

## Identifying Threats to Network Security

Predicting threats and analyzing the risks involved forms the foundation of network security design. Threat modeling and risk analysis not only helps determine the countermeasures that should be used, but can also help provide justification to credit union leadership for resource allocation.

When identifying possible threats to your network it is important to understand what motivates attackers. In addition, you need to know what ways an attacker can compromise a network. To do this we will use the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege) threat model.

Most successful attacks on networks succeed by exploiting common and well know vulnerabilities or weaknesses including: Weak passwords - Employees use predictable passwords, short passwords or blank passwords. Unpatched software - Service packs are not maintained and security fixes are not applied. Incorrectly configured hardware and software - Users have too many privileges or applications run as the Local System account. Social Engineering - E-mails and phone calls requesting employee to “login” to a website with company credentials. Weak security on Internet connections - Unused services and ports are not secured. Firewalls and routers are used improperly. Unencrypted data transfer - Authentication packets are sent in clear text. Important data is sent over the Internet in a clear text.

Attacks on networks often follow the same pattern. As a result, methods should be designed to detect, respond, and prevent attacks during each of the following stages:

1. **Footprint.** In this stage the attacker researches the target organization and it's employees. This stage also includes completing port scans on all computers and devices that are accessible from the Internet.
2. **Penetration.** After identifying potential vulnerabilities, the attackers will try to take advantage of the most advantageous vulnerability. For example, the attacker exploits a web server that lacks the latest security updates.

3. Elevation of privilege. Once the attacker has penetrated the network the next step is to obtain administrator or system-level rights. Often, poor security as a result of using default settings allows an attacker to obtain network access without much effort.
4. Exploit. After the attacker has obtained the necessary rights, they then carry out the exploit, or method of breaking into the network. For example, the attacker chooses to deface the organizations public web site.
5. Cover-up. The final stage of an attack is where an attacker attempts to hide there actions to escape detection or prosecution. Erasing relevant log files and resetting privileges are common examples of cover-up.

A threat model is a structured approach that helps you predict potential threats to information security. The potential threats that you discover while performing threat modeling enable you to create an accurate risk management plan. By predicting threats, you can proactively reduce your risk.

The STRIDE model is a simple way to categorize threats according to their characteristics. There are six categories of threats in the STRIDE model. Remember, a threat may belong to more than one category.

Spoofing:	Forging e-mail messages Replaying Authentication packets
Tampering:	Altering data during transmission Changing data in files
Repudiation:	Deleting a critical file and denying it Purchasing a product and later denying it

Information disclosure:	Expose information in error messages Expose code on Web sites
Denial of service:	Flood network with SYN packets Flood with forged ICMP packets
Elevation of privilege:	Exploit buffer overruns to gain system privileges Obtain administrator privileges illegitimately

Use the following steps to predict threats using a threat model. First, define the scope. Decide what hardware and software you will evaluate during the threat modeling exercise. By defining the hardware and software, you can focus exclusively on the object of the threat modeling, such as a Web server or a branch office, rather than the entire network. Next, create a team. The team should include a variety of technical skills and experience. Ideally, each team member can think about the object of the threat modeling exercise from many perspectives, including those that may be far-fetched or illegal. To preserve objectivity, choose team members that have a limited stake in the object of the threat modeling. Finally, predict threats! Meet in a room with white boards, flipcharts and relevant documentation to discuss the possible ways that the object could be attacked. Keep the sessions short and schedule several sessions so that the team has time to think about the object. Ask someone not involved in the discussion to document the findings of the team.

There are a couple things you need to keep in mind when identifying threats with a threat model. One, be sure to provide team members with relevant documentation such as network diagrams, hardware and software configuration, and data flow diagrams. Two, encourage creative thinking among team members. Some suggestions, no matter how unrealistic, may prompt others to discover additional valid threats. Three, when assembling your team, consider including a trusted third party that specializes in network penetration testing.

Predicting threats to network security does not have to be a time consuming activity. With teamwork and good documentation you will be well on your way to having a complete network threat assessment.