The Internet of Unpatched Things

Sarthak Grover and Nick Feamster
Princeton University
Current State of Consumer Smart Devices

- Many different manufacturers, small startups, novice programmers
- Low capability hardware, not enough for security protocols
- Most data goes to an online server on the cloud
- Even devices in the same home communicate via the cloud
Unpatched IoT Devices Put Our Privacy at Risk

IoT device network traffic:

- Leaks user information
- Identifies the device being used
- May also identify current user activity and behavior!

email:xxx@y.com

URI: smart-light

json: {'activity': 'switch_on'}
Case Study of Some Common Home IoTs

- Ubi Smart Speaker
- Sharx Security IP Camera
- PixStar Digital Photoframe
- SmartThings Hub
- SmartSense Multi-sensor
- Belkin WeMo Switch
- Nest Thermostat
- Ubi Smart Speaker
- Laptop Gateway (Passive Monitor)
Digital Photoframe: Traffic Analysis

- All traffic and feeds (RSS) cleartext over HTTP port 80
- All actions sent to server in HTTP GET packet
- Downloads radio streams in cleartext over different ports
- DNS queries: api.pix-star.com, iptime.pix-star.com
Photoframe: Privacy Issues

- User email ID is in clear text when syncing account
- Current user activity in clear text in HTTP GET
- DNS queries and HTTP traffic identifies a pix-star photoframe
IP Camera: Traffic Analysis

- All traffic over cleartext HTTP port 80, even though viewing the stream requires login password
- Actions are sent as HTTP GET URI strings
- Videos are sent as image/jpeg and image/gif in the clear
- FTP requests also sent in clear over port 21, and FTP data is sent in clear text over many ports above 30,000
- DNS query: www.sharxsecurity.com
IP Camera: Privacy Issues

- **Video can be recovered** from FTP data traffic by network eavesdropper
- DNS query, HTTP headers, and ports identify a Sharx security camera

<table>
<thead>
<tr>
<th>Sequence</th>
<th>IP Address</th>
<th>Port</th>
<th>Protocol</th>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>14.679939608</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>9</td>
<td>14.820736600</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>10</td>
<td>14.821660000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 TCP</td>
</tr>
<tr>
<td>11</td>
<td>14.823297000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>12</td>
<td>14.957638000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>13</td>
<td>14.959688000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 TCP</td>
</tr>
<tr>
<td>14</td>
<td>14.995143000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 TCP</td>
</tr>
<tr>
<td>15</td>
<td>15.892593000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>31786</td>
<td>60649 TCP</td>
</tr>
<tr>
<td>16</td>
<td>15.893262000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 TCP</td>
</tr>
<tr>
<td>17</td>
<td>15.896821808</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>18</td>
<td>15.230540000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 TCP</td>
</tr>
<tr>
<td>19</td>
<td>15.231793000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>45962</td>
<td>21 FTP</td>
</tr>
<tr>
<td>20</td>
<td>15.233158000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>21</td>
<td>15.233544000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>22</td>
<td>15.233885000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>23</td>
<td>15.371483000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>31786</td>
<td>60649 TCP</td>
</tr>
<tr>
<td>24</td>
<td>15.371922000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>31786</td>
<td>60649 TCP</td>
</tr>
<tr>
<td>25</td>
<td>15.372409000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>26</td>
<td>15.372557000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>27</td>
<td>15.372976000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
<tr>
<td>28</td>
<td>15.373113000</td>
<td>10.42.0.44</td>
<td>46.252.157.130</td>
<td>66649</td>
<td>31786 FTP-DATA</td>
</tr>
</tbody>
</table>
Ubi: Traffic Analysis

- All voice-to-text traffic sent in clear over port 80
- Activities sent in clear, and radio streamed over port 80
- Sensor readings are synced with server in the background over port 80
- Only communication with google API used HTTPS on port 443 and port 5228 (google talk)
Ubi: Privacy Issues

- Although HTTPS is clearly available, Ubi still uses HTTP to communicate to its portal. Eavesdropper can intercept all voice chats and sensor readings to Ubi’s main portal.
- Sensor values such as sound, temperature, light, humidity can identify if the user is home and currently active.
- Email in the clear can identify the user.
- DNS query, HTTP header (UA, Host) clearly identifies Ubi device.
Nest Thermostat: Traffic Analysis

- All traffic to nest is HTTPS on port 443 and 9543
- Uses TLSv1.2 and TLSv1.0 for all traffic
- We found some incoming weather updates containing location information of the home and weather station in the clear. **Nest has fixed this bug after our report.**
- DNS query: time.nestlabs.com, frontdoor.nest.com, log-rts01-iad01.devices.nest.net. transport01-rts04-iad01.transport.home.nest.com
Nest: Privacy Issues

- Fairly secure device: all outgoing personal traffic, including configuration settings and updates to the server, use HTTPS
- *User zip code bug has been fixed
- DNS query as well as the use of the unique port 9543 clearly identifies a Nest device.
Smartthings Hub: Traffic Analysis

- All traffic over HTTPS on port 443 using TLS v1.2
- No clear text port 80 traffic
- Flows to an Amazon AWS instance running smartthings server
- 3-5 packets update every 10 sec in the background
- DNS query: dc.connect.smartthings.com
Smartthings: Privacy Issues

- Very secure: No information about IoT devices attached to hub is leaked
- Background updates every 10 seconds (over HTTPS) fingerprint the hub
- DNS query identifies Smartthings hub, but not individual devices
Conclusion: Be Afraid!

● Very difficult to enforce security standards
  ○ Multiple manufacturers
  ○ Low capability devices
  ○ Use of non-standard protocols and ports

● Difficult to maintain and patch due to low workforce and/or expertise
  ○ Who is responsible? (ISPs? Consumers? Manufacturers?)
  ○ Who is liable? Who should pay?
Conclusion: Be Afraid!

- Very difficult to enforce security standards
  - Multiple manufacturers
  - Low capability devices
  - Use of non-standard protocols and ports

- Difficult to maintain and patch due to low workforce and/or expertise
  - Who is responsible? (ISPs? Consumers? Manufacturers?)
  - Who is liable? Who should pay?

Can we solve this on the network? If so, how?

- How much information about user behavior do devices leak to the network?
- Can we offload device security to the home gateway or the cloud?
Thanks!
Smartthings: outlet and door sensor

- t=0 to t=100: Switch outlet ON and OFF repeatedly using mobile app
- >t=100: Background activity
- y-axis: Bytes per 10s
Smartthings hub (Work in progress)

- Difference in activity pattern for door sensor and smart outlet
- May identify type of user activity and device category (if not the exact device) from this limited list: http://www.smartthings.com/compatible-products
- Associate network pattern with activity
- Eavesdrop to predict user behavior