Simple Threat Model

Simple Threat Model

In our view too much emphasis has been placed on the enumeration and modeling of threats and frankly too little on fixing them. As such our purpose was not to add to the discourse, but rather to simplify it. In this regard, we wholeheartedly concur with the 1994 sentiments of Marcus Ranum which ring just as true today as they did then, namely that **“By understanding the fundamental paradigms of attack and defense, one can defend against broad categories of problems - whereas many "security experts" of today are really only concerned with catalogs of detailed nitpicks”.** Our simplified model outlined below creates an abridged taxonomy of sorts, whose main purpose was again not so much enumeration and organization, but rather to serve as an abstractive aid for illuminating solution analysis and direction as well as execution focus.

Threat Group	Threats
Client~Network~Server~Service	• Code Vulnerability Exploitation • Activity or Communication Logging • Sniffer/Sniffing • Internal Theft (Rogue Employees) • Denial of Service • Spam
Client	• Keystroke Logger (Software) • Keystroke Logger (Hardware) • Screen Capture • Logging: App Web Site Activity/Process etc. • Spoofing (Software, Controls, Trustmark's) • Code injection/Hooking, including Man-in-the-Browser • Memory Scan/ Dump • Virus Distribution (botnet) • Brute Force • Crypto Analysis • Ransomware • Unintended Actions (Adware, Pop-ups)
Network	• Spoofing (Phishing, Pharming, DNS Poisoning, IP Spoofing, Side Channels) • Replay • Recon (Network Enumeration, Scanning, Mapping) • Man-in-the-Middle
Server	• DDOS/Volumetric Flooding • Targeted Services (SSH, FTP, Web Service, Database)

Continued on next page

Trusted Service

- CA -Single Point Of Failure
- CA-Revocation List Inactive
- CA-Compromised Private Key
- CA-Instantiated Trust Violation

Reverse Engineering

- Unhooking
- Tester Neutralization
- Debugging
- Disassembly (Static)
- Disassembly (Dynamic) i.e. slicing
- Fuzzing/Trial and Error
- Error Manipulation
- Data Format Analysis