IoT security from the consumer’s perspective

Jorge Pinto

Confraria de Segurança da Informação
24th June 2015
AP2SI

Born in 2012, AP2SI is a non lucrative private association characterized by:

- Openness by associating with every individual to help in information security matters;
- Focus with the dedication to fulfill its objectives and mission;
- Non competitive: has no goal in information security services;
- Independent: not controlled by organizations.
- From concerned individuals to the society.
Mission

Actively contribute to the information security mindset development in Portugal:

- Raising awareness to the value of information and requirements to protect it;
- Developing guidelines/best practices to enhance knowledge and help qualifying information security personnel;
So....

What is the IoT?

(from the consumer’s perspective)
The IoT is cool, right?

Well... yes... kind of...
Smart home hacking is easier than you think

Scary stories of hacking Internet of Things devices are emerging, but how realistic is the threat?

By Colin Neagle | Follow
Network World | Apr 2, 2015 4:14 AM PT

http://www.networkworld.com/article/2905053/security0/smart-home-hacking-is-easier-than-you-think.html
Dick Cheney had the wireless disabled on his pacemaker to avoid risk of terrorist tampering

By Carl Franzen on October 21, 2013 06:54 pm  @carlfranzen

Insulin pump hack delivers fatal dosage over the air

Sugar Blues, James Bond style

27 Oct 2011 at 06:23, Dan Goodin

In a hack fitting of a James Bond movie, a security researcher has devised an attack that hijacks nearby insulin pumps, enabling him to surreptitiously deliver fatal doses to diabetic patients who rely on them.

The attack on wireless insulin pumps made by medical devices giant Medtronic was demonstrated Tuesday at the Hacker Halted conference in Miami. It was delivered by McAfee's Barnaby Jack, the same researcher who last year showed how to take control of two widely used models of automatic teller machines so he could to cause them to spit out a steady stream of dollar bills.

Jack's latest hack works on most recent Medtronic insulin pumps, because they contain tiny radio transmitters that allow patients and doctors to adjust their functions. It builds on research presented earlier this year that allowed the wireless commandeering of the devices when an attacker was within a few feet of the patient, and knew the serial number of his pump. Software and a special antenna designed by Jack allows him to locate and seize control of any device within 300 feet, even when he doesn't know the serial number.

"With this device I created and the software I created, I could actually instruct the pump to perform all manner of commands," Jack told The Register. "I could make it dispense its entire reservoir of insulin, which is about 300 units. I just scan for any devices in the vicinity and they will respond with the serial number of the device."

http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/
Samsung spy telly scandal erupts after firm admits its television will RECORD your "personal and sensitive" conversations

BY JASPER HABILL

New Big Brother telies will make audio recordings and beam them back to mysterious "third parties"
CogniToys: Internet-connected Smart Toys that Learn and Grow

We bring toys to life with speech and a personality, allowing them to interactively engage and grow with a child.

Created by
Elemental Path

2,256 backers pledged $275,000 to help bring this project to life.

https://www.kickstarter.com/projects/522717158/cognitoys-internet-connected-smart-toys-that-learn
An anthropomorphic device, perhaps in the form factor of a doll or toy, may be configured to control one or more media devices. Upon reception or detection of a social cue, such as movement and/or a spoken word or phrase, the anthropomorphic device may interpret the social cue and map it to a media device command. Then, the anthropomorphic device may transmit the media device command to a media device, instructing the media device to change state.
HYUNDAI IS THE FIRST AUTOMAKER TO LAUNCH ANDROID AUTO

Miles Johnson
Manager, Connected Care Publicity
(714) 366-1948
Miles.Johnson@hmausa.com

Fueling a New Generation of Health Insights

People today want more information to inform the decisions they make about their health. Many different factors that affect one's health: nutrition, lifestyle, medical history - and today, much of this information can be captured in data. **Personal fitness trackers, wearable health monitors, and other connected devices are generating more and more data every day**. But without a glimpse into all the information out there, individuals only receive a fragmented view of the whole picture.

For the first time, IBM Watson Health is creating a more complete and personalized picture of health, powered by cognitive computing. Now individuals are empowered to understand more about their health, while doctors, researchers, and insurers can make better, faster, and more cost-effective decisions.

BIOTECHNOLOGY

Electronic Tattoos for Baby and You

MAR 11, 2014 02:35 PM ET // BY GLENN ZORPETTE, IEEE SPECTRUM

Athletes, soldiers, and just about everybody else in the future will have embedded electronic tattoos.
FRANKY DE MEYER/GETTY IMAGES

A baby born five to 10 years from now in a developed country may get a tattoo not long after her first feeding. It would be an integrated circuit, a discreet and flexible affair, smaller than a postage stamp and probably placed on the chest. It would monitor such biometric parameters as electrocardiogram (EKG), physical activity, nutritional status, sleep duration, breathing rate, body

IoT funnel

- communications
- devices
- protocols

code
...and...

we know that everyone can code
...but, can they code securely?
An average of 19 vulnerabilities per day were reported in 2014, according to the data from the National Vulnerability Database (NVD) - http://nvd.nist.gov/

<table>
<thead>
<tr>
<th>Year</th>
<th># of vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>4,258</td>
</tr>
<tr>
<td>2011</td>
<td>3,532</td>
</tr>
<tr>
<td>2012</td>
<td>4,347</td>
</tr>
<tr>
<td>2013</td>
<td>4,794</td>
</tr>
<tr>
<td>2014</td>
<td>7,038</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application</th>
<th># of vulnerabilities</th>
<th># of HIGH vulnerabilities</th>
<th># of MEDIUM vulnerabilities</th>
<th># of LOW vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet</td>
<td>242</td>
<td>220</td>
<td>22</td>
<td>0</td>
</tr>
<tr>
<td>Explorer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Google Chrome</td>
<td>124</td>
<td>86</td>
<td>38</td>
<td>0</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>117</td>
<td>57</td>
<td>57</td>
<td>3</td>
</tr>
<tr>
<td>Adobe Flash Player</td>
<td>76</td>
<td>65</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>Oracle Java</td>
<td>104</td>
<td>50</td>
<td>46</td>
<td>8</td>
</tr>
<tr>
<td>Mozilla Thunderbird</td>
<td>66</td>
<td>36</td>
<td>29</td>
<td>1</td>
</tr>
<tr>
<td>Mozilla Firefox ESR</td>
<td>61</td>
<td>35</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>Adobe Air</td>
<td>45</td>
<td>38</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Apple TV</td>
<td>86</td>
<td>29</td>
<td>49</td>
<td>8</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>44</td>
<td>37</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>Adobe Acrobat</td>
<td>43</td>
<td>35</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>Mozilla SeaMonkey</td>
<td>63</td>
<td>28</td>
<td>34</td>
<td>1</td>
</tr>
</tbody>
</table>

Total Number Of Apps By App Store

- iOS App Store
- Google Play
- Amazon Appstore

Source: appFigures

Business Insider

...so...

what can we do?

to raise consumer awareness
and improve security using market rules
One way is to promote self assessments
Another is to legislate
Better yet – use both
No testing
No controls

Full testing
Existing Controls
Score

Access Controls

Code Testing

User Agreements Transparency

Encryption

Privacy

Tampering

Resilience

Supply chain

Cloud

ToU transparency

Local vs remote (maintenance/comms, etc.)

Not Exaustive
This presentation was inspired by:

**Building Code for Medical Device Software Security** by Tom Haigh e Carl Landwehr

**I Am The Cavalry**
*Five Star Automotive Cyber Safety Framework*

https://www.youtube.com/watch?v=oqe6S6m73Zw
Thank you for your time

Questions?
Find us on:
https://ap2si.org
https://facebook.com/ap2si

Find me on:
jorge.pinto@ap2si.org
https://www.linkedin.com/in/jorgepinto