Why is this important?
Attacks

I. Assets vs. Perimeters
II. Black Box vs. White Box
III. Security vs. Functionality
IV. Build In vs. Bolt On
V. Ongoing vs. Periodic

About ISE

ISE Confidential - not for distribution
About ISE

Perspective

• White box

Analysts

• Hackers; Cryptographers; RE

Exploits

• iPhone; Android; Ford; Exxon; Diebold

Research

• Routers; NAS; Healthcare

Customers

• Companies w/ valuable assets to protect
I. Secure Assets, Not Just Perimeters
I. Secure Assets, Not Just Perimeters

Traditional Attacks

Traditional Defenses
I. Secure Assets, Not Just Perimeters
I. Secure Assets, Not Just Perimeters
II. Black Box Penetration Tests == Good
II. Black Box Penetration Tests == Good

White box vulnerability assessment == GOOD!
II. Black Box vs. White Box

• **Access Level**
  - Black Box
  - White Box

• **Evaluation Types**
  - Penetration Test
  - Vulnerability Assessment
II. Black Box vs. White Box
II. Black Box vs. White Box
II. Black Box vs. White Box
## II. Black Box vs. White Box

<table>
<thead>
<tr>
<th></th>
<th>Black Box</th>
<th>White Box</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time/cost</strong></td>
<td>2 mo. / 200 hrs.</td>
<td>2 mo. / 200 hrs.</td>
</tr>
<tr>
<td><strong>Severe issues</strong></td>
<td>4 potential issues</td>
<td>11 confirmed</td>
</tr>
<tr>
<td></td>
<td>1 confirmed</td>
<td></td>
</tr>
<tr>
<td><strong>Other issues</strong></td>
<td>none</td>
<td>10 confirmed</td>
</tr>
<tr>
<td><strong>Results</strong></td>
<td>no recommendations</td>
<td>21+ mitigation strategies</td>
</tr>
<tr>
<td><strong>Completeness/Confidence</strong></td>
<td>very low</td>
<td>high</td>
</tr>
<tr>
<td><strong>Cost/issue</strong></td>
<td>200+ hrs.</td>
<td>~9 hrs.</td>
</tr>
<tr>
<td><strong>Cost/solution</strong></td>
<td>∞</td>
<td>~9 hrs.</td>
</tr>
</tbody>
</table>
## SOHO Routers: Outcomes

<table>
<thead>
<tr>
<th>Models</th>
<th>Goals</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Any</td>
<td></td>
<td>Remote, Local, Both</td>
</tr>
<tr>
<td>&gt;30%</td>
<td></td>
<td>100% Broken</td>
</tr>
</tbody>
</table>

**Compromise**
<table>
<thead>
<tr>
<th>ROUTER</th>
<th>TRIVIAL</th>
<th>UNAUTHENTICATED</th>
<th>AUTHENTICATED</th>
<th>TRIVIAL</th>
<th>UNAUTHENTICATED</th>
<th>AUTHENTICATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linksys WRT310Nv2</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Belkin F5D8236-4 v2</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Belkin N300</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Belkin N900</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Netgear WNDR4700</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TP-Link WR1043N</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Verizon Actiontec</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>D-Link DIR-865L</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ASUS RT-N56U</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>ASUS RT-AC66U</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Linksys EA6500</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Netgear WNR3500</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>TRENDnet TEW-812DRU</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Hackers take control of 300,000 home routers
III. Security vs. Functionality
III. Security vs. Functionality

EMBARRASSINGLY OVERSIMPLIFIED CORPORATE STRUCTURE

SALES
IT
HR
...

IT FUNCTIONALITY
IT SECURITY
III. Security vs. Functionality
III. Security vs. Functionality

CONFLICT IS GOOD!
III. Security vs. Functionality
I. Security Separated From Functionality

**FUNCTIONALITY PRIORITIES**
- User Experience
- Performance
- Delivery Deadlines

**SECURITY PRIORITIES**
- Asset & credential protection
- Valid access control schema
- Defense in Depth
I. Security Separated From Functionality

FUNCTIONALITY PRIORITIES
- User Experience
- Performance
- Delivery Deadlines

SECURITY PRIORITIES
- Asset & credential protection
- Valid access control schema
- Defense in Depth

Conflict undermines objective, when *within* same team!
I. Security Separated From Functionality

**FUNCTIONALITY PRIORITIES**
- User Experience
- Performance
- Delivery Deadlines

**SECURITY PRIORITIES**
- Asset & credential protection
- Valid access control schema
- Defense in Depth

Conflict undermines objective, when *within* same team!

Conflict is beneficial when *between* teams!
<table>
<thead>
<tr>
<th>Friends Who Added You</th>
</tr>
</thead>
<tbody>
<tr>
<td>John C</td>
</tr>
<tr>
<td>Mike S</td>
</tr>
<tr>
<td>Cameron C</td>
</tr>
<tr>
<td>Smitty R</td>
</tr>
<tr>
<td>Surrey J</td>
</tr>
</tbody>
</table>
IV. “Build It In,” Not “Bolt It On”
IV. “Build It In,” Not “Bolt It On”

![Resource Investment Chart]

- Requirements
- Design
- Implementation
- Testing
- Deployment
- Maintenance
## IV. “Build It In,” Not “Bolt It On”

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
<th>Design &amp; User Needs</th>
<th>Develop Threat Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>DESIGN</td>
<td>Define Architecture</td>
<td>Design Defense in Depth</td>
</tr>
<tr>
<td>IMPLEMENTATION</td>
<td>Coding</td>
<td>Audit Code</td>
</tr>
<tr>
<td>TESTING</td>
<td>System Testing</td>
<td>White Box Vulnerability Assessment</td>
</tr>
<tr>
<td>DEPLOYMENT</td>
<td>Customer Roll-out</td>
<td>Configuration Guidance</td>
</tr>
<tr>
<td>MAINTENANCE</td>
<td>Resolve Bugs</td>
<td>Iteration Hardening</td>
</tr>
</tbody>
</table>
IV. “Build It In,” Not “Bolt It On”

<table>
<thead>
<tr>
<th></th>
<th>Built In</th>
<th>Bolted On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment cost</td>
<td>90%</td>
<td>100%</td>
</tr>
<tr>
<td>Assessment overhead</td>
<td>- - -</td>
<td>- - -</td>
</tr>
<tr>
<td>Mitigation cost / issue</td>
<td>1x</td>
<td>25x : application</td>
</tr>
<tr>
<td></td>
<td></td>
<td>300x : infrastructure</td>
</tr>
</tbody>
</table>
V. Security as Ongoing Process
V. Security as Ongoing Process

![Diagram showing feature development and iteration with increasing complexity over iterations.]
V. Security as Ongoing Process

Security: Long Periodicity

- Complexity
- Iteration

Red: Feature
Blue: Security
V. Security as Ongoing Process

![Security: Ongoing Graph](image)

- **Complexity**: Reflects the increasing complexity of security measures over iterations.
- **Iteration**:
  - **Feature**: Red line indicates feature development.
  - **Security**: Blue line indicates security enhancements.

ISE Proprietary
V. Security as Ongoing Process

<table>
<thead>
<tr>
<th>Description</th>
<th>Yearly</th>
<th>Bi-yearly</th>
<th>Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial assessment cost</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Full scope reassessment cost</td>
<td>90-95%</td>
<td>35-45%</td>
<td>20-30%</td>
</tr>
<tr>
<td>Full assessments / year</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Cost / year</td>
<td>X (0.9)</td>
<td>X (0.7)</td>
<td>X (0.8)</td>
</tr>
</tbody>
</table>
Actionable Guidance

Do:
• Protect assets
• Get $3^{rd}$ party security assessments
• Have a security person/team
• Build security in
• Perform security ongoing

Don’t:
• Focus just on perimeter
• Rely on black box
• Have security & IT as same
• Bolt security on
• Assess longer than biannually
Get Involved

SOHOpelessly BROKEN
Ted Harrington

Executive Partner

ted.harrington@security evaluators.com