The STRIDE Threat Model

11/12/2009 • 2 minutes to read

When you are considering threats, it is useful to ask questions such as these:

- How can an attacker change the authentication data?
- What is the impact if an attacker can read the user profile data?
- What happens if access is denied to the user profile database?

You can group threats into categories to help you formulate these kinds of pointed questions. One model you may find useful is STRIDE, derived from an acronym for the following six threat categories:

- **Spoofing identity**. An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.
- **Tampering with data**. Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- **Repudiation**. Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. **Nonrepudiation** refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
- **Information disclosure**. Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.
- **Denial of service**. Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.
- **Elevation of privilege**. In this type of threat, an unprivileged user gains privileged

access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

See Also

Applying STRIDE

STRIDE Threats in Commerce Server

Applying STRIDE

11/12/2009 • 2 minutes to read

The simplest way to apply the STRIDE model to your application is to consider how each of the threats in the model affects each Commerce Server component and each of its connections or relationships with other application components. Essentially, you look at each part of the application and determine whether any threats that fall into the S, T, R, I, D, or E categories above exist for that component or process. Most parts will have numerous threats, and it is important that you record all of them.

Following are some sample threats to a Web site. Note that this is a highly abridged list. In a two-hour threat-analysis meeting you will likely be able to identify 20 to 40 security threats.

- **Threat #1** A malicious user views or tampers with personal profile data en route from the Web server to the client or from the client to the Web server. (Tampering with data/Information disclosure)
- **Threat #2** A malicious user views or tampers with personal profile data en route from the Web server to the COM component or from the component to the Web server. (Tampering with data/Information disclosure)
- **Threat #3** A malicious user accesses or tampers with the profile data directly in the database. (Tampering with data/Information disclosure)
- **Threat #4** A malicious user views the Lightweight Directory Access Protocol (LDAP) authentication packets and learns how to reply to them so that he can act "on behalf of" the user. (Spoofing identity/Information disclosure/Elevation of privilege [if the authentication data used is that of an administrator])
- **Threat #5** A malicious user defaces the Web server by changing one or more Web pages. (Tampering with data)
- **Threat #6** An attacker denies access to the profile database server computer by flooding it with TCP/IP packets. (DoS)
- **Threat #7** An attacker deletes or modifies the audit logs. (Tampering with data/Repudiation)
- **Threat #8** An attacker places his own Web server on the network after killing the real Web server with a distributed DoS attack. (Spoofing identity; in addition, a particularly malicious user could instigate all threat categories by stealing

passwords or other authentication data, deleting data, and so on.)

See Also

The STRIDE Threat Model

STRIDE Threats in Commerce Server