GETTING TO THE SOUL OF INCIDENT RESPONSE
A fistful of metrics

John @achillean Matherly
Eireann @blackswanburst Leverett
“Things always become obvious after the fact.”

“Remember that you are a Black Swan.”

- Nassim Nicholas Taleb
The goals of this presentation

Give you metrics you like.

Give you metrics you don’t like.

Make you think, argue, and innovate.

Invent metrics quickly, THEN see if they are useful. NOT present old ones.

The honour of standing in front of you again.

Intellectual explorations for John and I.
Metrics Answer Questions

• Which is more widespread – ELK RCE or Unauthenticated MongoDB?
• What is the SSL capital of the world?
• How many cars in the USA have novelty license plates?
• Which countries are jumping on board IoT?
• Where are the bad neighborhoods of SSL?
• Is Internet-eavesdropping cultural?
Principles we found

If your metric wouldn’t help an attacker why are you measuring it? It’s dual use is a sign of it’s utility for defense!

Reduce external dependencies to ensure reproducibility.

Machine only metrics don’t translate to non-technical folks. That’s why economists say “per capita” and LD-50 is used by toxicologists.

Distributions matter. Populations are important.

All data is biased. Understanding the bias and adjust accordingly.
L-W cost

How does it work:

• Choose a vuln
• Scan network
• Distinguish vulnerable from N/A in total network
• Divide the cost over the vulnerable hosts

Why the cost?

• Because it translates to non-technical
• This is for vulnerability across constituencies.
• It’s easy to talk about.

Example usage:

• SSH brute forcing hosts on our internal network had a L-W cost of $4.89 USD.

Example usage:

• Elastic Search RCE has an L-W cost of $0.00024 across all of IPv4
How can I use it in practice?

1. You can compare networks
2. You can compare change over time
3. You can even imagine vulnerabilities you haven’t seen yet, and see how much effort it would take to patch

<table>
<thead>
<tr>
<th>Day</th>
<th>LW Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monday</td>
<td>$0.00277</td>
</tr>
<tr>
<td>Tuesday</td>
<td>$0.00245</td>
</tr>
<tr>
<td>Wednesday</td>
<td>$0.00256</td>
</tr>
<tr>
<td>Thursday</td>
<td>$0.00254</td>
</tr>
<tr>
<td>Friday</td>
<td>$0.00249</td>
</tr>
</tbody>
</table>

**Table:** CVE-2015-5377 ELK RCE Over time

<table>
<thead>
<tr>
<th>Name</th>
<th>ASN#</th>
<th>Ratio of vuln to visible hosts</th>
<th>LW Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>OVH</td>
<td>as16276</td>
<td>412/1447468</td>
<td>$0.0000015538728352889275</td>
</tr>
<tr>
<td>Amazon</td>
<td>as14618</td>
<td>132/5798144</td>
<td>$0.00019431610902150473</td>
</tr>
<tr>
<td>China Telecom</td>
<td>as4134</td>
<td>110/116815104</td>
<td>$0.00469785982912237</td>
</tr>
<tr>
<td>Net Acces</td>
<td>as8001</td>
<td>106/511232</td>
<td>$0.0000021335651289741947</td>
</tr>
<tr>
<td>Microsoft</td>
<td>as8075</td>
<td>75/12123392</td>
<td>$0.0007150832811991374</td>
</tr>
</tbody>
</table>

**Table:** Top five vulnerable organisations
Explore

Browse interesting projects, solving all types of interesting problems.

3D modeling

Productivity tools

Projects with great wiki

Science

Projects that power Github for Mac

Policies

Javascript game engines

Learn or level up your JS game dev skills and build amazing games together.
Welcome to Stack Overflow

Stack Overflow is a question and answer site for professional and enthusiast programmers. It's built and run by you as part of the Stack Exchange network of Q&A sites. With your help, we're working together to build a library of detailed answers to every question about programming.

We're a little bit different from other sites. Here's how:

Ask questions, get answers, no distractions

This site is all about getting answers. It's not a discussion forum. There's no chit-chat.

Just questions...

...and answers.

Why are function pointers safe?

I have read that converting a function pointer does not change the memory, but is not guaranteed to work. Why is this?
MODBUS QUESTIONS PER YEAR
POPULARITY ON STACKOVERFLOW

- MODBUS: 830
- BAC NET: 180
- SIEMENS S7: 83
- DNP3: 17
- OMRON FINS: 18
- ETHERNET/IP: 15
- NIAGARA FOX: 0
ICS Protocol Growth

- BACnet
- DNP3
- EtherNet/IP
- Modbus
- Niagara Fox
- Niagara Fox + SSL
- Siemens S7
#16 Australia
#17 Hungary
#18 China
#19 Malaysia
#20 Finland
#21 Switzerland
#22 Russia
#23 Lithuania
#14 Brazil
#15 Czech Republic
#16 China
#19 Lithuania
#20 Romania
#21 Russia
#22 Austria
#23 Switzerland
### Countries with the most IoT devices

<table>
<thead>
<tr>
<th>Country</th>
<th>Devices online per 100 people</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td>37.9</td>
</tr>
<tr>
<td>Demark</td>
<td>32.7</td>
</tr>
<tr>
<td>Swizerland</td>
<td>29</td>
</tr>
<tr>
<td>United States</td>
<td>24.9</td>
</tr>
<tr>
<td>Netherlands</td>
<td>24.7</td>
</tr>
<tr>
<td>Germany</td>
<td>22.4</td>
</tr>
<tr>
<td>Sweden</td>
<td>21.9</td>
</tr>
<tr>
<td>Spain</td>
<td>19.9</td>
</tr>
<tr>
<td>France</td>
<td>17.6</td>
</tr>
<tr>
<td>Portugal</td>
<td>16.2</td>
</tr>
<tr>
<td>Belgium</td>
<td>15.6</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>13</td>
</tr>
</tbody>
</table>

Data: Shodan/OECD
## SSL/TLS by sector

<table>
<thead>
<tr>
<th>Sector</th>
<th>Heartbleed</th>
<th>Count</th>
<th>SSLv2</th>
<th>SSLv3</th>
<th>TLSv1</th>
<th>TLSv1.1</th>
<th>TLSv1.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecommunications Services</td>
<td>2550</td>
<td>14357795</td>
<td>494756</td>
<td>663929</td>
<td>3041207</td>
<td>224645</td>
<td>229355</td>
</tr>
<tr>
<td>Industrials</td>
<td>3</td>
<td>11009</td>
<td>352</td>
<td>2176</td>
<td>4347</td>
<td>2498</td>
<td>3019</td>
</tr>
<tr>
<td>Consumer Discretionary</td>
<td>7014</td>
<td>8234391</td>
<td>40276</td>
<td>290888</td>
<td>1491892</td>
<td>1265697</td>
<td>1272378</td>
</tr>
<tr>
<td>Utilities</td>
<td>0</td>
<td>881</td>
<td>40</td>
<td>157</td>
<td>351</td>
<td>253</td>
<td>261</td>
</tr>
<tr>
<td>Consumer Staples</td>
<td>0</td>
<td>6679</td>
<td>43</td>
<td>202</td>
<td>3246</td>
<td>2974</td>
<td>2977</td>
</tr>
<tr>
<td>Health Care</td>
<td>3</td>
<td>10338</td>
<td>232</td>
<td>1433</td>
<td>4759</td>
<td>3520</td>
<td>3755</td>
</tr>
<tr>
<td>Materials</td>
<td>0</td>
<td>2563</td>
<td>104</td>
<td>291</td>
<td>659</td>
<td>398</td>
<td>478</td>
</tr>
<tr>
<td>Information Technology</td>
<td>223</td>
<td>6619025</td>
<td>7592</td>
<td>149568</td>
<td>2721123</td>
<td>2684986</td>
<td>2697873</td>
</tr>
<tr>
<td>Energy</td>
<td>0</td>
<td>2064</td>
<td>62</td>
<td>339</td>
<td>855</td>
<td>630</td>
<td>638</td>
</tr>
<tr>
<td>Financials</td>
<td>0</td>
<td>16338</td>
<td>93</td>
<td>1568</td>
<td>7334</td>
<td>5203</td>
<td>5791</td>
</tr>
<tr>
<td>Country</td>
<td>SSH/People</td>
<td>SSL/People</td>
<td>Telnet/People</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>------------</td>
<td>------------</td>
<td>---------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEYCHELLES</td>
<td>0.040536105</td>
<td>NETHERLANDS</td>
<td>GUAM</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IRELAND</td>
<td>0.030029077</td>
<td>IRELAND</td>
<td>ANTIGUA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINGAPORE</td>
<td>0.028632523</td>
<td>USA</td>
<td>SAINT VINCENT</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAINT VINCENT</td>
<td>0.025676664</td>
<td>LIECHTENSTEIN</td>
<td>NEW CALEDONIA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KYRGYZSTAN</td>
<td>0.021243156</td>
<td>SINGAPORE</td>
<td>SAINT KITTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ANTIGUA</td>
<td>0.017359736</td>
<td>LUXEMBOURG</td>
<td>TRINIDAD &amp; TOBEGO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAINT KITTS</td>
<td>0.017144729</td>
<td>MONACO</td>
<td>DOMINICAN REPUBLIC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NETHERLANDS</td>
<td>0.016761866</td>
<td>ISLE OF MAN</td>
<td>CAYMAN ISLANDS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GUAM</td>
<td>0.013781537</td>
<td>CAYMAN ISLANDS</td>
<td>NORWAY</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>0.012438426</td>
<td>GERMANY</td>
<td>GRENADA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HONG KONG</td>
<td>0.011747104</td>
<td>ITALY</td>
<td>SOUTH KOREA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPv6</td>
<td>IPv4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1. 80</td>
<td>1. 7547</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. 443</td>
<td>2. 80</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. 8080</td>
<td>3. 443</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. 53</td>
<td>4. 5060</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. 81</td>
<td>5. 4567</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. 20000</td>
<td>6. 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. 9080</td>
<td>7. 23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. 8888</td>
<td>8. 8080</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. 9100</td>
<td>9. 53</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. 9000</td>
<td>10. 21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
HTTP vs HTTPS
HTTP vs HTTPS

Most Encrypted
1. Cuba
2. Italy
3. Singapore
4. Guyana
5. Jersey

Least Encrypted
197. Saint Kitts
198. Egypt
199. Syria
200. Saint Vincent
201. Seychelles
Unencrypted vs Encrypted (POP)
Unencrypted vs Encrypted (POP)

**Most Encrypted**
1. Dominica
2. Antarctica
3. South Sudan
4. Turkmenistan
5. Myanmar

**Least Encrypted**
197. Botswana
198. Angola
199. South Korea
200. Mali
201. Swaziland
1.3% Novelty Plates
Universities Needing Toner

#1  Minnesota  89
#2  Hawaii      75
#3  Austin      60
#4  San Francisco 60
#5  Toronto     56
#6  Santa Cruz  55
#7  South Florida 55
#8  Boston      55
#9  Washington  54
#10 Pennsylvania 48
Open BGP

Search for port:179 open returned 119,548 results on 15-06-2016

Top Countries

1. Korea, Republic of 26,065
2. Italy 19,932
3. India 14,802
4. United States 14,205
5. Russian Federation 4,549
6. Germany 4,446
7. Brazil 3,890
8. Mexico 3,529
9. South Africa 2,939
10. Kazakhstan 2,833
Recursive DNS

Search for `port:53 recursion enabled` returned 3,636,849 results on 15-06-2016

Top Countries

1. China 1,141,763
2. Taiwan, Province of China
3. United States 255,129,308,662
4. Korea, Republic of 255,000
5. Russian Federation 174,062
6. India 164,970
7. Brazil 158,099
8. Turkey 98,795
9. Japan 59,360
10. Italy 46,037
<10 Abuse Emails

(for ICS/ IoT)
Questions?