Internet of Things

Lecture 13

Security and Privacy 3

Attack vectors and examples

Michael Engel

Attacks on IoT security

- Security is still one of the most urgent problems for IoT systems

The "s" in IoT stands for "security"

- **Challenge:** Security is difficult to implement due to limited computational resources, cost pressure, inexperienced developers from an application domain, insufficient hardware protection in small microcontrollers and applications as well as operating systems deficiencies [1]

- Typical **IoT attack types**:
  - Eavesdropping
  - Privilege escalation attack
  - Brute-force attack
  - Denial of service attack

Attacks on IoT security

- Eavesdropping
  - attacker could monitor targeted networks and steal personal data by exploiting security loopholes and weak connections between IoT devices and the server
- Privilege escalation attack
  - obtain unauthorized access of privileges or elevated rights by a malicious insider or an external attacker
  - threat actors exploit privilege escalation vulnerabilities, e.g. unpatched bugs, misconfiguration, or inadequate access controls
- Brute-force attack
  - most IoT device users keep default or easy-to-remember passwords
  - brute-force attackers can access the targeted IoT connections quickly
  - threat actors guess passwords using dictionaries or common word combinations to penetrate IoT networks
- (Distributed) Denial of service attack ((D)DoS)
  - overloading of the network connection of IoT devices to impede connectiviy and data exchange

Examples of IoT attacks: Mirai botnet

- The **Mirai botnet** (Dyn Attack) – IoT devices as attack vector
  - the largest recorded DDoS attack ever was launched in 2016 on service provider Dyn using an IoT botnet
  - huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN

- **IoT botnet** was made possible by a malware called Mirai
  - infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware

What do we know about Mirai?

- Malware that turns networked Linux devices into remotely controlled bots used as part of a botnet in large-scale attacks
- Primarily targets consumer devices such as IP cameras and home routers
- Devices infected by Mirai continuously scan the internet for the IP address of Internet of things (IoT) devices
  - Mirai includes a table of IP address ranges that it will not infect, including addresses allocated to the US Postal Service and DoD
- Mirai identifies vulnerable IoT devices using a table of more than 60 common factory default usernames and passwords,
  - logs into them to infect them with the Mirai malware
  - device remains infected until it is rebooted (malware in RAM)
  - Mirai will identify any "competing" malware, remove it from memory, and block remote administration ports
- DDoS attack Sept. 2016 on the Krebs on Security site reached 620 Gbit/s [3], 1 Tbit/s attack on French web hoster OVH recorded [4]

Mirai password lists

- Example from the source code [6]…

```
124     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x41\x11\x17\x13\x13", 10);                 // root     xc3511
125     add_auth_entry("\x50\x4D\x4D\x56", "\x54\x4B\x58\x5A\x54", 9);                      // root     vizxv
126     add_auth_entry("\x50\x4D\x4D\x56", "\x43\x46\x4F\x4B\x4C", 8);                      // root     admin
127     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C", 7);                  // admin    admin
128     add_auth_entry("\x50\x4D\x4D\x56", "\x1A\x1A\x1A\x1A\x1A\x1A", 6);                  // root     888888
129     add_auth_entry("\x50\x4D\x4D\x56", "\x5A\x4F\x4A\x46\x4B\x52\x41", 5);              // root     xmhdipc
130     add_auth_entry("\x50\x4D\x4D\x56", "\x46\x47\x44\x43\x57\x4E\x56", 5);              // root     default
131     add_auth_entry("\x50\x4D\x4D\x56", "\x48\x57\x43\x4C\x56\x47\x41\x4A", 5);          // root     juantech
132     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17\x14", 5);                  // root     123456
133     add_auth_entry("\x50\x4D\x4D\x56", "\x17\x16\x11\x10\x13", 5);                      // root     54321
134     add_auth_entry("\x51\x57\x52\x52\x4D\x50\x56", "\x51\x57\x52\x52\x4D\x50\x56", 5);  // support  support
135     add_auth_entry("\x50\x4D\x4D\x56", "", 4);                                          // root     (none)
136     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x52\x43\x51\x51\x55\x4D\x50\x46", 4);      // admin    password
137     add_auth_entry("\x50\x4D\x4D\x56", "\x50\x4D\x4D\x56", 4);                          // root     root
138     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x10\x11\x16\x17", 4);                      // root     12345
139     add_auth_entry("\x57\x51\x47\x50", "\x57\x51\x47\x50", 3);                          // user     user
140     add_auth_entry("\x43\x46\x4F\x4B\x4C", "", 3);                                      // admin    (none)
141     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51", 3);                          // root     pass
142     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x43\x46\x4F\x4B\x4C\x13\x10\x11\x16", 3);  // admin    admin1234
143     add_auth_entry("\x50\x4D\x4D\x56", "\x13\x13\x13\x13", 3);                          // root     1111
144     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x51\x4F\x41\x43\x46\x4F\x4B\x4C", 3);      // admin    smcadmin
145     add_auth_entry("\x43\x46\x4F\x4B\x4C", "\x13\x13\x13\x13", 2);                      // admin    1111
146     add_auth_entry("\x50\x4D\x4D\x56", "\x14\x14\x14\x14\x14\x14", 2);                  // root     666666
147     add_auth_entry("\x50\x4D\x4D\x56", "\x52\x43\x51\x51\x55\x4D\x50\x46", 2);          // root     password
```

Which devices were vulnerable?

- Which devices and hardware makers were being targeted? [5]
  - easy to tell from looking at the list of usernames and passwords included in the Mirai source code (available on github [6])
- Device types
  - IP cameras
  - routers
  - printers
  - VoIP phones
  - speakers
  - TV receivers
  - digital video recorders
- Many different manufacturers

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

How could Mirai log in to the IoT devices?

- Many IoT devices in the home are behind a NAT router [7]
  - "Network address translation": customers are assigned one public IP address by their network provider, NAT coordinates the multiplexing of connections from the private home network
  - This normally makes devices behind the NAT router (e.g. in a non-routable 192.168.x.x network) inaccessible from the outside

- However, many IoT devices use Universal Plug and Play (UPnP)
  - technology to automatically open specific ports
  - essentially poking a hole in the router's shield for that device that allows it to be communicated with from the wider Internet
  - this exposed TCP and UDP ports of vulnerable devices to attackers

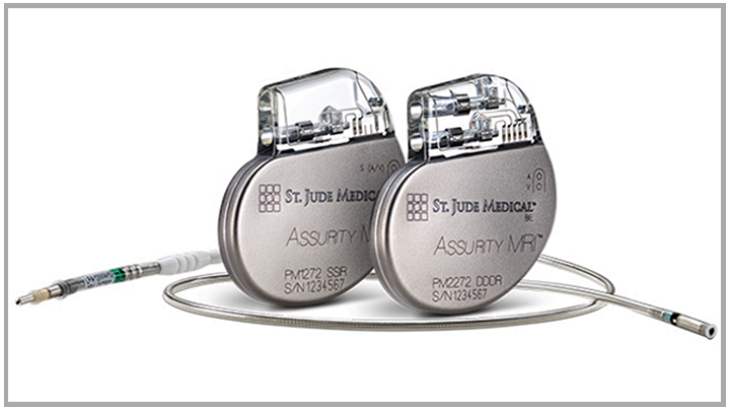
IoT security lessons learned from Mirai

- Mirai did ***not*** rely on a security deficiency of the Linux kernel!

- Devices that cannot have their software, passwords, or firmware updated should never be implemented
- Changing the default username and password should be mandatory for the installation of any device on the Internet
- Passwords for IoT devices should be unique per device, especially when they are connected to the Internet
- Always patch IoT devices with the latest software and firmware updates to mitigate vulnerabilities

- As of 2016, several IoT device makers — including Hikvision, Samsung, and Panasonic — have begun to require unique passwords by default, with most forcing a mix of upper and lowercase letters, numbers, and special characters
  - …but there are lots of new vulnerable devices on the market every month

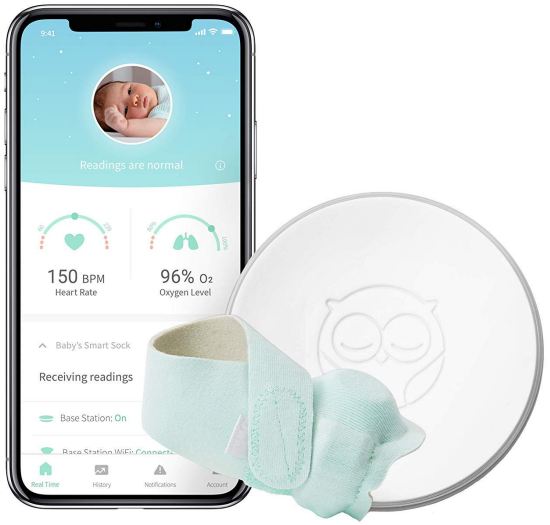
Examples of IoT attacks: Hackable Cardiac Devices



- St. Jude Medical's implantable cardiac devices had vulnerabilities that could allow a hacker to access a device – 465,000 devices affected
- Once in, they could ***deplete the battery*** or ***administer incorrect pacing or shocks*** (according to the US FDA) [8]
- The devices, like pacemakers and defibrillators, are used to monitor and control patients' heart functions and prevent heart attacks
- The vulnerability occurred in the transmitter that reads the device's data and remotely shares it with physicians
  - Hackers could control a device by accessing its transmitter
- Firmware update was provided by the manufacturer ***after five months***
  - *addresses some, but not all, known cyber security problems* (according to FDA)
  - Takes three minutes in-person with the patient's provider
  - This update cannot be done from home
  - The device will run on backup mode during the process, but all life-sustaining features will still be available…

Examples of IoT attacks: WiFi Baby Heart Monitor

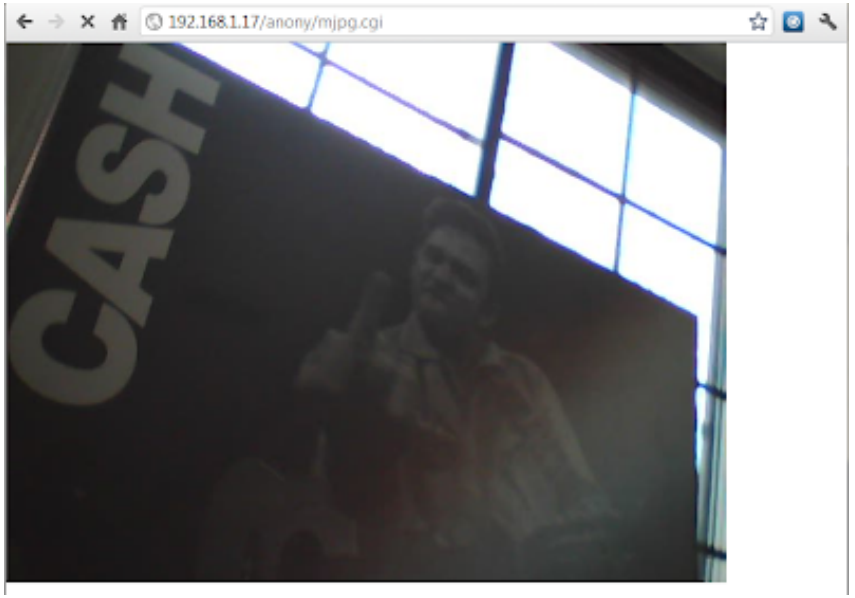
- Another medical device affected:
  Owlet WiFi baby heart monitor
  - Sensor babies wear in a sock that monitors their heartbeat and relays data wirelessly to a nearby hub
  - Tagged "worst IoT security of 2016" by The Register [9]
- *End-user license agreement has a big section indemnifying the company from litigation if the device malfunctions and the wearer dies*



- Owlet base station encrypts data sent to and received from the manufacturer's servers, which contact parents' phones if needed
- But the ***ad-hoc Wi-Fi network*** linking the base station to the sensor device ***is completely unencrypted*** and ***doesn't require any authentication*** to access
- A single unauthenticated command over HTTP can make the Owlet base station leave your home Wi-Fi network and join one of one's choosing
  - One can also take control of the system and monitor a stranger's baby and prevent alerts from being sent out…

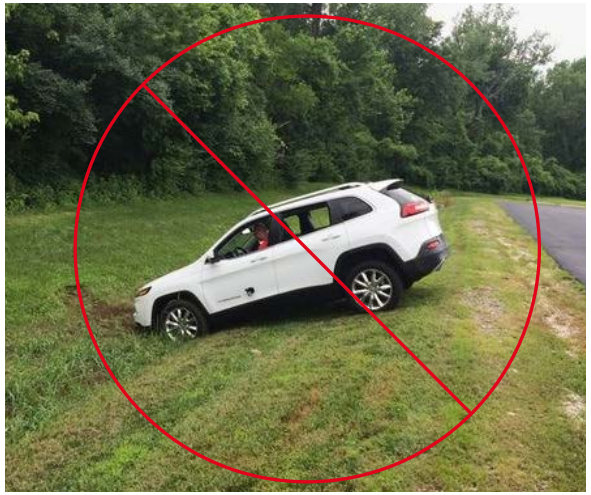
Examples of IoT attacks: TRENDnet Webcam Hack

- TRENDnet "*SecurView*" networked cameras
  - various uses ranging from home security to baby monitoring
  - hack allowed attackers to view video streams [11]
  - access to `http://[ip]/anony/mjpg.cgi` enables watching the camera video stream without requiring credentials
  - at least 9500 affected cameras found by an internet scan
- Further, from at least April 2010 until about January 2012, TRENDnet transmitted user login credentials in clear, readable text over the Internet
  - mobile apps for the cameras also stored consumers' login information in clear, readable text on their mobile devices



Examples of IoT attacks: Jeep Hack

- Jeep hack: take total control of a Jeep SUV using the vehicle's CAN bus
  - reported by the IBM security intelligence website [12]
- By exploiting a firmware update vulnerability, security researchers hijacked the vehicle over the *Sprint cellular network*
  - could make it ***speed up, slow down, and even veer off the road***
- ***Vulnerability:*** a wide open port 6667 [13,14] – D-Bus over IP protocol
- 1.4 million cars were recalled



```
$ telnet 192.168.5.1 6667
Trying 192.168.5.1...
Connected to 192.168.5.1.
Escape character is '^]'.
a
ERROR "Unknown command"
```

Conclusion

- IoT devices can be attacked…
  - in order to compromise information on them
  - in order to use them for DDoS network attacks
    - especially attractive due to the large number of identical networked devices

- Underlying security problems…
  - not always a "classical" security hole, e.g. an exploit for a buffer overflow in C code
  - often, sloppy configuration or badly written user-level code
  - also, often a "layer 8 problem" – users are overwhelmed by the complexity of managing IoT devices

References

[1] Zhi-Kai Zhang et al. *IoT security: ongoing challenges and research opportunities,* 7th intl. conference on service-oriented computing and applications. IEEE, 2014

[2] John Biggs, *Hackers release source code for a powerful DDoS app called Mirai*, TechCrunch, Oct 10, 2016
https://techcrunch.com/2016/10/10/hackers-release-source-code-for-a-powerful-ddos-app-called-mirai/

[3] The Economist, *The internet of stings*, 8 October 2016

[4] Douglas Bonderud, *Leaked Mirai Malware Boosts IoT Insecurity Threat Level,* https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/

[5] Brian Krebs, *Who Makes the IoT Things Under Attack*, October 2016 https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

[6] Mirai source code – https://github.com/jgamblin/Mirai-Source-Code

[7] K. Egevang and Paul Francis. RFC631: *The IP network address translator (NAT)*, 1994

[8] https://www.healthcareitnews.com/news/fda-patients-st-jude-pacemakers-update-needed-keep-hackers-out-devices

[9] https://www.theregister.com/2016/10/13/possibly_worst_iot_security_failure_yet/

[10] https://www.wired.com/2012/02/home-cameras-exposed/

[11] http://console-cowboys.blogspot.com/2012/01/trendnet-cameras-i-always-feel-like.html

[12] Jeep Case Study and the Automotive Cybersecurity Framework (CMU Webinar) https://resources.sei.cmu.edu/asset_files/webinar/2016_018_100_465585.pdf

[13] https://www.darkreading.com/risk/jeep-hack-0day-an-exposed-port

[14] https://illmatics.com/Remote%20Car%20Hacking.pdf