Unidirectional Security Gateways
Stronger Than Firewalls

Andrew Ginter
VP Industrial Security
Waterfall Security Solutions
### 13 Ways Through a Firewall

1. Phishing / drive-by-download - victim pulls attack
2. Social engineering / steal a password / keylogger
3. Compromise domain controller - create fwall acct
4. Attack exposed servers - SQL injection / DOS / etc
5. Attack exposed clients - compromise web servers
6. Session hijacking - MIM / steal HTTP cookies
7. Piggy-back on VPN - split tunnelling / malware
8. Firewall vulnerabilities - zero-days / design vulns
9. Errors and omissions - bad rules / IT errors
10. Forge an IP address - rules are IP-based
11. Bypass network perimeter - e.g.: rogue wireless
12. Physical access to firewall - reset to fact defaults
13. Sneakernet - removable media / laptops

---

*Every data path through a firewall is also an attack channel...*
Targeted Attacks - How They Do It

- Fake email tricks users into providing passwords or installing malware
  - Or just attack exposed servers with buffer overflow, SQL injection
- Low-volume, custom malware defeats anti-virus
- Remote control: steal credentials, propagate
- Steal administrator credentials, create own passwords
- Patching: no need for vulnerabilities if you have passwords
- Create accounts, don’t guess long passwords
- Firewalls allow connections with passwords

Well-known techniques are sufficient to defeat IT-style security technologies
Unidirectional Security Gateways

- Laser in TX, photocell in RX, fibre-optic cable – you can send data out, but nothing can get back in to protected network
- TX uses 2-way protocols to gather data from protected network
- RX uses 2-way protocols to publish data to external network
- Absolute protection against online attacks from external networks
Secure Historian Replication

- Hardware-enforced unidirectional historian replication
- Replica historian contains all data and functionality of original
- Corporate workstations communicate only with replica historian
- Industrial network and critical assets are physically inaccessible from corporate network & 100% secure from any online attack
### Unidirectional Security Gateway Connectors

#### Leading Industrial Applications/ Historians
- OSIsoft PI, PI AF, GE iHistorian, GE iFIX
- Scientech R*Time, Instep eDNA, GE OSM
- Siemens: WinCC, SI NAUT/Spectrum
- Emerson Ovation, Wonderware Historian
- SQLServer, Oracle, Postgres, MySQL, SAP
- AspenTech, Matrikon Alert Manager

#### Leading Industrial Protocols
- OPC: DA, HDA, A&E, UA
- DNP3, ICCP, Modbus

#### Remote Access
- Remote Screen View™
- Secure Manual Uplink

#### Other connectors
- UDP, TCP/IP
- NTP, Multicast Ethernet
- Video/Audio stream transfer
- Mail server/mail box replication
- IBM MQ series, Microsoft MSMQ
- Antivirus updater, patch (WSUS) updater
- Remote print server

#### Leading IT Monitoring Applications
- Log Transfer, SNMP, SYSLOG
- CA Unicenter, CA SIM, HP OpenView, IBM Tivoli
- HP ArcSight SI EM, McAfee ESM SI EM

#### File/Folder Mirroring
- Folder, tree mirroring, remote folders (CIFS)
- FTP/FTFP/SFTP/TFPS/RCP
Remote Screen View

- Screen shots replicated to external web server in real time
- Remote support is under control of on-site personnel
- Any changes to software or devices are carried out by on-site personnel, supervised by vendor personnel who can see site screens in real-time
- Vendors supervise site personnel
- Site people supervise the vendors

Each perspective is legitimate, both needs are met
Deployed World-Wide

- All American nuclear generators use unidirectional gateways
- Hundreds of sites world-wide, in every critical infrastructure sector
- Remote support, central engineering, occasional remote control and other apparently bi-directional needs are met routinely

Control systems can safely be connected directly to Internet through unidirectional gateways

To try this with a firewall is heresy to security practitioners
Trends in Standards and Guidance

- Increasingly, regulations, standards and best-practice guidance recognizes hardware-enforced unidirectional communications
- Most recent: ISA SP-99-3-3/IEC 62443-3-3 and NERC-CIP V5

<table>
<thead>
<tr>
<th>General ICS Security</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISA SP 99-1</td>
<td>ISA SP 99-2</td>
<td>NIST 800-82</td>
<td>ISA SP 99-1 v2</td>
<td>ISA Tech Rep</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DHS Catalog</td>
<td>DHS DII</td>
<td>DHS Catalog V7</td>
<td></td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nuclear Generation</td>
<td>NEI 04-04</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electric Power</td>
<td>NERC 1200</td>
<td>NERC CIP v1</td>
<td>CIP v2</td>
<td>CIP v4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CIP v3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Chemical</td>
<td>API Guidelines v2</td>
<td>CFATS</td>
<td>DHS CFATS Guidance</td>
<td>INGAA Guidelines</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ACC Resp Care</td>
<td>API Guidelines v3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>API 1164 v1</td>
<td>API 1164 v2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Water</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></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>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Unidirectional Gateways: Stronger Than Firewalls

- Security: absolute protection of safety and reliability of control system assets, from network attacks originating on external networks
- Compliance: best-practice guidance, standards and regulations are evolving to recognize strong security
- Costs: reduces security operating costs: improves security and saves money

andrew.ginter@waterfall-security.com
www.waterfall-security.com