Spoofing - Pretending to be something or someone you're not

Tampering - Modifying something you're not supposed to modify. This can be on disk, in memory, and/or in transit ("on the wire")

Repudiation - Claiming you didn't do something, whether or not you actually did

Denial of Service (DoS) - Taking actions to prevent the system from providing service to legitimate users; this can include "crashing" the service, making it unusably slow, or consuming all of its storage (memory and/or disk)

Information Disclosure - Exposing information to people who aren't authorised to see it

Elevation of Privilege - Being able to perform operations you aren't supposed to be able to do

Element	S	T	R	I	D	E
External Entity	**X**		**X**			
Process	**X**	**X**	**X**	**X**	**X**	**X**
Data Flow		**X**		**X**	**X**	
Data Store		**X**	**?**	**X**	**X**	

NOTE: In Data Store/Repudiation, the '?' indicates this threat would be applicable if the data store contains *logs*

Spoofing Threats

Threat Examples	What the Attacker Does	Notes
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Replacing a well-known process with a malicious process with the same name
	Renaming	Naming your process something “legitimate-sounding”
Spoofing a File	Creates a file in a local directory	
	Creates a link and changes it	Change should happen between check and access
	Creates many files in the expected directory	Useful for spoofing .pid or .lock files
Spoofing a Machine	ARP Spoofing	
	IP Spoofing	
	DNS Spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar, or DNS operator
	IP Redirection	Switch/Router level
Spoofing a Person	Sets e-mail display name	
	Takes over a real account	
Spoofing a Role	Declares themselves to be that role	Opening a special account with a relevant name Asserting role through request/profile manipulation

Tampering Threats

Threat Examples	What the Attacker Does	Notes
Tampering with a File	Modifies a file they own, and on which you rely	
	Modifies a file you own	
	Modifies a file on a file server that you own	Processes can include files from remote domains
	Modifies a file on their file server	XML frequently includes remote schema refs
	Modifies links or redirects	
Tampering with Memory	Modifies your code	Hard to defend against when the attacker is already running code as the same user
	Modifies data supplied to your API	Pass by value, never by reference, when crossing a trust boundary
Tampering with a Network	Redirects data flow to their machine	Often first stage of Tampering
	Modifies data flowing over a network	Even easier when wireless networks are involved

Repudiation Threats

Threat Examples	What the Attacker Does	Notes
Repudiating an Action	Claims not to have clicked	
	Claims not to have received	How do we “prove” receipt?
	Claims to have been a fraud victim	
	Uses someone else’s account	
	Uses someone else’s payment instrument	
Attacking the Logs	Notices you have no logs	
	Puts attacks in the logs to confuse logs, log-reading code, or a person reading the logs	Corrupting the logs can invalidate them as evidence

Information Disclosure Threats

Threat Examples	What the Attacker Does	Notes
Information Disclosure against a Process	Extracts secrets from error messages	
	Extracts machine secrets from error cases	Can make ASLR less useful
	Extracts business/ personal secrets from error cases	
Information Disclosure against Data Stores	Takes advantage of inappropriate or missing ACLs	
	Takes advantage of bad database permissions	
	Finds file protected by obscurity	
	Finds crypto keys on disk, or in memory	
	Sees interesting information in file names	
	Reads files as they traverse the network	
	Gets data from logs or temp files	
	Gets data from swap or other temp storage	
	Extracts data by obtaining device and changing OS	
Information Disclosure against a Data Flow	Reads data on the network	
	Redirects traffic to enable reading data on the network	
	Learns secrets by analysing traffic	
	Learns who's talking to whom, by watching DNS	
	Learns who's talking to whom by Social Media disclosure	

Denial of Service Threats

Threat Examples	What the Attacker Does	Notes
Denial of Service against a Process	Absorbs memory	
	Absorbs CPU	
	Uses process as an amplifier	
Denial of Service against a Data Store	Fills up data store	
	Makes enough requests to slow down system	
Denial of Service against a Data Flow	Consumes network resources	

Elevation of Privilege Threats

Threat Examples	What the Attacker Does	Notes
Elevation of Privilege against a Process by Corrupting the Process	Sends inputs that the process does not handle properly	Very common, and frequently high-impact
	Gains access to read or write memory inappropriately	Reading memory can enable further attacks
Elevation through Missed Authorisation Checks		
Elevation through Buggy Authorisation Checks		Centralise checks, to make errors easier to find and manage
Elevation through Data Tampering	Modifies bits on disk (or in memory) to do things other than what the authorised user intends	