Compliance Cautions

Rock Stevens, Kevin Halliday, Michelle Mazurek
Josiah Dykstra, James Chapman, Alexander Farmer
Wendy Knox Everette
Garrett Bladow

// University of Maryland
// Independent Researchers
// Leviathan Security Group
// Dragos, Inc.
Compliance Standards

- What are they?
- Why use them?
- How are they enforced?
- What’s the problem?
First empirical evaluation of compliance standards for security issues that exist within perfect compliance.

Even if you had perfect compliance, what else could go wrong?
Standards we examined
Study Methods

1. Audit: Six researchers conducting line-by-line audit of three standards.

2. Expert evaluations: Four compliance experts evaluate researchers’ findings.

3. Disclosure: Various approaches to responsibly disclose findings to organizations.
Real-world experience
Exploitation in the wild
Unanimous agreement
<table>
<thead>
<tr>
<th>Severity</th>
<th>Unlikely</th>
<th>Seldom</th>
<th>Occasional</th>
<th>Likely</th>
<th>Frequent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td>Critical</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>E</td>
</tr>
<tr>
<td>Moderate</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>H</td>
</tr>
<tr>
<td>Negligible</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
</tr>
</tbody>
</table>

E - Extremely High  H - High  M - Moderate  L - Low
In total, 148 issues ranging from low to extremely high risk.
Six researchers conducting a line-by-line audit of three standards.
Six researchers conducting line-by-line audit of three standards.
Under-defined process

Audit

Six researchers conducting line-by-line audit of three standards
Risk Estimates for IRS Compliance Standard

- Under-defined process
- Data vulnerability
- Unenforceable
- Ambiguous specification
LASER Talking Points, Pt 1

- Cold calling the experts!
  - Friends/past contacts
  - Industry experts met a previous conferences
- Interrater reliability
- Codebook development
LASER Talking Points

● Interrater reliability
  ○ How to get results when people are in 4 different time zones, and everyone has a full-time job??
  ○ Calculated with Krippendorff's alpha
● Codebook development
# LASER Talking Points

<table>
<thead>
<tr>
<th>ID</th>
<th>Employment¹</th>
<th>Role²</th>
<th>Org Size</th>
<th>IT Exp (yrs)</th>
<th>Edu³</th>
<th>Docs⁴</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>A, G</td>
<td>M, R</td>
<td>500</td>
<td>18</td>
<td>MS</td>
<td>I,P,N</td>
</tr>
<tr>
<td>R2</td>
<td>G</td>
<td>M, R</td>
<td>10k+</td>
<td>16</td>
<td>PhD</td>
<td>I,P</td>
</tr>
<tr>
<td>R3</td>
<td>A, G*, I</td>
<td>M, R</td>
<td>100</td>
<td>20</td>
<td>BS</td>
<td>I,N</td>
</tr>
<tr>
<td>R4</td>
<td>I</td>
<td>M, R</td>
<td>35</td>
<td>15</td>
<td>JD</td>
<td>I,P</td>
</tr>
<tr>
<td>R5</td>
<td>A, G*, I</td>
<td>M, D</td>
<td>100</td>
<td>8</td>
<td>BS</td>
<td>I,N</td>
</tr>
<tr>
<td>R6</td>
<td>G</td>
<td>M, D</td>
<td>100</td>
<td>5</td>
<td>BS</td>
<td>I,N</td>
</tr>
<tr>
<td>E1</td>
<td>G, I</td>
<td>M</td>
<td>150</td>
<td>10</td>
<td>BS</td>
<td>I</td>
</tr>
<tr>
<td>E2</td>
<td>G</td>
<td>M</td>
<td>150</td>
<td>15</td>
<td>MS</td>
<td>I</td>
</tr>
<tr>
<td>E3</td>
<td>G*, I</td>
<td>M, D</td>
<td>1k</td>
<td>18</td>
<td>MS</td>
<td>P</td>
</tr>
<tr>
<td>E4</td>
<td>A, G*, I</td>
<td>R</td>
<td>5k</td>
<td>20</td>
<td>MS</td>
<td>N</td>
</tr>
</tbody>
</table>

¹ A: Academia, G: Government, I: Industry, *: Previous experience  
² M: Management, R: Research, D: Development  
³ BS: Bachelor’s, MS: Master’s, PhD: Doctorate, JD: Juris Doctorate  
⁴ I: IRS P1075, P: PCI DSS, N: NERC CIP
LASER Talking Points

- Codebook development
  - Determine root cause
  - Do it iteratively until you have agreement
  - Define terms upfront!!!
CISOs and authors Challenge assumptions Validate findings Provide context
Confirmed real-world misuse of compliance standards

“White box” pentest
Various approaches to responsibly disclose findings to organizations

Enforcers
Creators
Aggregators
Various approaches to responsibly disclose findings to organizations:

3 Disclosure

- CVEs
- NDAs
- RFCs
- RFCs closed
- Direct reporting
- "Not my Job"
- Cease communications!
What did you try that did not succeed before getting to the results you presented?

8 months to finish first part,
  8 months of NDA negotiations, and
  Several follow-on interviews to clarify survey data
Wrap-up

• Wrap up discussion
• Next steps?
• Plans for post-workshop paper?

Questions / Feedback? rstevens@cs.umd.edu | @ada95ftw