Capability Analysis of Internet of Things (IoT) Devices in Botnets & Implications for Cyber Security Risk Assessment Processes (Part One)

Presented by:
Andrew Schmitt
Theresa Chasar
Mangaya Sivagnanam
Andrew Schmitt

- Network Administrator, but more of an Infrastructure and Security Engineer
- Grad Student: Master of Science in Security Technologies – U of M

Favorite part about security: Its challenging and its hard

Favorite IT Literature: 12 Networking Truths (RFC 1925) Published in 1996, still very relevant today
Theresa Chasar

- Sr. Director, Compute & Storage for Newell Brands
- CISSP, Grad Student: Master of Science in Security Technologies – U of M

Favorite part about security: Building systems to protect data

Favorite part of my job: The ever-changing landscape of cybersecurity is fascinating.
Mangaya Sivagnanam

- Sr. Software Engineer, Industrial Control Systems for Ingersoll Rand (Trane)
- CSPO, Grad Student: Master of Science in Security Technologies – U of M

Favorite part about security: Innovation and Engineering to Secure Systems

Favorite Security Phrase: “Hackers only need to get it right once, we need to get it right every time.”
Why Focus on IoT?

Everyone else is, so why not us (Kidding!)
Importance of IoT

• Frequency of IoT botnet DDoS attacks is increasing and is becoming mainstream
• Attacks generating bandwidth traffic over 1 Tb/sec (Becoming Common)
• Limited research on:
  • How to quantify attack capabilities of IoT
  • Identification of specific device capabilities
• Assist risk managers and security architects to understand attack capabilities of IoT
• Spark future research on the topic
Goals of Part One

- Get people talking about all parts of IoT security, not just what to do in the future from a development/manufacturing perspective
- Determine a methodology for quantifying the number of IoT devices used in a single target, non-amplified attack
- Determine a methodology for quantifying the attack capability for IoT devices in a botnet in a single target, non-amplified attack
- Apply methodology for quantifying number of IoT devices used in an attack to analyze information security risk
- Establish a theoretical foundation to pursue additional IoT and DDoS focused research
Current Available Research

• IoT Risk Assessment
  • Number of IoT devices significantly increasing
  • Insufficient authentication, security configurability, firmware updates
  • Lack of encryption

• DDoS and Botnet Attack Capabilities
  • IoT distributed architecture allows attackers to hijack unsecured devices
  • Hijacked devices can be converted to bots that participate in attacks
  • Denial of Service Attacks – pooled comprised devices

• Limited research on:
  • How to quantify attack capabilities of IoT
  • Identification of specific device capabilities
Original Hypotheses

• Available CPU, RAM, and Network Capability will have an impact on IoT device denial of service capability
  • The faster the CPU and the more RAM, the more denial of service capability

• Network capability will not be the limiting factor as devices will not approach the limitation of 802.3 (Ethernet) or 802.11 (Wi-Fi) standards
Definitions: Denial of Service Attacks

- **HTTP GET/POST**: Sending large amount of GET/POST requests that result in the consumption of resources and an inability to respond to legitimate requests.

- **SYN Flood**: Sending SYN messages to a target that results in multiple open TCP connections resulting in an inability to respond to legitimate requests.

- **Reflection Attack**: An attacker sends messages to a third party with a spoofed IP address (the IP address of the target) with the goal of the reply from the third party being larger than the original message.

- **DNS Amplification**: Similar to a reflection attack, the attacker uses a spoofed IP address with the goal of an amplified response from a DNS server to the target (DNS has the ability to send large packets for a small request).
Definitions: Sockets

• This is how devices communicate using TCP/IP
• Sockets are layer 4 on the OSI model (Transport Layer)
• Consists of an IP address and port (i.e. 10.0.0.1:31296)
• Upon a successful socket connection, data can be passed between two points

```python
def rocket_socket (Server_IP, Bind_Port, Bandwidth_File):
    fhand = open(Bandwidth_File, 'r')
    S_data = fhand.read()
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.connect((Server_IP, Bind_Port))
    s.sendall(S_data)
    s.close()
```
Technical Information: Buffers

• An allocation of memory that allows a server to continue to receive packets and hold them in queue until they can be processed
• Often used to compensate for varying speeds between devices
  • Allows two devices of different capability to communicate without high wait times
• Common buffer size: 8,192 bytes
**Definitions: Packets**

- Layer 3 on the OSI model (Network Layer)
- Consists of control information and user data (Payload)
- Total size (data and header) must be between 7 and 65,535 bytes
  - RFC 675 limits TCP/IP packet size to 65,535 bytes
Definitions: HTTP GET/POST Requests

- **GET**: A client requests data and the HTTP server responds with the data or issues an error.

- **POST**: A client submits data to the HTTP server and the HTTP server accepts it (i.e. uploading a document, submitting a web form).

- **Other HTTP requests include**:
  - HEAD
  - PUT
  - DELETE
  - TRACE
  - CONNECT
  - OPTIONS
  - PATCH
Basic Anatomy: Amplification/Reflection Attacks

HTTP Request and Response

1. Browser Request
GET/index.html HTTP/1.1
Source: Spoofed IP of Target
Destination: Legitimate IP

2. Web Server Finds File
var/www/.../index.html

3. Server Response
HTTP/1.1 200 OK
<html>...
</html>

4. Browser Displays Page
Page displayed on Target
Methodology: IoT Emulation Through Virtualization

- Scale CPU and RAM resources through Hyper-V
  - First Condition: Max RAM, scale CPU incrementally
  - Second Condition: Max CPU, scale RAM incrementally
- Linux based client (Emulate IoT devices)
- Windows based web server (Target Box)
- Bandwidth measured at the web server
Methodology: IoT Emulation Through Virtualization
Methodology: Data Collection

• Specify the proper resources for the emulated IoT Device (CPU and RAM)
• Establish a socket using Python scripts on the client and server
• Specify a specific buffer size (in bytes)
• Pass data through the socket
• Measure bandwidth
  • Highest observed bandwidth recorded
Part One
Testing

Single Socket, Single Target
## Raw Data: IoT Emulation

### CPU Resources (GHz)

<table>
<thead>
<tr>
<th>Data</th>
<th>5%</th>
<th>10%</th>
<th>15%</th>
<th>20%</th>
<th>25%</th>
<th>30%</th>
<th>35%</th>
<th>40%</th>
<th>45%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Size (B)</td>
<td>0.11</td>
<td>0.23</td>
<td>0.34</td>
<td>0.45</td>
<td>0.57</td>
<td>0.68</td>
<td>0.79</td>
<td>0.91</td>
<td>1.02</td>
<td>1.14</td>
<td>1.36</td>
<td>1.59</td>
<td>1.82</td>
<td>2.04</td>
<td>2.27</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>482.83</td>
<td>410.42</td>
<td>403.70</td>
<td>347.08</td>
<td>345.88</td>
<td>344.53</td>
<td>345.13</td>
<td>344.58</td>
<td>345.23</td>
<td>342.71</td>
<td>344.07</td>
<td>346.59</td>
<td>343.88</td>
<td>344.66</td>
<td>343.01</td>
<td>362.29</td>
</tr>
<tr>
<td>1024</td>
<td>753.06</td>
<td>653.25</td>
<td>646.67</td>
<td>672.06</td>
<td>637.16</td>
<td>610.21</td>
<td>605.24</td>
<td>614.38</td>
<td>616.23</td>
<td>655.50</td>
<td>646.30</td>
<td>627.04</td>
<td>618.64</td>
<td>612.51</td>
<td>616.11</td>
<td>638.96</td>
</tr>
<tr>
<td>2048</td>
<td>1495.04</td>
<td>1290.24</td>
<td>1280.00</td>
<td>1228.80</td>
<td>1218.56</td>
<td>1218.56</td>
<td>1259.52</td>
<td>1259.52</td>
<td>1280.00</td>
<td>1259.52</td>
<td>1218.56</td>
<td>1218.56</td>
<td>1372.16</td>
<td>1311.20</td>
<td>1279.32</td>
<td></td>
</tr>
<tr>
<td>4096</td>
<td>3072.00</td>
<td>2662.40</td>
<td>3768.32</td>
<td>2662.40</td>
<td>2488.32</td>
<td>2549.76</td>
<td>2457.60</td>
<td>2682.88</td>
<td>2365.44</td>
<td>2529.28</td>
<td>2560.00</td>
<td>2488.32</td>
<td>2529.28</td>
<td>2344.96</td>
<td>2385.92</td>
<td>2636.46</td>
</tr>
<tr>
<td>8192</td>
<td>7321.60</td>
<td>4874.24</td>
<td>5713.92</td>
<td>4843.52</td>
<td>4771.84</td>
<td>4689.92</td>
<td>5376.00</td>
<td>4833.28</td>
<td>4904.96</td>
<td>4935.68</td>
<td>4945.92</td>
<td>4945.92</td>
<td>4710.40</td>
<td>4761.60</td>
<td>4403.20</td>
<td>5068.80</td>
</tr>
<tr>
<td>16384</td>
<td>10905.60</td>
<td>10188.80</td>
<td>9728.00</td>
<td>9318.40</td>
<td>10219.52</td>
<td>9512.96</td>
<td>9728.00</td>
<td>9502.72</td>
<td>9625.60</td>
<td>9625.60</td>
<td>9410.56</td>
<td>9553.92</td>
<td>9738.24</td>
<td>9328.64</td>
<td>9226.24</td>
<td>9707.52</td>
</tr>
<tr>
<td>32768</td>
<td>22282.24</td>
<td>19015.68</td>
<td>19517.44</td>
<td>18769.92</td>
<td>18647.04</td>
<td>18944.00</td>
<td>19872.32</td>
<td>18984.96</td>
<td>18595.84</td>
<td>18780.16</td>
<td>18768.80</td>
<td>18585.60</td>
<td>19087.36</td>
<td>19425.28</td>
<td>18083.84</td>
<td>19030.70</td>
</tr>
<tr>
<td>65536</td>
<td>40048.64</td>
<td>36884.48</td>
<td>36321.28</td>
<td>34385.92</td>
<td>33935.36</td>
<td>34416.64</td>
<td>35164.16</td>
<td>37181.44</td>
<td>42127.36</td>
<td>35706.88</td>
<td>36075.52</td>
<td>35584.00</td>
<td>40325.12</td>
<td>38256.64</td>
<td>40048.64</td>
<td>37097.47</td>
</tr>
</tbody>
</table>

### Bandwidth Observed (Kb/s)

### RAM Resources (MB)

<table>
<thead>
<tr>
<th>Data</th>
<th>10%</th>
<th>15%</th>
<th>20%</th>
<th>25%</th>
<th>30%</th>
<th>35%</th>
<th>40%</th>
<th>45%</th>
<th>50%</th>
<th>60%</th>
<th>70%</th>
<th>80%</th>
<th>90%</th>
<th>100%</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer Size (B)</td>
<td>409.60</td>
<td>614.40</td>
<td>819.20</td>
<td>1024.00</td>
<td>1228.80</td>
<td>1433.60</td>
<td>1638.40</td>
<td>1843.20</td>
<td>2048.00</td>
<td>2457.60</td>
<td>2867.20</td>
<td>3276.80</td>
<td>3686.40</td>
<td>4096.00</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>345.44</td>
<td>346.22</td>
<td>345.10</td>
<td>349.87</td>
<td>343.11</td>
<td>344.82</td>
<td>346.17</td>
<td>345.22</td>
<td>345.25</td>
<td>343.22</td>
<td>344.20</td>
<td>350.10</td>
<td>345.90</td>
<td>343.10</td>
<td>345.55</td>
</tr>
<tr>
<td>1024</td>
<td>613.55</td>
<td>610.57</td>
<td>612.00</td>
<td>611.99</td>
<td>615.17</td>
<td>612.67</td>
<td>613.55</td>
<td>611.10</td>
<td>625.30</td>
<td>622.41</td>
<td>659.11</td>
<td>612.31</td>
<td>613.70</td>
<td>615.16</td>
<td>620.61</td>
</tr>
<tr>
<td>2048</td>
<td>1310.72</td>
<td>1313.72</td>
<td>1317.25</td>
<td>1313.09</td>
<td>1311.11</td>
<td>1313.47</td>
<td>1311.49</td>
<td>1312.99</td>
<td>1228.80</td>
<td>1274.10</td>
<td>1333.90</td>
<td>1317.10</td>
<td>1311.37</td>
<td>1313.66</td>
<td>1305.91</td>
</tr>
<tr>
<td>4096</td>
<td>2426.88</td>
<td>2499.12</td>
<td>2429.11</td>
<td>2417.34</td>
<td>2501.11</td>
<td>2400.84</td>
<td>2412.17</td>
<td>2437.64</td>
<td>2488.32</td>
<td>2497.33</td>
<td>2333.55</td>
<td>2500.00</td>
<td>2429.40</td>
<td>2501.30</td>
<td>2448.15</td>
</tr>
<tr>
<td>8192</td>
<td>4126.72</td>
<td>4200.10</td>
<td>4129.15</td>
<td>4201.71</td>
<td>4100.63</td>
<td>4101.33</td>
<td>4122.10</td>
<td>4206.30</td>
<td>5017.60</td>
<td>5050.80</td>
<td>4207.40</td>
<td>4217.44</td>
<td>4126.66</td>
<td>4100.63</td>
<td>4272.76</td>
</tr>
<tr>
<td>16384</td>
<td>9277.44</td>
<td>9270.11</td>
<td>9276.10</td>
<td>9314.64</td>
<td>9300.98</td>
<td>9207.47</td>
<td>9255.19</td>
<td>9236.50</td>
<td>9502.72</td>
<td>9500.44</td>
<td>9276.66</td>
<td>9274.30</td>
<td>9177.50</td>
<td>9255.11</td>
<td>9294.65</td>
</tr>
<tr>
<td>32768</td>
<td>17991.68</td>
<td>17999.34</td>
<td>17995.44</td>
<td>17876.34</td>
<td>17888.20</td>
<td>17997.60</td>
<td>18004.15</td>
<td>17852.46</td>
<td>17899.52</td>
<td>17774.30</td>
<td>17999.41</td>
<td>17991.66</td>
<td>17944.90</td>
<td>17898.97</td>
<td>17936.71</td>
</tr>
<tr>
<td>65536</td>
<td>34938.88</td>
<td>34200.77</td>
<td>34732.25</td>
<td>34741.95</td>
<td>34900.11</td>
<td>34918.80</td>
<td>34917.77</td>
<td>34219.50</td>
<td>33792.00</td>
<td>34341.20</td>
<td>34744.11</td>
<td>34993.54</td>
<td>34732.50</td>
<td>34918.44</td>
<td>34649.42</td>
</tr>
</tbody>
</table>

### Bandwidth Observed (Kb/s)
## CPU Incremental Testing

<table>
<thead>
<tr>
<th>Buffer Size (B)</th>
<th>5%</th>
<th>25%</th>
<th>50%</th>
<th>80%</th>
<th>100%</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>512</td>
<td>482.83</td>
<td>345.88</td>
<td>342.71</td>
<td>343.88</td>
<td>343.01</td>
<td>362.29</td>
</tr>
<tr>
<td>1024</td>
<td>753.06</td>
<td>637.16</td>
<td>655.50</td>
<td>618.64</td>
<td>616.11</td>
<td>638.96</td>
</tr>
<tr>
<td>2048</td>
<td>1,495.04</td>
<td>1,218.56</td>
<td>1,280.00</td>
<td>1,259.52</td>
<td>1,331.20</td>
<td>1,279.32</td>
</tr>
<tr>
<td>4096</td>
<td>3,072.00</td>
<td>2,488.32</td>
<td>2,529.28</td>
<td>2,529.28</td>
<td>2,385.92</td>
<td>2,636.46</td>
</tr>
<tr>
<td>8192</td>
<td>7,321.60</td>
<td>4,771.84</td>
<td>4,935.68</td>
<td>4,710.40</td>
<td>4,403.20</td>
<td>5,068.80</td>
</tr>
<tr>
<td>16384</td>
<td>10,905.60</td>
<td>10,219.52</td>
<td>9,625.60</td>
<td>9,738.24</td>
<td>9,226.24</td>
<td>9,707.52</td>
</tr>
<tr>
<td>32768</td>
<td>22,282.24</td>
<td>18,647.04</td>
<td>18,780.16</td>
<td>19,087.36</td>
<td>18,083.84</td>
<td>19,030.70</td>
</tr>
<tr>
<td>65536</td>
<td>40,048.64</td>
<td>33,935.36</td>
<td>35,706.88</td>
<td>40,325.12</td>
<td>40,048.64</td>
<td>37,097.47</td>
</tr>
</tbody>
</table>

**Observed Maximum Bandwidth (Kbps)**
CPU Incremental Testing

![Chart showing CPU Incremental Testing with different conditions and buffer sizes. The x-axis represents Buffer Size, and the y-axis represents Observed Maximum Bandwidth (Kbps). The chart includes lines for CPU Resources Allocated (RAM 100%) with varying percentages (5%, 25%, 50%, 80%, 100%) and an average line.](image-url)
## RAM Incremental Testing

<table>
<thead>
<tr>
<th>Buffer Size (B)</th>
<th>RAM Resources Allocated (CPU 100%)</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10%</td>
<td>25%</td>
<td>50%</td>
<td>80%</td>
<td>100%</td>
<td></td>
</tr>
<tr>
<td>512</td>
<td>409.6 MB</td>
<td>1024 MB</td>
<td>2048 MB</td>
<td>3277 MB</td>
<td>4096 MB</td>
<td>345.55</td>
</tr>
<tr>
<td>1024</td>
<td>613.55</td>
<td>611.99</td>
<td>625.30</td>
<td>612.31</td>
<td>615.16</td>
<td>620.61</td>
</tr>
<tr>
<td>2048</td>
<td>1,310.72</td>
<td>1,313.09</td>
<td>1,228.80</td>
<td>1,317.10</td>
<td>1,313.66</td>
<td>1,305.91</td>
</tr>
<tr>
<td>4096</td>
<td>2,426.88</td>
<td>2,417.34</td>
<td>2,488.32</td>
<td>2,500.00</td>
<td>2,501.30</td>
<td>2,448.15</td>
</tr>
<tr>
<td>8192</td>
<td>4,126.72</td>
<td>4,201.71</td>
<td>5,017.60</td>
<td>4,127.44</td>
<td>4,100.63</td>
<td>4,272.76</td>
</tr>
<tr>
<td>16384</td>
<td>9,277.44</td>
<td>9,314.64</td>
<td>9,502.72</td>
<td>9,274.30</td>
<td>9,255.11</td>
<td>9,294.65</td>
</tr>
<tr>
<td>32768</td>
<td>17,991.68</td>
<td>17,876.34</td>
<td>17,899.52</td>
<td>17,991.66</td>
<td>17,898.97</td>
<td>17,936.71</td>
</tr>
<tr>
<td>65536</td>
<td>34,938.88</td>
<td>34,741.95</td>
<td>33,792.00</td>
<td>34,993.54</td>
<td>34,918.44</td>
<td>34,649.42</td>
</tr>
</tbody>
</table>

**Observed Maximum Bandwidth (Kbps)**
RAM Incremental Testing

The graph shows the observed maximum bandwidth (Kbps) as a function of buffer size. The x-axis represents buffer size (512 to 65536) and the y-axis represents observed maximum bandwidth (0 to 40000). The graph includes different allocations of RAM resources allocated with CPU utilization (10%, 25%, 50%, 80%, 100%), and their respective averages. The data indicates an increasing trend in bandwidth with an increase in buffer size for all allocations, with the 100% allocation showing the highest observed maximum bandwidth.
Hypotheses Review

- Okay... So we proved ourselves mostly wrong (better than someone else doing it!)
- **CPU and RAM had no effect** on the ability for a device to transmit more or less bandwidth in a single socket
- No scenario was able to approach the limitations of 802.3 (Ethernet) or 802.11 (wireless) standards (woohoo, we got something right!)
- It turns out that the **buffer size has the most impact on bandwidth**
  - Based on protocols and standards
Analysis Assumptions

- The default buffer size of most web servers is 8,192 bytes
  - All devices are communicating with a target that uses this buffer size
- The average packet size used on the internet is 512 bytes
- Attack is being performed in connection oriented conditions (TCP)
- All devices in the botnet are performing the same type of attack
- The devices in this botnet are attacking a single target
- If the attack uses amplification, each bot achieves the same amount of additional attack capability
- Each device is dedicated to attack capability and is not performing other processes
Risk Assessment
Risk Assessment: IoT Device Implications

• Devices in a single socket, single target attack are not impacted by resource availability
  • Limited to standards and protocols
• All IoT devices are created equal in terms of capability
  • Same amount of risk for high end streaming devices as low end microcomputers

Maximum Bandwidth Generated =
[Average Bandwidth Observed at Specific Buffer Size]
Risk Assessment: IoT Botnet
Capabilities and Implications

• Mirai continues to grow and evolve into more effective variants

• Industry estimates 50 Billion IoT devices by 2020

• IoT devices continue to be consumed into botnets
  • DynDNS: 100,000 bots
  • OVH: 145,000
Risk Assessment: IoT Botnet Capabilities and Implications

Maximum IoT Botnet Capability = [Number of IoT Bots] * [Average Bandwidth Observed at a Specific Buffer Size]

Maximum IoT Botnet Capability = Amplification Factor([Number of IoT Bots] * [Average Bandwidth Observed at a Specific Buffer Size])
Risk Assessment: IoT Botnet Capabilities and Implications

![IoT Botnet Attack Capability Graph](image)
Risk Assessment: IoT Botnet Capabilities and Implications

• 500,000 devices could generate over 2 Tbps of DDoS traffic
  • Non-amplified traffic
  • There are a lot more IoT devices than 500,000 at present
• Approximately 1 Tbps took DynDNS, OVH offline
  • It took about half of that to take down Krebs on Security
• IoT botnets carry a very high risk for enterprises (All enterprises)
Real World: Krebs on Security

• Non-amplified, direct attack
  • HTTP GET, POST
  • SYN

<table>
<thead>
<tr>
<th>Observed DDoS Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>636 Gbps</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Estimated Bandwidth using Bandwidth Calculator</th>
<th>Estimated Number of Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>645 Gbps</td>
<td>145,000</td>
</tr>
</tbody>
</table>
Real World: DynDNS

<table>
<thead>
<tr>
<th>Observed Attack Bandwidth</th>
<th>Industry Estimated Number of Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.2 Tbps</td>
<td>100,000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Amplified Capability</th>
<th>Estimated Amplification Needed to Achieve Observed Attack Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>445 Gbps</td>
<td>Approximately 276% of Original Request Size</td>
</tr>
</tbody>
</table>
Real World: DynDNS

- Original attack capability of approximately 4 Mbps, amplified to approximately 12-13 Mbps of sustained capability
- Each packet sent at 512 Bytes would be amplified to over almost 2 KB
  - Not hard to do
- This is more serious when we start talking about connectionless protocols
  - UDP
  - CLDAP
Risk Assessment: Individuals

- DDoS-ing home users is nothing new
  - In fact, this is where Mirai got its start (allegedly)
- Most home users have somewhere between 10 – 100 Mbps download speeds
- Our findings show that this means anywhere from 6-22 IoT devices in a botnet could result in a denial of service
- This size of botnet is well within the grasp of a script kiddie or someone with a small amount of bitcoin
Risk Assessment: Enterprises

• Large enterprises are being affected now
  • Krebs, OVH, DynDNS

• Majority of enterprises do not have the resources to withstand 1 Tbps of DDoS traffic AND maintain production capability

• In an IoT based botnet attack, there is no level of certainty

• Enterprises have elevated levels of risk
  • Mitigation becomes more difficult when the number of devices attacking an organization reaches the hundreds of thousands
Key Takeaways

• In regards to single socket, single target attacks, the low quality devices perform just like the high quality devices
  • **CPU and RAM have no impact**, devices are limited by standards and protocols
  • Buffer size plays a large role
• IoT based botnets will continue to be a high risk threat in the short and long term
  • Home users and enterprises alike
• Security starts at development, but shouldn’t be the only focus regarding IoT security
  • We need to continue to strive to finds way to defend ourselves
  • There will be another “Mirai” - developing defenses will benefit organizations in the long term
• **There is a need to know more!**
Future Research

- Impact of CPU and RAM on simultaneous multi-targeted attacks
- Impact of embedded architecture vs traditional architecture
- Impact of connectionless vs connection oriented protocols
- Maximum attack capability of amplified/reflected attacks
- Maximum attack capability of mixed method attacks (single target and amplified/reflected attacks)
- Quantification of the number of IoT devices in a botnet of unknown composition
- Determining resiliency of target systems during an attack
  - Number of devices that can attack a system and remain fully functional