

# Network Threat Modeling

Jesper M. Johansson, Ph.D.  
Program Manager, Security Business Unit, Microsoft Corporation  
jesperjo@microsoft.com

## Threat Modeling

Threat modeling is an important risk assessment and mitigation practice that provides the capability to secure a network environment. Threat modeling includes understanding and communicating the threats to the network computing environment. It is critical to be aware of the types of threats and how to reduce or mitigate the risk both in systems and applications on network aware devices.

The information and protections discussed in Howard & LeBlanc's Writing Secure Code, 2<sup>nd</sup> Ed., in writing more secure software can be applied to networks as well as to software applications.

## Network Security Hardening

Default OS configuration is acceptable for a trusted network that is carefully controlled. However, for most networks the default configuration poses serious risks on several fronts. For example, Windows 2000 (W2K) is very open by default as apposed to Windows Server 2003 which is much more secure. In W2K, Internet Information Server (IIS) is turned on by default along with the installations of samples and web printing, among other services. Anonymous users can connect and enumerate all shares, users, list administrators and obtain auto admin logon credentials.

Numerous other examples of problems with default installations and settings exist as well. What is critical is that it is necessary to understand the target environment, the default settings, the protocols, etc., when performing an installation or re-configuration of systems and software. Performing a security risk analysis will help provide a clearer picture of the network, system, and software environment.

Steps that can be taken to mitigate the identified security risks are:

**Document** the environment and configurations, including performing a baseline of the systems and software. The purpose is to communicate what the environment looks like. Use well understood modeling techniques such as modified Data Flow Diagrams

(DFD's) and Threat Trees. A graphic representation showing communication between objects aids in describing the activities that process data and how data flows through a system and network. It shows the logical sequence of associations and activities. This type of model is sometimes known as a process model.

**Segregate** systems by application and security requirements. Which systems should be trusted and to what level? Verify that the security requirements between trusted systems are equivalent; or let less sensitive systems depend on more sensitive systems for their security. However, more sensitive systems **MUST NEVER** depend on less sensitive systems.

**Restrict** the environment and the privileges to those that are needed. Documenting the known threats and exposures can aid in this process. Think like a hacker as to how one would take advantage of the network, what types of information one would want, and what chain of events might generate high risk. Use of Fault Trees can help demonstrate logical paths through the network or systems and highlight faults. Fault trees can aid in determining where to correct or protect detected weaknesses or faults in the environment.

In application of restrictions follow the principle of least privilege for setting up accounts, roles, and permissions. Also, restrict communications between systems and applications within the network environment to those that are required. Disable or remove unused services and ports, and use secure communications between systems and users as needed.

## Conclusion

- Hardening networks requires understanding the environment
- Optimal hardening requires deep understanding
- There is a fundamental tradeoff between security and usability
- Three-phase approach to network hardening
  - Document
  - Segregate
  - Restrict