A virtual laboratory for decision support in viral disease treatment

Threat Model for MOCCA Component Environment

http://virolab.cyfronet.pl

Objective

This model has been created to assess potential vulnerabilities in MOCCA and to find a secure solution for integration of MOCCA and Shibboleth.

MOCCA Security Requirements

1. **Authentication** – identity verification, Single Sign On to access kernels distributed on various nodes in different locations.
2. **Authorization** – need to map user attributes to H2O role-based users to check permissions for e.g. deploy or run software.
3. **Credential delegation** – to enable component running in one container to deploy or run code in another container.
4. **Integrity** – it is crucial to protect both user data (input and output) as well as code from tampering or destruction.
5. **Confidentiality** – to protect data and code, that might contain classified information.
6. **Availability** – of the security infrastructure and protection H2O kernels from attack, spare nodes in case of DDoS attack

Sample Use Case

**Entry points**
- plaintext transport via sockets
- secure transport using SSL

Trust levels
- Administrator
- Deployer
- User
- Guest

Future Work

- To provide easy credential delegation from Shibboleth to GSI-based systems
- To combine our client library for Shibboleth SSO with GridShib library that allows propagating Shibboleth assertions as part of non-critical extensions to X.509 GSI certificate.

Threats to the System

**STRIDE Classification Categories**

- **S**ecuring: pretending you are someone you aren’t
- **T**ampering: causing corruption of data
- **R**epudiation: claiming that you did not agree on something, but in fact you have
- **I**nformation disclosure: leaky of user’s status or code
- **D**enial of service: system becomes unstable
- **E**vasion of policy: avoid being detected

**Threats to the system**

<table>
<thead>
<tr>
<th>Name</th>
<th>EP</th>
<th>Cat.</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brute force</td>
<td>1</td>
<td>IL</td>
<td>Brute force attack is not encrypted data is not encrypted</td>
<td></td>
</tr>
<tr>
<td>Man-in-the-middle</td>
<td>2</td>
<td>STP</td>
<td>Man-in-the-middle attack is not encrypted data is not encrypted</td>
<td></td>
</tr>
<tr>
<td>Privilege escalation</td>
<td>3</td>
<td>TTP</td>
<td>Privilege escalation is not encrypted data is not encrypted</td>
<td></td>
</tr>
<tr>
<td>Root code virus</td>
<td>4</td>
<td>D</td>
<td>Root code virus is not encrypted data is not encrypted</td>
<td></td>
</tr>
<tr>
<td>Distributed Worm</td>
<td>5</td>
<td>D</td>
<td>Distributed Worm is not encrypted data is not encrypted</td>
<td></td>
</tr>
</tbody>
</table>

**References**