Cybersecurity for Gateways

Jim Basney <jbasney@ncsa.Illinois.edu>

Trusted CI (https://trustedci.org)
Outline

• What is so special about cybersecurity for gateways?
• Managing Cybersecurity Risks
• IT Security Risks: Self-Evaluation (Exercise)
• Risks to the Science Mission (Exercise)
• Open Discussion
What are your cybersecurity challenges?
Is cybersecurity a concern for gateways?

- Security practices for web apps well-understood
- Open access
- No sensitive data
- Not a major attack target
- Hosting provider / campus takes care of it
- … any others?
Cybersecurity is part of Sustainability

- Sustainability builds on trust
- Cybersecurity failures can erode trust
  - Data loss caused by ransomware
  - Downtime caused by system compromise
  - Reputation impact of malicious content on gateway
  - Resource access (AWS, XSEDE, etc.) put at risk due to misuse
  - Password compromise puts user accounts at risk due to password re-use at other services
Example Gateway Compromises

- Wordpress hacks
- XSEDE “community user” account compromise
- AWS credentials on GitHub
- … any others?
Managing Cybersecurity Risks

• There’s no perfect security
• Some risks you mitigate, some you accept
• Mitigate risks via cybersecurity controls
  • Not all controls are technical – also include documentation, policy, procedures, training, etc.
• Who has the authority to accept risks?
  • Do team members silently accept risks?
  • Do team members know who to talk to about risks?
  • Is someone asking about risks?
Example Control: Acceptable Use Policy

• Communicate expectations to users
• Document consequences for violating policy
• Can require explicit acknowledgement on signup and policy change
• Example AUP from Trusted CI
  • https://trustedci.org/guide/
IT Risks: Self-Evaluation Worksheet

- Policy and Procedure
- Host Protection (our exercise will focus on this)
- Network Security
- Physical Security
- Monitoring and Logging

http://trustedci.org/guide/docs/commodityIT
<table>
<thead>
<tr>
<th>Section</th>
<th>Risk</th>
<th>Goal</th>
<th>Recommended Control</th>
<th>Mitigated?</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Poor credential management by users can lead to compromise by an attacker. Resources can be used for unacceptable/illegal purposes.</td>
<td>Ensure users are aware of their responsibilities when using IT resources.</td>
<td>Have a published <strong>acceptable use policy</strong> that all users are required to accept and uphold.</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Implementation of security procedures can be overlooked or conflicting implementations can be put in place.</td>
<td>Make certain IT staff are knowledgeable of and support security policy, requirements, and procedures.</td>
<td>Designate an Information Security Officer for your project, with clear responsibilities, authority, and relationships to project leadership and personnel. Develop and communicate <strong>project wide security policies</strong> and procedures to staff.</td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>Mistakes and omissions can occur when people are unsure of what is required of them, therefore creating inefficiencies that cost time and money.</td>
<td>Ensure IT staff have a clear understanding of their role, function, and responsibilities.</td>
<td>Maintain and <strong>communicate roles and responsibilities</strong> for all IT staff.</td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td>IT assets that are not documented are at greater risk of becoming targets for attackers. Neglect can result in the lack of critical OS/service patches, unused/dormant accounts targeted, and insufficient monitoring to alert IT staff of active attacks.</td>
<td>Maintain an accurate inventory of IT infrastructure.</td>
<td>Develop and maintain a complete <strong>inventory of IT assets</strong>. Tools such as nmap can be used to discover host and services on a network.</td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>Ineffective or delayed emergency response may cause incidents to continue unmitigated, increasing the impact of a compromise.</td>
<td>Respond effectively to security events.</td>
<td>Develop and communicate an <strong>incident response plan</strong> to operational staff. Test the plan on an annual basis to ensure plan completeness and to make adjustments as needed.</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>Intruders may install a variety of tools and destroy data. It can be impossible to determine whether intruder tools have been completely removed.</td>
<td>Recover quickly from damage.</td>
<td>Hosts which are known to be compromised should be rebuilt from a known good image. Keep regular <strong>backups</strong> of system configurations and user data to ensure restoration of services and data.</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Risk</td>
<td>Goal</td>
<td>Recommended Control</td>
<td>Mitigated?</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>HOST PROTECTION</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.1</td>
<td>Exploits against known vulnerabilities may provide remote and local privilege escalation allowing an attacker to gain root or privileged access to a resource.</td>
<td>Keep patches up to date.</td>
<td>Apply <strong>patches</strong> as soon as possible.</td>
<td></td>
</tr>
<tr>
<td>3.2</td>
<td>Changes and patches may expose a security vulnerability that was previously closed.</td>
<td>Ensure information systems are secure after patching.</td>
<td>Test systems with <strong>vulnerability assessment tools</strong> to verify that patches and changes work as expected and have not introduced new security issues. Common vulnerability testing tools to consider: Nessus, OpenVAS, Metasploit.</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td>Inconsistent procedures to update systems may result in vulnerable systems.</td>
<td>Proper Configuration Management.</td>
<td>Use a centralized <strong>configuration management</strong> tool to ‘push’ new configuration files to hosts on the network.</td>
<td></td>
</tr>
<tr>
<td>3.4</td>
<td>Unnecessary services introduce weaknesses. Default software installations often start up services that are not needed. These services may be used to garner information about the system, or may have a default configuration that allows unintentional access to a system.</td>
<td>Disable/remove unnecessary services.</td>
<td>Services should be <strong>audited</strong> on installed systems. If possible, start with all services disabled and add the ones that are required. Or, at a minimum, services that are not required should be disabled.</td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>System installers often install numerous setuid/setgid programs that are unnecessary, and in some case introduce vulnerabilities, which enable privilege escalation.</td>
<td>Eliminate unnecessary setuid/setgid programs.</td>
<td><strong>setuid/setgid</strong> programs which are not needed for proper functioning of the system should be removed or disabled. Those that are needed should be evaluated for vulnerability and configuration issues.</td>
<td></td>
</tr>
<tr>
<td>3.6</td>
<td>Services designed to work within a particular trust boundary sometimes have vulnerabilities, which can be exploited across those boundaries.</td>
<td>Restrict access to services.</td>
<td>Services that are only to be accessed from within a trust boundary (e.g. only hosts on the same cluster) should have access restricted to those hosts only. Even if the service does not have a known vulnerability, it should be restricted only to the hosts/networks here it is needed. Where access is allowed across <strong>trust boundaries</strong>, a strong authentication mechanism should be used to authenticate hosts or users. For example, host based SSH authentication should be restricted to nodes within a cluster.</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Risk</td>
<td>Goal</td>
<td>Recommended Control</td>
<td>Mitigated?</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>3.7</td>
<td>HOST PROTECTION</td>
<td>Networks are commonly monitored by attackers. Any network outside of local control must be assumed to be monitored. Cleartext authentication credentials can be intercepted across networks.</td>
<td>Protect authentication credential.</td>
<td>Use <strong>strong authentication</strong> mechanisms (e.g., strong password, GSI, SSH keys, OTP) for services. Where passwords are transmitted across a network, they must be encrypted.</td>
</tr>
<tr>
<td>3.8</td>
<td>Users with privileged access may be targeted in order for an attacker to elevate privileges.</td>
<td>Control access to privileged accounts and require individual accountability and higher security requirements for users who have privileged access.</td>
<td>When possible, use <strong>multifactor authentication</strong> mechanisms for privileged access. (Password + One Time Password or SSH Key + One Time Password). Privileged access should be limited to those that need it. sudo (with a password other than the user password) should be used where possible. Remote root access should not be allowed across trust boundaries, and should be further restricted wherever possible. Root access by users should be done in a manner that provides accountability to the user. Root passwords should be different across trust boundaries. Root passwords must be changed when staff with the root password leaves or changes roles.</td>
<td></td>
</tr>
<tr>
<td>3.9</td>
<td>Trust relationships that cross a trust boundary can be exploited by an attacker from one side of the trust boundary to gain unauthorized access on the other side.</td>
<td>Define trust boundaries and reduce transitive trust relationships across those boundaries.</td>
<td>Machines with which there is a <strong>trust relationship</strong> (e.g., NFS servers, DNS servers) must be considered within the same trust boundary and must be protected at least as well as the rest of the system.</td>
<td></td>
</tr>
<tr>
<td>3.10</td>
<td>Files services such as NFS traditionally have limited authentication capabilities. These systems, if accessible outside of the trust boundary, can easily be exploited to gain privileged access and/or to corrupt data.</td>
<td>Protect NFS service from access from unauthorized hosts, and prevent users from circumventing access controls.</td>
<td>NFS service should be limited to the local (preferably internal) network of the cluster. File systems should be mounted with nosuid, nodev, root=nobody options. Where possible, <strong>file systems</strong> should be mounted read-only and/or with noexec option. NFS servers must be configured to refuse mount requests from unprivileged source ports. Network filtering should be used to block NFS traffic from hosts which are not clients of the NFS server. NFS requires that uid mappings be consistent across all clients.</td>
<td></td>
</tr>
<tr>
<td>3.11</td>
<td>Attackers may tamper with local log files to hide their access and ‘erase’ unauthorized changes to a host.</td>
<td>Maintain an accurate accounting of all system logs for accounting, auditing and forensic needs.</td>
<td>Have all machines export their log data to a centralized and protected <strong>log server</strong>. Perform analysis on log data to identify any unusual activity.</td>
<td></td>
</tr>
<tr>
<td>Section</td>
<td>Risk</td>
<td>Goal</td>
<td>Recommended Control</td>
<td>Mitigated?</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>NETWORK SECURITY</td>
<td>4.1</td>
<td>Some attacks at the network level cannot be detected at the host level.</td>
<td>Provide network monitoring capability.</td>
<td>Be prepared to monitor/capture network data as necessary. Network flow information can provide useful information about attacker activities and source, and outbound intruder activity.</td>
</tr>
<tr>
<td></td>
<td>4.2</td>
<td>Address spoofing and man-in-the-middle attacks can be used to take advantage of trust relationships between machines, allowing an attacker to obtain user's credentials and/or hijack a user's session.</td>
<td>Prevent IP address spoofing both inbound and outbound.</td>
<td>Use anti-spoofing filters for both ingress and egress at trust boundaries. Use Public Key Infrastructure to attest to trust relationships between the machines and users.</td>
</tr>
<tr>
<td></td>
<td>4.3</td>
<td>Vulnerable network services are subject to remote exploitation. Sometimes these services cannot be fixed at the host level.</td>
<td>Block services that cannot be access controlled at the host level.</td>
<td>Configure network devices to block packets at the host/port level as necessary.</td>
</tr>
<tr>
<td></td>
<td>4.4</td>
<td>Compromise of network devices can be used for Denial of Service (DoS) attacks, credential harvesting, scanning activities, spam generation, and attacks of other hosts.</td>
<td>Manage and protect network devices.</td>
<td>Employ a security scanning service to identify vulnerable hosts for remediation. Only encrypted authentication methods are to be supported for remote access to network devices. If feasible, deploy an Intrusion Detection Service to alert malicious network activity.</td>
</tr>
<tr>
<td>PHYSICAL SECURITY</td>
<td>5.1</td>
<td>Physical access can be used to compromise hosts within a trust boundary.</td>
<td>Protect information systems from unauthorized physical access.</td>
<td>Physical access to systems must be restricted to only authorized individuals.</td>
</tr>
<tr>
<td>Section</td>
<td>Risk</td>
<td>Goal</td>
<td>Recommended Control</td>
<td>Mitigated?</td>
</tr>
<tr>
<td>---------</td>
<td>------</td>
<td>------</td>
<td>---------------------</td>
<td>------------</td>
</tr>
<tr>
<td>MONITORING AND LOGGING</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>Inaccurate system timestamps can make it very difficult to analyze log files from hosts/systems.</td>
<td>Consistent and accurate date and times across infrastructure.</td>
<td>Use <strong>NTP</strong> (Network Time Protocol) to synchronize the clocks of all hosts/systems.</td>
<td></td>
</tr>
<tr>
<td>6.2</td>
<td>If logs are unmonitored, administrators' first notification of an intrusion is often a service or services going down.</td>
<td>Monitor log files for indications of intrusion attacks, intruder activity, and privilege escalation.</td>
<td>Implement and configure <strong>log monitoring</strong> tools. Have tools available for analysis of logs during and after a security event.</td>
<td></td>
</tr>
<tr>
<td>6.3</td>
<td>Logging data is often erased or modified by an intruder once a host is compromised.</td>
<td>Ensure high integrity of all logging data.</td>
<td>Forward all logs to a <strong>central log host</strong>. The log host should be well protected. Logs on the log host should be rotated and archived for as long as possible.</td>
<td></td>
</tr>
<tr>
<td>6.4</td>
<td>Particular log information can be critical for determining information about an attack.</td>
<td>Implement a minimum set of <strong>event logging</strong>.</td>
<td>Record connections to services: local and remote host, local user with accurate timestamps. Log all critical services: system boot and shutdown, all root logins, su, and sudo.</td>
<td></td>
</tr>
<tr>
<td>6.5</td>
<td>Process accounting can be useful in determining attacker activity.</td>
<td>Enable <strong>process accounting</strong>.</td>
<td>Enable process accounting and archive pacct files.</td>
<td></td>
</tr>
</tbody>
</table>
Exercise: IT Security Self-Evaluation

• Fill in “Mitigated?” column with current/planned status of your gateway
  • A: Risk Accepted (or not applicable)
  • C: Controls in place to mitigate the risk
  • P: Partially mitigated – area for future work
  • N: Not mitigated – area for future work
  • ?: Not sure – let’s discuss

• Start with the Host Protection section
  • We will compare results from this section
  • Look at other sections as time permits today or later
Exercise: IT Security Self-Evaluation

- For the 11 items in the Host Protection section:
  - Who had “A” and/or “C” for 5 or more? For all 11?
  - Who had more “A”s than “C”s? More “C”s than “A”s?

- Any comments/questions about the worksheet?
Risks to the Science Mission

• Open Science Cyber Risk Profile
  • https://trustedci.github.io/OSCRP

• Provides an enumeration of common scientific assets and the IT risks associated with each
  • Scientific assets are resources critical to science mission
  • Focus on consequences to science mission rather than specific actors/tactics/vulnerabilities
  • List of common science assets. Each linked to a diagram showing science concerns, consequences, and avenues of attack.
Science Asset: Generated or Collected Public Data

Consequences

- Reproducible: lost effort reproducing data
- Not reproducible: lost science time and opportunities
- Incorrect science results

Concerns

- Inaccessible or lost data
- Corrupted data
- Issues with sensor equipment (see Instruments Assets)
- Issues with communication or storage (see Facilities Assets, or Systems and Hardware Assets)
- Issues with data processing (see Software Assets)

Avenues of Attack
Science Asset: User Portal

Consequences
- Conditional on data type (see Data Assets)

Concerns
- Portal unavailable
- Portal not performing as expected

Avenues of Attack
- Service Provider's equipment or project's system damaged
- Mis-configuration
- DoS affecting Service Provider or project's system
- If project's system, portal interface issues (see Software Assets)
- Service Provider malicious insider or unauthorized user on project's system
Science Asset: Accounting Data

Consequences

- Lost science time due to administration issues or forensic setbacks
- Reduced reputation

Concerns

- Inaccessible or lost data
- Corrupted data
- Exposed data

Avenues of Attack

- Issues with communication or storage (see Facilities Assets, or Systems and Hardware Assets)
- Issues with front-ends, back-ends, user portals or software (see Systems and Hardware Assets or Software Assets)
Science Asset: Project Budget

Consequences
- Reduced reputation
- Competitor publishes first
- Legal action

Concerns
- Lost science time and opportunities
- Issues with personnel or collaboration (see Intangible and Human Assets)
- DoS affecting billable usage
- Issues with contracts (e.g., licenses, consulting)
- Issues with Facilities, or Staff Computing & Networking (see Facilities Assets)

Avenues of Attack
Exercise: OSCRP Diagrams

• Choose an asset and draw an OSCRP diagram

• Example assets:
  • **Data**: public, embargoed, internal, documentation, accounting
  • **Facilities**: power & climate control, physical access control
  • **System**: networks, file storage, web site, database, user portal, servers, desktops, laptops, mobile devices
  • **Software**: external, internal
  • **Intangible/Human**: reputation, staff, financial
Cybersecurity Resources

• Trusted CI – https://trustedci.org/
  • Open Science Cyber Risk Profile - https://trustedci.github.io/OSCRP/
  • Guide to Developing Cybersecurity Programs - https://trustedci.org/guide/

• Open Web Application Security Project - https://www.owasp.org/

• CIS Top 20 - https://www.cisecurity.org/controls/
Open Discussion

Cybersecurity for Gateways