy and civil liberties on the burgeoning computer network. At the time banks and other large commercial interests just beginning to establish an online presence. Today there's a lot more to worry about.

Readings for This Week And Assignment Due March 19th

Also read about:

California's Internet of Things Security Law

For all of the readings in this set (i.e. including those on the preceding slides):

- Write at least two pages presenting your opinion regarding the security **and** privacy issues associated with internet of things devices.
- Cite to the readings above, as well as any other sources you can find to support your position. Be sure to present opposing views in your discussion.
- Post your discussion to the D2L discussion forums (which you will receive information about before monday).
- Comment and provide feedback on the postings of other students.

First Some Context

- Video Clip

Then Student Presentations

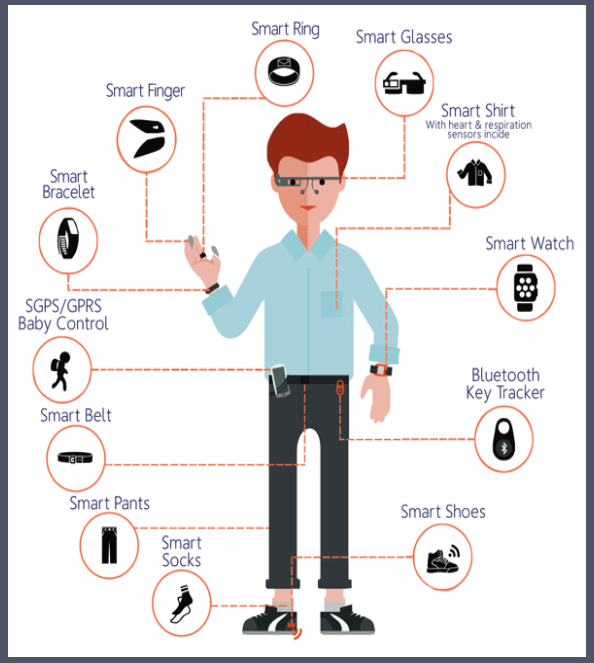
PRIVACY AND SECURITY ISSUES OF WEARABLES

Pratheek Athreya
5994431189

Wearables - What are they?

- Smart electronic devices which can be placed either on, close to or under the skin and can detect, analyze and transmit data about the user via the internet.

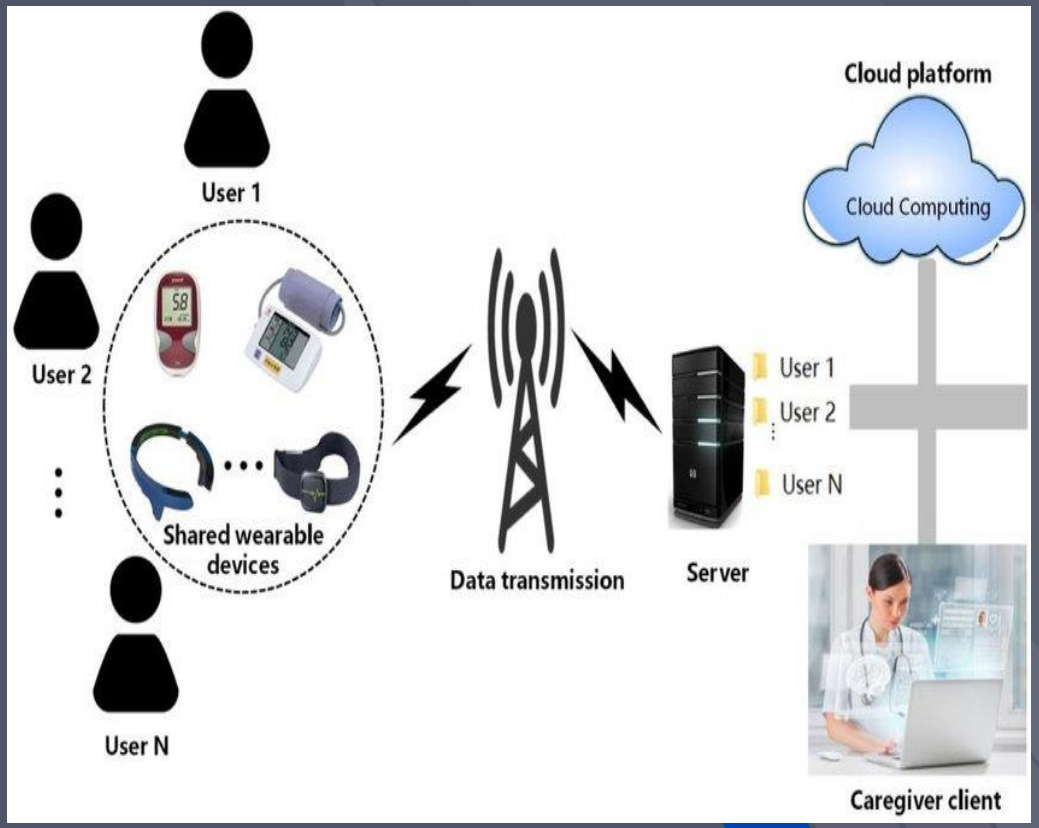
- COMPONENTS USED:
  - Microcontrollers
  - Sensors
  - The components used to make a wearable are contingent upon its form and function. For example, Project Jacquard uses conductive threads called Jacquard threads to make a smart denim jacket that can help you capture pictures remotely and receive notifications among many other functions.



Wearables- How do they work?

- As mentioned in the previous slide, wearable technology consists of sensors that can monitor various attributes of the user such as heart rate, temperature and muscle activity. This data is aggregated and fed to the processor inside the wearable which, in turn, produces the corresponding output.

- This data may also be transmitted over the internet to the manufacturer's server where it can be analysed.



Wearables- Markets and Statistics

- In 2016, the number of connected wearables was around 325 million. With the advent of 5G, this number is projected to rise to 1.105 billion in the year 2022.

- Smart watches occupy approximately 52% of the global market shares, with Apple, Fitbit, Samsung and Garmin being the top-contenders. Among these, Apple holds the largest share in the market.

- Fitbit’s demand for smartwatches was overtaken by Xiaomi, with nearly 150 million units being shipped out in the first three quarters of 2019.

- Although businesses, military and medical professionals have been using wearables for decades, it is only recently that private consumers have been using items such as smart watches, fitness trackers and smart shoes.

- With fitness trackers and smart watches currently being two of the most sought-after wearables in the market, earwear is soon projected to join that list. Almost 270 million units of earwear are projected to be sold by 2023.

- In North America alone, the number of connected wearable devices produced has increased from 38.65 million in 2015 to 378.8 million in 2020. Continuing on this trend, it is projected to increase to 439 million in 2022.

Wearables- What do they collect?

- Heart rate
- Steps Walked
- Blood Pressure
- Calories Burned
- Seizures
- Demographics data
- Forecasting changes in mood,stress and health
- Advertisements based on a user’s activity such as their location, mood, activity, etc.
- Measuring blood alcohol content

Security Issues

- Human interaction introduces vulnerability
- Data captured by healthcare wearables typically flow across short, unlicensed wireless links to a monitoring hub in the patient’s home, which then passes the information to the broadband network, routing it to the cloud.
- Medical devices have been key points of vulnerabilities and have been subject to attacks
- Important to maintain secure infrastructure to avoid cybersecurity attacks

Wearables - Privacy Issues

- External Data Sharing Policy
  - Often ambiguous
    - Can share data with third parties without consent from user
    - HIPAA and HITECH not applicable
    - These laws however are applicable to wearables developed to enhance people’s health but not to consumer wearables health data

Wearables - Privacy Issues

- External Data Sharing Privacy - Mitigation Methods
  - Anonymization of micro as well as aggregated data : For eg - k-anonymity, l-diversity
  - In spite of using various anonymization techniques, sometimes the data obtained from wearables - even in the aggregated form - can reveal the user's identity.
  - The reason for this breach of privacy is the uniqueness of some of the traits monitored by the wearable.
  - Commonly, movement patterns, walking speed and step length are vulnerable to this transparency. Behavioral inferences can be made using such data.
  - Some proposed solutions for this problem are the usage of an anonymous user ID or having multiple user IDs for sharing between different groups of people. For example, using an ID for sharing information between peers and using a different ID for sharing information between a user and other devices.

Wearables - Privacy Issues

- Workplace Adaptation and Ethical Issues:
  - As aforementioned, wearables are beneficial in many ways. However, some employers ban these devices in the workplace fearing that the device might cause distraction among the workforce or that it might record sensitive information. Other fears are of these wearables being affected negatively in sensitive environments such as oil and gas industries and also, the tracking of the employee by the employer.
  - In order to mitigate these concerns, the use of anonymous user IDs and other anonymity measures can be enforced. Moreover, the policies that govern the use and ethics of these devices can be established and made more stringent, if they are already in existence.

Wearables - Privacy Issues

- Data Jurisdiction and Privacy Policies:
  - Data jurisdiction refers to the level of access / control that a user is given over their data. The privacy policies differ with countries and organizations.
  - Users' data might also be at risk due to some organizations' arcane and ambiguous privacy policies. This allows the former to have complete control over their users' data and potentially exploit the same.
  - A solution to this problem would be to use Block Chain technology.
  - The framework LinkShare ensures compliance of the users' data with the company's privacy policies and hence increases the chances of data being protected. This framework uses Natural Language Processing (NLP) which ensures the compliance between the data and policies and lets only those transactions which obey the policies to be stored in the block chain, where they are free of being tampered with.

Wearables - Some other Privacy Issues

- Data collected today can be used for a different purpose tomorrow
- Bystander privacy - Collection of information of bystanders
  - Mitigation Techniques : Blurring of bystanders using deep learning algorithms or usage of notification systems
- Fears that wearable data will be used by criminals to harass an user.
- Many times it isn’t apparent that someone is wearing a wearable device in public

Conclusion

- Wearables began in an era when security and privacy risks were low and was used by businesses.
- People have become tech savvy as a result there is more demand for innovative products
- Compromise of security at the cost of innovation
- Demand or supply side do not address privacy
- Policy or self-regulation should address these concerns

REFERENCES

- A. J. Perez and S. Zeadally, "Privacy Issues and Solutions for Consumer Wearables," in *IT Professional*, vol. 20, no. 4, pp. 46-56, Jul./Aug. 2018, doi: 10.1109/MITP.2017.265105905.

  https://ieeexplore.ieee.org/abstract/document/7950844

- Kapoor, Vidhi & Singh, Rishabh & Reddy, Rishabh & Churi, Prathamesh. (2020). Privacy Issues in Wearable Technology: An Intrinsic Review. SSRN Electronic Journal. 10.2139/ssrn.3566918.

  https://www.researchgate.net/publication/340484444_Privacy_Issues_in_Wearable_Technology_An_Intrinsic_Review/citation/download

- American Bar Association Website

  https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/

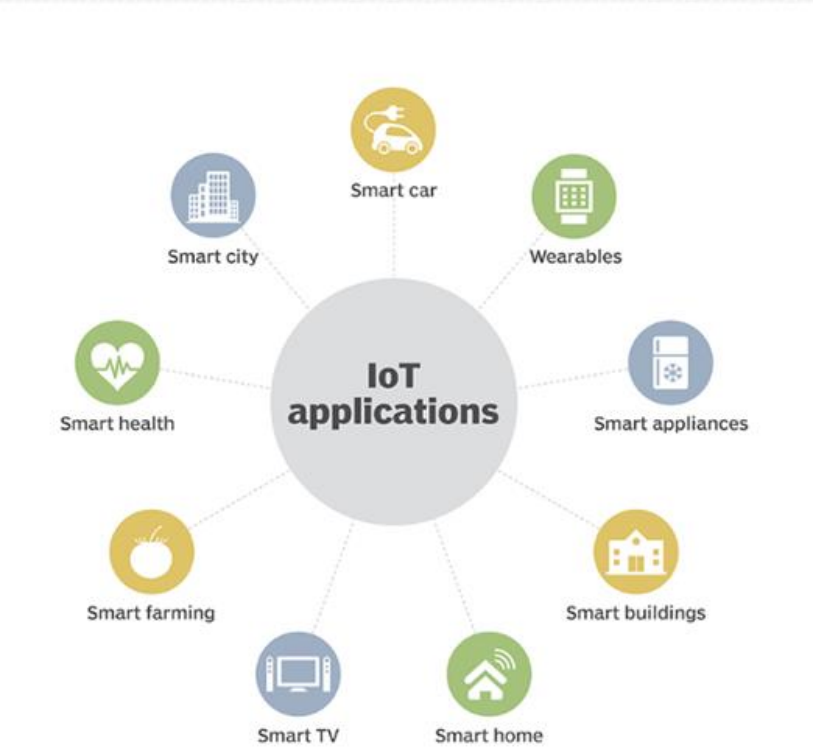
Cybersecurity in Automotive

Arzu Karaer

IOT

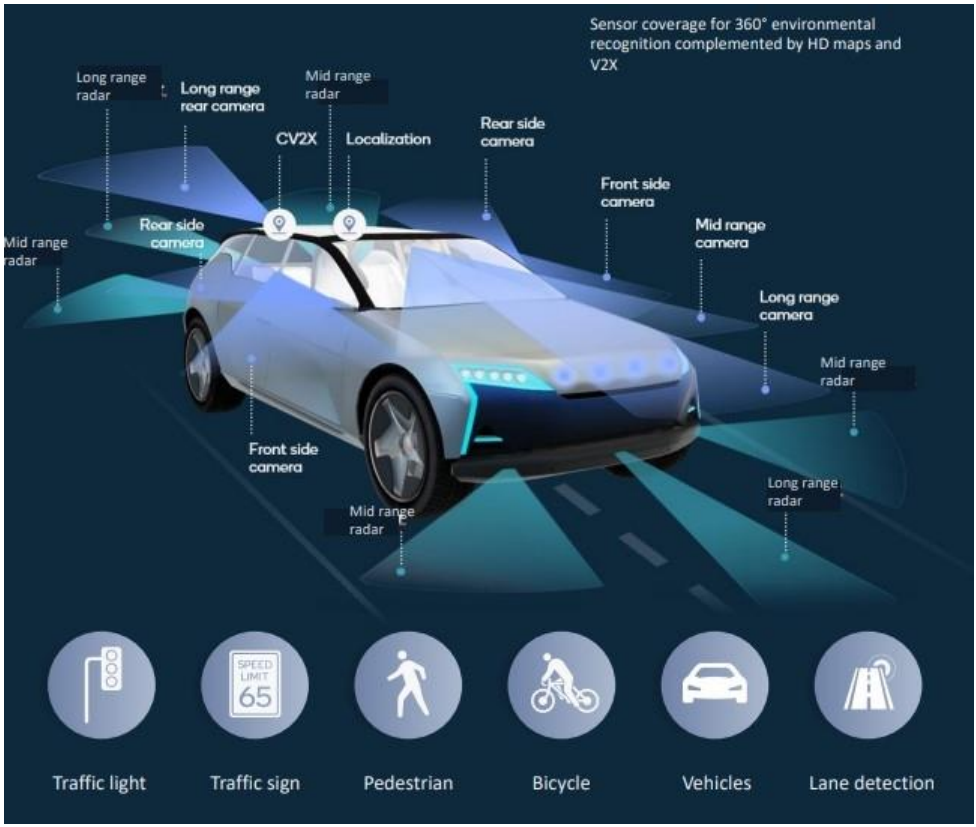
- Network of physical “things” that are embedded with sensors, software and other technologies for the purpose of exchanging information over the Internet

- https://www.1rti.com/internet-of-things-iot-what-is-it/



IOT in Automotive

- Fleet Management
- Connected Cars
- Automotive Maintenance System
- Autonomous Vehicles
- In-Vehicle Infotainment and Telematics

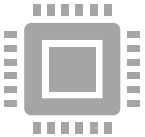


Why is Cybersecurity Important?

- FBI assessment “the automotive industry likely will face a wide range of cyber threats and malicious activity in the near future as the vast amount of data collected by Internet-connected vehicles and autonomous vehicles become a highly valued target for nation-states and financially-motivated actors.”
- Direct impact on road users’ safety and security.
- Fleet wide attacks and multivehicle remote control
  - Injury and death to hundreds even thousands
- Financial impact to governments, insurance, trucking and logistics companies
- Protect the privacy of the data

Security Weaknesses in Automotive

The rising number of connected vehicles have increased vulnerabilities and entry points for hackers to leverage.



Different suppliers provide components to car manufacturers. These include hardware, software including firmware, operating systems, middleware, application software, all of which may use proprietary or open-source code.
Each component can have vulnerabilities which are not evaluated.

No regulations until recently

Top Cybersecurity Vulnerabilities in Automotive

- 663 publicly reported attacks between 2010-2020
- Server Attacks (32%)
  - Involves a range of server types, including telematics command-and-control servers, database servers, web servers, and more.
- Keyfob and Keyless Entry Attacks (26%)
- Mobile App Vulnerabilities (<10%)

Regulations

- Two new UN Regulations on Cybersecurity and Software Updates adopted in June 2020.
  - Automakers will be required to complete risk analysis
  - Suppliers will be required to disclose all risks about their hardware and software
  - Automakers will be required to have a full inventory of all firmware and software in every different make and model
  - Automakers will be required to monitor vehicles post-sale and fix any vulnerabilities
  - Provide safe and secure OTA updates
- The regulations will apply to passenger cars, vans, trucks and buses.
- Other countries like China and the US have so far not issued similar regulations, only guidelines and best practices.
- Expectation is the new UN regulations to become a de facto standard even beyond its members.

References

IOT and Automotive:

https://www.biz4intellia.com/blog/iot-applications-in-automotive-industry/

https://www.fierceelectronics.com/electronics/qualcomm-lays-out-its-smart-transport-vision-including-vehicle-prediction-ai

Upstream Security Global Automotive CyberSecurity Report 2021:

https://upstream.auto/automotive-cybersecurity-standards-and-regulations/

McKinsey & Company CyberSecurity in Automotive

https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf

DST80 cryptographic algorithm

https://en.wikipedia.org/wiki/Digital_signature_transponder

Regulatory:

https://unece.org/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll-out-connected-vehicles

Social Engineering and IoTs

---- Bolong Pan

IoT & IoT Security

IoT:

Network of physical objects that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet

IoT Security:

A security strategy and protection mechanism that specifically safeguards from the possibility of cyberattacks on IoT devices that are connected to the network and purposely built for a fixed set of functionalities.

Social Engineering

Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

The consequences of social engineering attacks in the IoT could be worse than the same attacks in the “IT Internet” of today!

- Delay adoption of technologies
- Undermine confidence in the safety – not just the security – of the IoT
- Raise the levels of regulation in a reflexive and ill-conceived manner

Social Engineering Stages

Social engineering occurs in three stages:

1. Research—the attacker performs reconnaissance on the target to gather information like organizational structure, roles, behaviors, and things that target individuals may respond to.
2. Planning—the attacker selects their mode of attack and designs the strategy and specific messages they will use to exploit the target individuals' weaknesses.
3. Execution—the attacker carries out the attack .

Social Engineering Techs with help from IoT

1. Phishing using smart devices instead of email messages, because targets believe in those devices more than cell-phones, laptops.
2. Watering hole attacks on smart devices because they have less secure defending softwares.
3. Whaling attacks becomes easier if the targets are surrounded by smart devices, so attackers have more opportunity to find a way to conduct attacks to specific targets
4. Pretexting: Attackers have more choices and they can use the most vulnerable device in a smart home to conduct attacks.

Scenario: Smart TVs

IoT devices often hold the trust of users as they belong to a family of devices which they have been able to safely use for years. So users can rarely think they are suspicious and never imagine they could become social engineering platforms.

Smart TVs can be compromised. So can heart pacemakers, even airplanes.

Thank You

---- Bolong Pan

Digital Assistant Devices

Danielle Sim
Security and Privacy in Informatics

What are they?

- "The point of communication between you and **all your connected devices**...streamline your relationship with technology" [1]
- Wake word → voice recordings transcribed into digital text → commands

"Hey Alexa"

Google Assistant

"Hey Google"

"Hey Siri"

1. https://www.reviews.com/home/smart-home/best-voice-assistant/

Infringing on our Privacy

- Command queries stored by the company → associated with an individual/household even after deletion/removal of account/device
  - Where we go, what's our schedule, who we communicate with, what we purchase
  - Companies business models depends on collecting user data
  - Third party brokers, advertisers
- Voice-identification and "anonymized" user data
- "Always listening" even without wake word
- Children and minors
  - Virtual childcare, entertainment, homework help

Security Risks

- Home security → privacy security tradeoff
- Company mishaps
  - Mishearing wake words, recording conversations, sending audio clips to contacts
- Data storage on cloud → secure networks for company and for user
- Software updates → Alexa has 90,194 skills, 24.2% of which have a privacy policy [2]
  - "A first problem is that **Amazon has partially activated skills automatically** since 2017. Previously, users had to agree to the use of each skill. Now they hardly have an overview of where the answer Alexa gives them comes from and who programmed it in the first place." [2]
  - "When a skill is published in the skill store, it also displays the developer's name. We found that **developers can register themselves with any company name when creating their developer's account with Amazon. This makes it easy for an attacker to impersonate any well-known manufacturer or service provider.**" [2]
  - ‘Academics smuggle 234 policy-violating skills on the Alexa Skills Store’ [3]

2. https://www.zdnet.com/article/why-would-you-ever-trust-amazons-alexa-after-this/
3. https://www.zdnet.com/article/academics-smuggle-234-policy-violating-skills-on-the-alexa-skills-store/

In the News

12/21/2018
11:30 AM

DARK Reading

Dark Reading Staff
Quick Hits

3 COMMENTS
COMMENT NOW

Login
100% 0%

Like
Tweet
Share

Amazon Slip-Up Shows How Much Alexa Really Knows

Amazon mistakenly sent one user's Alexa recordings to a stranger but neglected to disclose the error.

Your worst fears about home assistants came true for one Amazon customer whose Alexa recordings were accidentally sent to a complete stranger. Amazon failed to disclose the mistake, but don't worry: The recipient learned enough about the Alexa owner to reach out.

It started when a German Amazon customer requested his Amazon-owned data, which he has a right to do under the General Data Protection Regulation (GDPR). After several weeks, the company sent a downloadable 100-Mb zip file. Some of its contents reflected the customer's Amazon searches. However, hundreds were .wav files and one contained transcripts of voice commands recorded by Alexa. The person had never owned an Alexa, so he reported the issue to Amazon, which did not respond but killed the link to the data.

However, the customer had already saved the files, so he reached out to German magazine c't because he worried Amazon hadn't shared the mistake with the data's rightful owner. By listening to the files, the publication was able to learn the person's name, habits, jobs, musical taste, and more intimate details that "got our hair standing on end," the report states. First and last names helped determine his close friends; Facebook and Twitter data filled in more of the details.

C't learned enough about the victim to contact him and inform him of the mistake. Amazon did not share the error with him, he said, but the company later contacted both the victim and accidental recipient. It claims a staff member made "a one-time error," Gizmodo reports.

npr

SIGN IN NPR SHOP DONATE

NEWS ARTS & LIFE MUSIC SHOWS & PODCASTS SEARCH

TECHNOLOGY

Oregon Couple Unplugs Alexa After Private Conversation Is Recorded

May 25, 2018 · 6:39 AM ET
Heard on Morning Edition

27-Second Listen + PLAYLIST

The couple tells KIRO-TV that they had a private conversation. Their Amazon Echo recorded it, and then sent the audio to someone on their contact list. Amazon says this is extremely rare.

Search **Bloomberg** Sign In

an opportunity. Get alerts to help you stay in the know. **Enable Notifications.** Allow Later

Technology

Amazon Workers Are Listening to What You Tell Alexa

A global team reviews audio clips in an effort to help the voice-activated assistant respond to commands.

By Matt Day, Giles Turner, and Natalia Drozdiak
April 10, 2019, 3:34 PM PDT

Digital Assistants and our Expectation of Privacy

July 20, 2017

"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create

Eric Boughman, Sara Beth A.R. Kohut, David Sella-Villa, Michael V. Silvestro

https://www.americanbar.org/groups/business_law/publications/blt/2017/07/05_boughman/

- Siri and Alexa are simply the intermediary between us and our online queries
  - We know data is collected, shared, accessed and used by third party companies and gov't
- Reasonable expectation of privacy when voice recording is held locally on our device in our home
  - Ultimately all recordings stored on company's cloud

Arkansas v. Bates

- Law enforcement seized an Amazon Echo device and issued a **search warrant to Amazon seeking data associated with the device, including audio recordings, transcribed records, and other text records** during the 48-hour period around the time of death

- Implications:
  - Data collected by digital assistants are no exception to the Fourth Amendment (in contrast to cell-phone *device*)
  - Cannot expect a greater degree of privacy than our search engine queries
  - First Amendment protections for "expressive content"

In Conclusion

- Use at your own risk
- Many benefits, highly convenient, can improve quality of life
- Most important aspect is to be aware of your expectations of privacy and what you can do to support your expectations
- Technology is always improving - both to be more secure and to make smarter inferences
- Ultimately, companies are responsible for creating safe products, and government legislation needs to update its policies to regulate data usage and protect its users

Thank you!

Questions & Comments?

DS529:
IoT in Smart Home Security

Are They Really Secure?

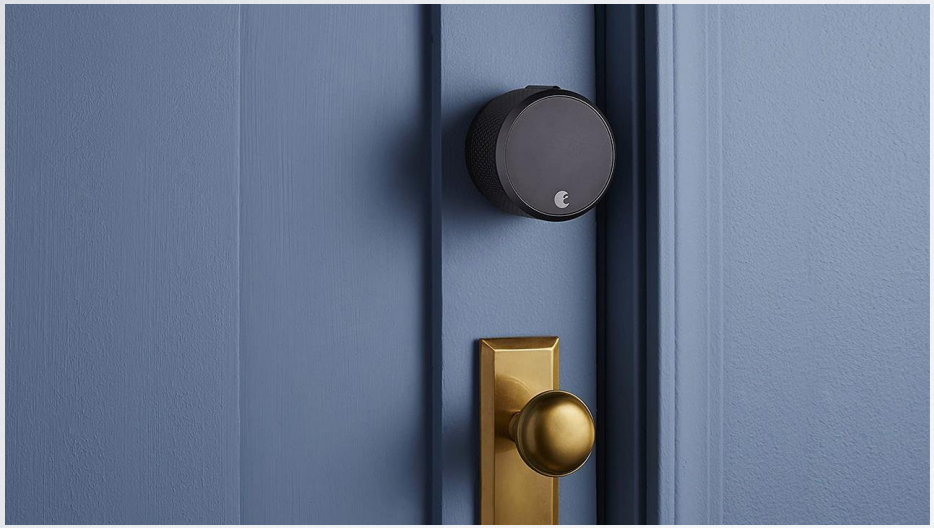
Jinyu Zhao

What is Smart Home

- A smart home allows homeowners to control locks, lights, and other devices remotely using a smartphone or tablet through an internet connection.

Smart Home Security

Access Control



Video Monitoring

Access Control - Smart Lock

- **What is Smart Lock**

A lock with IoT sensors to operate keyless entry remotely, through a smartphone or other internet-connected devices.

- **Why We Use It**
  - Can check remotely if the door is locked.
  - Control guest list, give them permanent or temporary access to the lock.Do not need to give them physical keys.
  - Lock/Unlock using third party devices like Amazon Alexa.

- **How Popular It Is**

According to a report, more than 7 million smart lock units were sold in 2019.

Smart Lock - Vulnerability

- **Cloud Security(Internet-enabled)**

According to a security firm, a threat actor might have the ability to access data stored on cloud servers, including a lock's IP address. It is enough to physically locate and open it.

- **Cloud Monitoring & Lack of Encryption**

If a user sends an unlock command through a smartphone app while the attacker is monitoring the cloud server, he could capture it. At the same time, many smart locks use plain text to communicate between cloud and devices. In U-Tec’s case, it is founded that the app sends unlock command using the same string every time. A researcher replays the string from his laptop, the lock opens without any authorization.

- **Not only the lock itself, the Wi-Fi network can also be hacked**

Smart Lock -

1st: connect to Wi-Fi, no keyboard, need to send credentials

2nd: connect via app, turn to set - up mode, send credential

3rd: The exchange of credentials can be captured

4th: An intruder gain full access to your local network.

Security: control other devices.

Privacy: gain all information transferred through local Wi-Fi

Video Monitoring Smart Camera

- **What Is Smart Camera(IP Camera)**

With a IoT-based camera, the video signals are transmitted over the internet. People use cloud storage to save the video footage for later viewing.

- **Why We Use It**
  - Record both the outside and inside of our home. If a burglary does occur, polices can use these videos to capture the culprit.
  - Checking in on family. (baby monitor)
  - Real-time communication.(door bell)

- **How Popular It Is**

According to a report, more than 54 million smart cameras were sold in 2018.

Smart Camera - Vulnerability

- **Credential Cracking**
The process of guessing at password multiple times until the correct one achieved.

- **Credential Stuffing**
Instead of guessing, hackers use correct passwords directly. They can gain credentials from other data breaches. The combination of large data breaches and reusing of same passwords-make the work easy.(52% reuse)

- **Cloud Misconfiguration(High privacy expectation)**

Smart Camera - Event(Misconfiguration)

- A baby monitor brand called iBaby relies on Amazon Web Service for cloud storage. All the video clips and records are stored in cloud.
- Due to its misconfiguration, a user of one monitor can gain access to all others' cloud-stored videos and pictures. (more about privacy)

Smart Camera - Event(Credential)

- In 2019, Ring urged more than 3,000 users to change their passwords. The reason why was that login information had been exposed online. These passwords could allow bad actors to access someone's Ring app and see live camera footage. However, according to a Ring spokesperson, "there is no evidence of unauthorized intrusion of Ring's system". Instead, the account information might come from other data breaches.(Credential Stuffing)

- A family installed a Ring security camera in the bedroom. Four days after the installation, a built-in speaker started playing songs and a man started speaking from the camera. The family's Ring security system had been hacked. But Ring's security team had no evidence of an unauthorized intrusion. The fact was that malicious actors obtained this user's credential from other services, and reused it to log in to his Ring account.

How to Keep Smart Home Safe

1.Set your router correctly(routers are primary IoT target for hackers)

Change router's default name

Use highest level of encryption(WPA2 or 3)

2.Use strong password

Use unique and complex passwords for home security.

3.Create a separate Wi-Fi network for IoT devices

As putting IoT devices to separate network, if hackers gain access to your IoT devices, you can prevent other more important and sensitive devices like your laptops and smartphones.

4.Choose devices from huge company

Enable better protection of your data. Stronger ability to publish patches.

5.Keep your device up to date

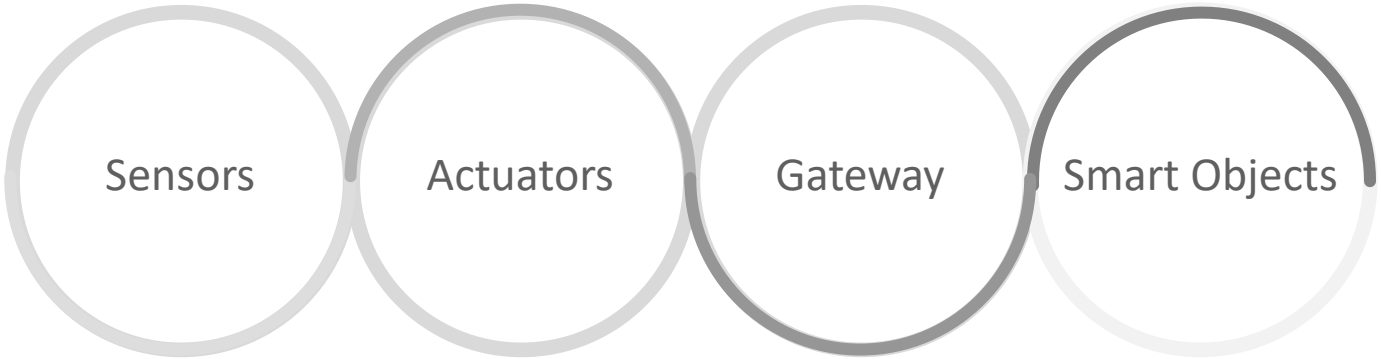
Updates on your devices may not happen automatically, usually need to process security patches by yourself.(fix vulnerabilities)

THANKS FOR LISTENING

Privacy And Security Challenges in Smart Homes

Rosy Zhou

Smart Home Technology



Sensors can range from werables (e.g. bracelets) to non-werable (e.g. IP cameras) sensors. Video cameras and microphones are most privacy-violating sensors.

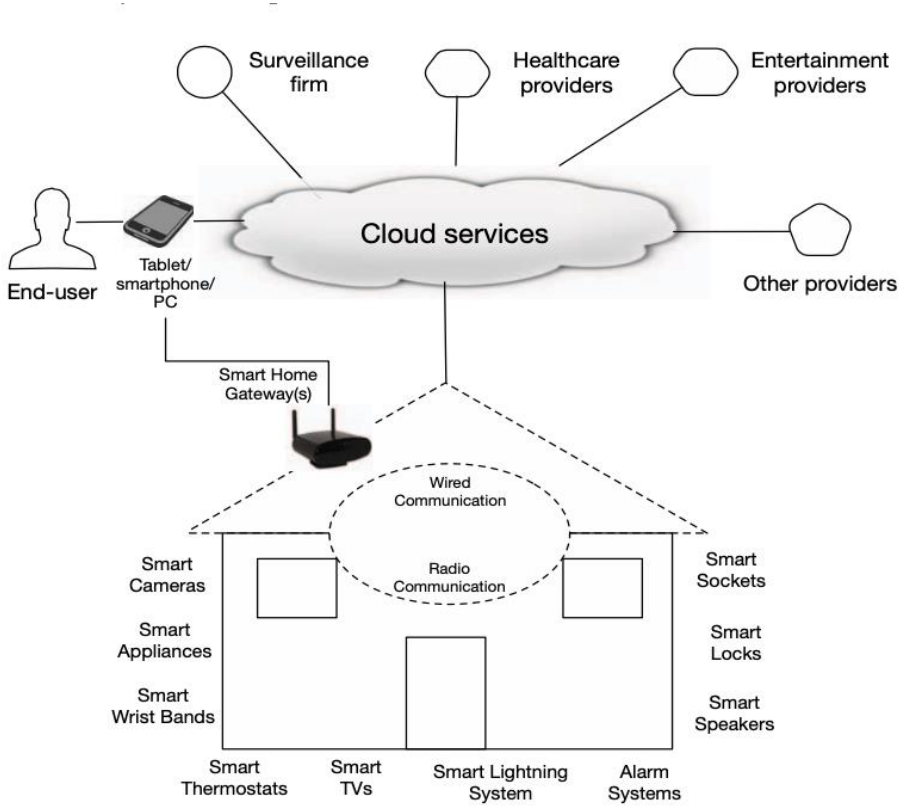
Actuators perform actions such as switching on/off or dimming lights, closing windows, triggering alarms, etc.

Gateway serves as an access point to the home commonly allowing the owner to monitor, control, and manage the home appliances or sensors remotely. Also, it serves as an aggregation point in order to send data to an external network such as utility companies.

Smart objects are devices composed of sensors or actuators, that are connected to the Home Area Network. E.g. smart appliances such as smart locks that answer doorbells and provide for time-based access controls.

Smart Home Architecture

Devices (sensors and actuators), equipped with a telecommunication interface, a processing unit, limited storage and software applications are connected to the internet. IoT enables the integration of objects into the internet, establishing the interaction between people and devices among devices.



Vulnerability (1)

Smart homes require very stringent security requirements, due to the importance of the private information a home environment contains. The main challenges present in a smart home that prevent the use of standard security mechanisms adopted in conventional networks are following:

Energy constraints: Majority of smart home devices are designed to work with low-power and reduced-size hardware, which constrain their computing performance and storage capabilities.

Physical Access: in a smart home devices can be left unattended all the time, becoming easy targets of tampering attacks. If an attacker obtains physical access of a device in a smart home, he may be able to extract from a device the pre-defined encryption keys and other sensitive information.

Vulnerability (2)

Unreliable Communications: Majority of the communication protocols do not guarantee reliability of packet delivery. In fact, packets could fail or being damaged due to collisions or highly congested nodes. Retransmissions and error handling algorithms require large overhead, not tolerable in low-power networks devices.

Heterogeneous Communication Protocols: The different communication protocols possibly used to interconnect the devices in a smart connected home require the use of bridges, hubs or gateways. Additionally, a device may use a proprietary protocol (e.g. non IP-based) locally and a standard one to connect to the cloud. These factors coupled with hardware limitations could lead network engineers to opt for weaker encryption schemes.

Nest Thermostat was reported been hacked, 2019

A couple in Wisconsin experienced 24 hours of terror when hackers infiltrated their Nest smart thermostat. They started feeling unusual heat coming from their vents. It wasn't until they started hearing a frightening voice coming from their Nest in the kitchen that they realized what had happened: A hacker had broken into their system. The couple ended up unplugging their Nest system and resetting their WiFi. Google responded to the matter, claiming the issue was likely caused by a leak of the couple's password. Google highlighted the importance of setting up two-factor authentication as deterrence against incidents like this in the future.

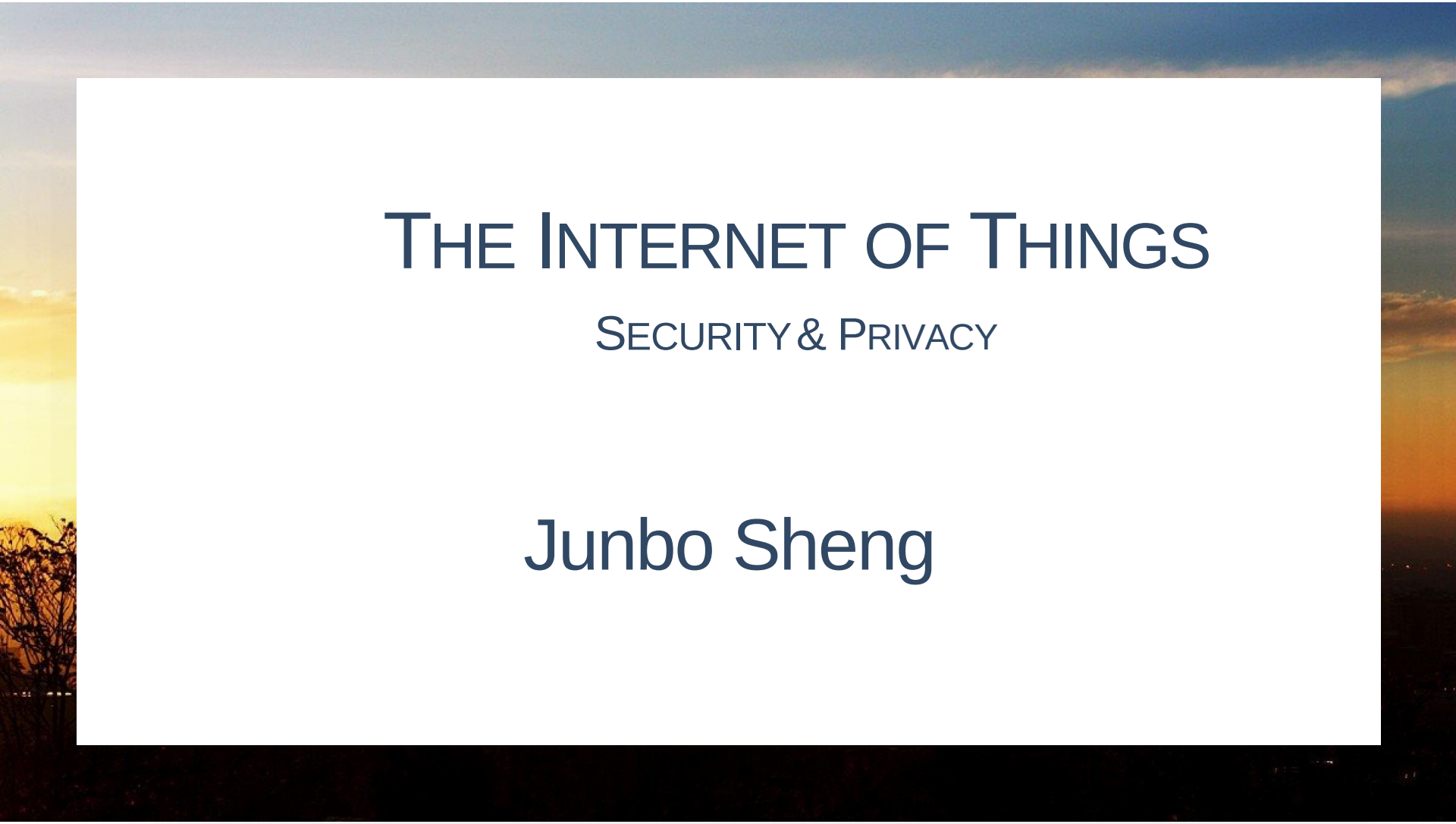
Hacker exploits LIFX mini smart light bulb flaws to extract WiFi credentials, encryption key

It took a hacker less than an hour to hack a smart light bulb and extract the WiFi username and password, which was stored in plaintext on the connected bulb's memory. A security researcher demonstrated three vulnerabilities in an internet-connected LIFX mini white light bulb. Besides extracting the user's WiFi credentials from the LIFX mini, it's also possible to extracted the RSA private encryption key and root certificate, as well as discovered the device had no security settings whatsoever.

Methods to Mitigation Risk

- ***User Authentication:*** Process of software updates, security patches need to be performed by authorized users only: without strong user authentication, a smart home is vulnerable from attackers.
- ***Device Authentication:*** A smart home network must be protected from compromised nodes' attacks. Device authentication shall provide the ability to identify legitimate devices from unauthorized devices in the smart home network.
- ***Network Monitoring:*** It is fundamental to have an intrusion detection system and monitoring tool to detect network intrusions and report traffic anomalies.
- ***Secure Key Management:*** Since some of the sensor devices are deployed with pre-installed network keys, it is required to have a secure key-management scheme to protect the smart home from attackers that compromised devices inside the network.
- ***Physical Protection:*** Unattended devices become vulnerable to tampering attacks. Tamper resistant devices or anti-reverse engineering schemes would be solutions against tampering attacks.

Thank you!



The Internet of Things

Security & Privacy

Junbo Sheng

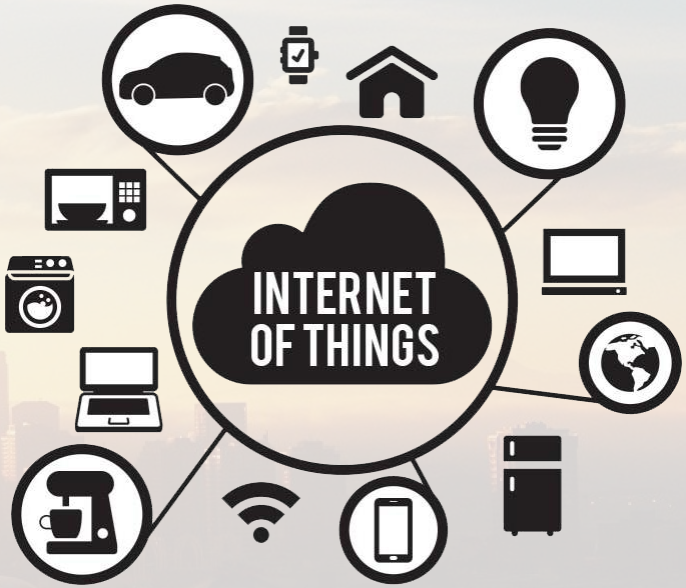
IOT PRIVACY

Devices

- Wearable Gadgets
- Smart Home
- Smart City
- Public Service

Issues

- 98% of all IoT device traffic is unencrypted
- Data Leakage



IOT SECURITY

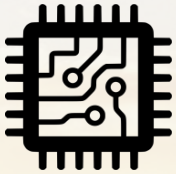
Data Confidentiality

Data Integrity

Data Availability

Authentication

IOT ARCHITECTURE



Perception
Data collection

- RFID
- GPS
- Sensors
- Connected devices

Network
Data transmission

- 4G, 5G
- WiFI, Bluetooth

Processing
Data storage&processing

- Cloud
- Servers

Application
User interaction

- Wearable Gadgets
- Smart home
- Smart city
- Public services

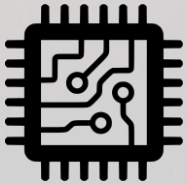
PERCEPTION

Challenges

- Replay Attack
- Timing Attack
- Node Capture
- Fake Node and Malicious Data

Mechanisms

- Authentication
- Encryption
- Anonymity



NETWORK

Challenges

- DoS Attack
- Man-in-The-Middle Attack
- Sybil Attack
- Malicious Code Injection

Mechanisms

- Authentication
- Routing Security

PROCESSING

Challenges

- DoS Attack
- Unauthorized Access
- Malicious Insider

Mechanisms

- Authentication
- Encryption
- Intrusion Detection

APPLICATION

Challenges

- DoS Attack
- Phishing
- Malicious Code Attack

Mechanisms

- Authentication
- Encryption
- Intrusion Detection
- Firewall


Thank You

US warns of cyberattacks targeting medical devices – RT 14 June 2013

- The FDA is warning that implanted medical devices, such as pacemakers and defibrillators, are often connected to networks that are vulnerable to cyber attacks that could shut down or manipulate the machinery.
- Hackers with malicious intentions could introduce malware into the equipment, thereby gaining access to configure settings in medical devices or hospital networks, the Food and Drug Administration said in a warning sent to hospitals, medical device manufacturers, user facilities, and biomedical engineers.
- “Over the past year, we’ve become increasingly aware of cyber security vulnerabilities in incidents that have been reported to us,” William Maisel, deputy director for science at the FDA’s Center for Devices and Radiological Health, told Reuters. “Hundreds of medical devices have been affected, involving dozens of manufacturers.”
- Maisel noted that most of the infections were most likely unintentional, but that they demonstrate a very real possibility that hackers could intentionally inflict damage upon them.
- The FDA report identified 300 medical devices that are at risk of crippling cyber attacks, including insulin pumps, implantable cardioverter defibrillators, anesthesia devices, drug infusion pumps, ventilators, and pacemakers. Some of these devices can even be remotely accessed through the Internet, the FDA report said.

Good Practices / Isolation

- For manipulators
- How we connect
  - Pairing with local controller
  - Security of Controller then becomes issue
- Local Governor – No override to unsafe states
- Problems arise from conflict between always on access and need to protect.
- Push data from device, rather than pull/poll.
  - But that creates power/efficiency issues

Accessible Telemetry

- GP Devices (smartphones, tablets laptops)
  - More vulnerable to malware and other compromise
  - If compromised can collect event more data than we have configured them to collect.
- Telemetry:
  - Audio, Video, Location, Vibration

Camera Access

- Disable Your Laptop's Built-in Webcam to Protect Your Privacy – Mark Wilson – Lifehacker – 6/27/14
- Windows: Webcams offer a window into your home, and they've been known to targets for malware. If you have a built-in camera, here's how disable it and protect yourself.

- Malware can take over webcams, so there is potential for your camera to spy on you. You can easily disable an external webcam just by unplugging it, but things are a little different for integrated cameras.
- The simple solution is to just pop a piece of tape over the lens, but this is not ideal. Sticky residue is left behind, and there is a risk that your improved privacy shield could fall off. You could turn to third party software, but you can also disable a webcam from within Device Manager.

Turning Devices Off

- How the NSA can 'turn on' your phone remotely – CNN Money June 6 2014 - Jose Pagliery

- Even if you power off your cell phone, the U.S. government can turn it back on.
- That's what ex-spy Edward Snowden revealed in last week's interview with NBC's Brian Williams. It sounds like sorcery. Can someone truly bring your phone back to life without touching it?
- No. But government spies can get your phone to play dead.
- It's a crafty hack. You press the button. The device buzzes. You see the usual power-off animation. The screen goes black. But it'll secretly stay on -- microphone listening and camera recording.

Monitoring Vibration

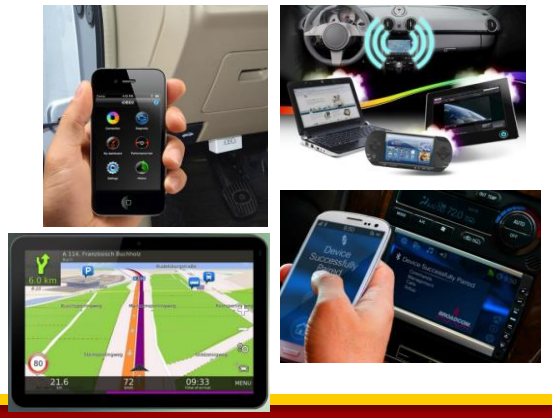
- iPhone Accelerometer Could Spy on Computer Keystrokes – Olivia Salon - Wired UK – 10/19/11
- The accelerometers in many smartphones could be used to decipher what you type into your PC keyboard — including passwords and e-mail content — according to computer scientists at Georgia Tech.
- The technique depends on the person typing at their computer with their mobile phone on the desk nearby. The vibrations created by typing onto the computer keyboard can be detected by the accelerometer of the phone and translated by a program into readable sentences with as much as 80 percent accuracy.
- The technique involves working through probability by detecting pairs of keystrokes, rather than individual keys. It models “keyboard events” in pairs and then works out whether the pair of keys pressed is on the left or the right side of the keyboard and whether they are close together or far apart on the QWERTY keyboard. Once it has worked this out, it compares the results to a preloaded dictionary where each word has been broken down in the same way.

Back to Internet of Things

- At Home
  - HVAC (Climate Control)
  - Internet Web Cameras
  - Television and Entertainment Devices
  - Alarm Systems
  - Doors and Locks
  - Routers and Wifi
  - SAN (Storage Area Networks) network disks
  - Coffee Makers, Toasters, Refrigerators
  - Home Automation, Lights, etc
  - Garage Door Openers

IoT Devices



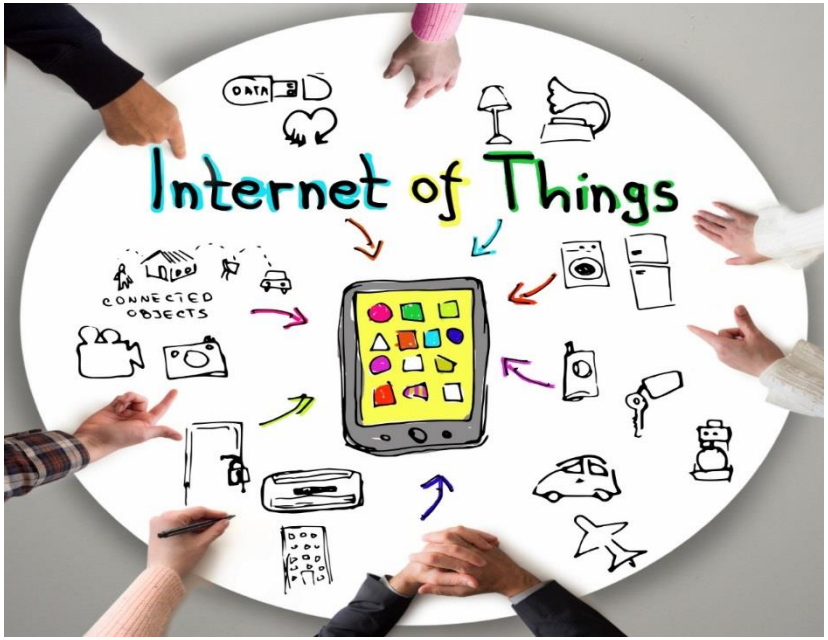



Slide by Veronica Molina

IOT in Home Security Systems

What is the role of IOT here ?

- Embedded devices with minimum CPU, memory and power resources and able to connect to internet.
- Ability of devices to perform actions and not just sense the surroundings.
- Ability to integrate into existing electronic systems at home such as smart phone, computer and other devices.

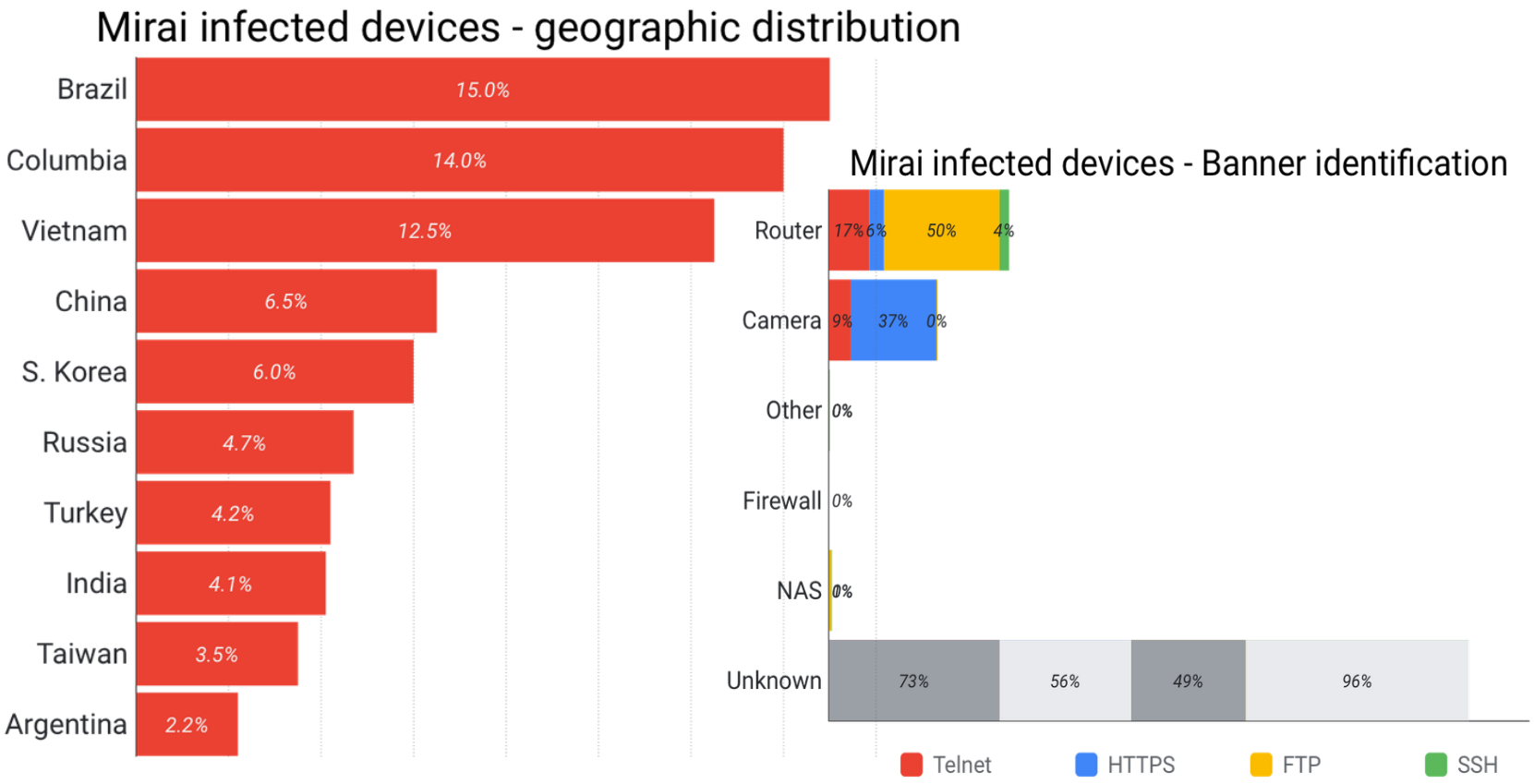


Slide by Veronica Molina

What are the attack surfaces ?

- Insecure web interfaces - Cross site scripting, SQL injection, session management etc.
- Insufficient Authentication / Authorization - Multifactor authentication, secure password recovery mechanism.
- Insecure network services - Open ports, Buffer overflow, Denial-of-Service.
- Lack of data encryption - Unencrypted services via local or internet. SSL/TLS implementation
- Insecure mobile interfaces - Account lock-out, Unencrypted data transfer over network.
- Insufficient security configurations - Granular access control, strong passwords.
- Insecure software / firmware - Updateable software / firmware, Encrypted update files, Update file integrity verification.
- Privacy concern - End to end data encryption, Avoid collection of unnecessary user data, Secure storage of PII information.

The Mirai Botnet?



Standards (or lack of any)

- By default no set rules/standards in designing architecture
- Developments from past year https://www.forbes.com/sites/aarontilley/2016/07/27/two-major-internet-of-things-standards-groups-strike-alliance/#1b42c1cd4520

- This year, US Department of Commerce finally took note of the issue that IoT standards cannot be left to market. www.zdnet.com/article/iot-standards-cannot-be-left-to-the-market-us-department-of-commerce/

CA IoT Security Law

- Effective January 1, 2020 is the California Internet of Things Security Law (the Act)
  - Senate Bill 327, AKA "California's IoT security law" titled Security of Connected Devices
  - Signed into law September 28, 2018 and is the first IoT security law in the nation
  - Aimed at establishing “reasonable security features” for connected devices
- This law applies to any Bluetooth or other device assigned an IP address, including medical devices, copy machines, headsets, automobile entertainment centers, smart watches, smart appliances, etc.

Security & Privacy Requirements

- Manufacturer "shall equip the device with a reasonable security feature or features“-
  - Appropriate to the nature and function
  - Appropriate to information collected or used
  - Protect from unauthorized access, destruction, use, modification, or disclosure
- Subject to the preceding requirements, a connected device equipped with a means for authentication outside a local area network will be deemed a reasonable security feature if either of the following requirements are met:
  - Pre-programmed password unique to each device
  - User can change password
- **Note**: The law does not apply to connected devices already subject to federal security standards -
  - HIPAA
  - California's Confidentiality of Medical Information Act

Penalties for Non-Compliance

- Biggest misstep – implementation of set of controls that are not meant specifically for IoT security device.
- Enforcement is instead delegated "exclusively to the California Attorney General, city attorneys, county counsels, and district attorneys."
  - No specificity regarding types of penalties that exist
  - In a nutshell, difficult to penalize organizations for failure to comply, but also difficult prove that there was a violation in the first place.

Potential weaknesses remain

- Unchanged passwords
- Password theft or social engineering
- Password changes in the clear
  - Password entropy

Recommendations

1. At minimum include passwords or shared secrets following legal requirements and policies
2. Certificate-based approach
3. TPM and secure boot to ensure integrity
4. Better to take national or global wide approach, securing all devices rather than controlling which go to California and which do not

Major Issues Many Home IoT Devices

- Many of these devices are general purpose
  - GP interface is hidden, and user only sees application running on top of Linux or other platform.
  - Many IoT devices are not updated/patched regularly to address new vulnerabilities that are discovered. Or updates occur automatically without permission of owner.
  - Many devices enable inbound access through your Firewall.
  - IoT Device is full fleged device on your home network, and if compromised from outside, allows attacker node inside your firewall to attack observe other activity.
  - Many users leave their devices with the default passwords or access controls.
  - May devices enable “open access” to users within local network segement. (open or hacked wifi and other IoT devices can be an issue)

How can I protect myself ?

- As we have seen, its not just the device or the network or clients contributing to vulnerabilities.
- There are many attack surfaces involved and each of them need to be evaluated and secured.
- Understand the security aspects considered by the service provider and the response time to discovered vulnerabilities and frequency of updates to device software or firmware.

How easy is it to hack a home network?

Mark Ward - BBC News – 25 February 2016

My home is under attack - Right now, skilled adversaries are probing its defences seeking a way in. They are swift, relentless and smart. No weakness will escape their notice. But I am not without defences. I've tried to harden the most vulnerable devices to stop them being compromised and I've set up warning systems that should alert me if the attackers get inside. In the end, all that effort was for nothing because the attackers found so many ways to get at me and my home network. And, they said, even if the technology had defeated them, the weakest link of all - me - would probably have let them in.

Swiss cheese - I found out just how severely compromised my home network was in a very creepy fashion. I was on the phone when the web-connected camera sitting on the window sill next to me started moving. The lens crept round until it pointed right at me. I knew that the attackers were on the other end watching what I was doing, and potentially, listening to the conversation. It is a gadget my children and I have used to see if any wildlife passes through our garden and one which many people have for home security or as an alternative baby monitor. I was lucky that I knew my attackers who, at that moment, were sitting in my living room waiting to show me how straightforward it was to subvert these domestic devices. The picture they took of me via the camera was evidence enough.

Inferences from Home Sensors

- Your daily Routine
  - When you leave, get home, what is the best time to burglarize your house.
- What television programs you watch.
  - No more “Nielson families” – your TV or set top box collects this data and sends it to your provider.
- Power consumption can tell a lot about your activities too.

At Work and “On the Road”

- We pair with devices all the time
  - For printing, beaming data
  - NFC for payment
- Attaching to WiFi Hotspots
  - We broadcast the SSID’s with which we usually connect.
  - Evil twin or Rogue free WiFi
- Whenever we attach, it creates a path for malware infection, or for data to be collected by “peer”.
  - E.g. contact list on bluetooh connected audio in rental car.

In Our Vehicles

- Our vehicles are part of the IoT
  - OBDII
  - Wifi Hotspots
  - Entertainment systems
  - Blue tooth connectivity to our cellphones
    - Discussed earlier
  - Navigation
- Is your car Spying on You
  - NBC LA – November 15 2015
- Consider multi-step attacks
  - Cellphone malware – Entertainment - OBDII

Current Event Discussion

- http://csclass.info/USC/INF529/s21-lec8-ce.html