Understanding Which New Threats Operators Can Expect To Face Within The Next Two To Five Years To Improve The On-Going Management Of Security Systems

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Cyber Security For Process Control: Remote Oil & Gas Assets
CSPC16
Houston, Texas
June 23, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Cyber Security Evolution

- Computer security
- Computer security + Communications security
- Information security
- Information assurance
- Mission assurance
  - Larger than cyber security
Cyber Security Evolution

- Computer security
- Computer security + Communications security
- Information security
- Information assurance
- Mission assurance
  - Larger than cyber security

Things that can go boom is a game changer
Cyber Security Foundations

- Segregate
- Authenticate
- Authorize
- Monitor
- Contain
- Adapt
● Segregate
● Authenticate
● Authorize
● Monitor
● Contain
● Adapt

- Data Access versus System Access
- Human Users versus Machine Users
## Threat Matrix Examples

<table>
<thead>
<tr>
<th>High Skill</th>
<th>Opportunistic</th>
<th>Targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero-day attack</td>
<td>Stuxnet</td>
<td></td>
</tr>
<tr>
<td>Default passwords</td>
<td>Spear phishing</td>
<td></td>
</tr>
<tr>
<td>High Skill</td>
<td>Opportunistic</td>
<td>Targeted</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>Be better than your neighbor</td>
<td>??</td>
<td></td>
</tr>
<tr>
<td>Low Skill</td>
<td>Basic hygiene</td>
<td>Security awareness</td>
</tr>
</tbody>
</table>
ALLOW GOOD GUYS IN
KEEP BAD GUYS OUT

- IP Spoofing predicted in Bell Labs report ≈ 1985
- Unencrypted Telnet with passwords in clear
- 1st Generation firewalls deployed ≈ 1992
- IP Spoofing attacks proliferate in the wild ≈ 1993
- VPNs emerge ≈ late 1990’s
- Vulnerability shifts to accessing end-point
- Network Admission Control ≈ 2000’s

- Persists as a Distributed Denial of Service (DDoS) mechanism ≈ 2010’s
Ravi’s Laws 2010

1. Attackers exist
   ● You will be attacked

2. Attackers have sharply escalating incentive
   ● Money, terrorism, warfare, espionage, sabotage, …

3. Attackers are lazy (follow path of least resistance)
   ● Attacks will escalate BUT no faster than necessary

4. Attackers are innovative (and stealthy)
   ● Eventually all feasible attacks will manifest

5. Attackers are copycats
   ● Known attacks will proliferate widely

6. Attackers have asymmetrical advantage
   ● Need one point of failure
Cyber Security Principles

A. Prepare for tomorrow’s attacks, not just yesterday’s
   ● Good defenders strive to stay ahead of the curve, bad defenders forever lag

B. Take care of tomorrow’s attacks before next year’s attacks
   ● Researchers will and should pursue defense against attacks that will manifest far in the future BUT these solutions will deploy only as attacks catch up

C. Use future-proof barriers
   ● Defenders need a roadmap and need to make adjustments

D. It’s all about trade-offs
   ● Security, Convenience, Cost