

## ThreatModCon 23

### Developing a Threat Modeling Mindset (Workshop) – Oct 29, 2023

Robert Hurlbut

#### Handout

#### Data Flow Diagram (DFD) – Shapes and Examples

Notation element	Reference	Examples
	External entity	People (e.g., users), systems (e.g., other devices), cloud services, browsers
	Process	DDL, exe(D)COM, web service, virtual machine, threat
	Data store	File, database, registry, cache, cookie
	Data flow	http request or response, remote procedure call, UDP communication
	Trust boundary (inside you trust the processes and data stores, outside you don't)	Device boundary, process boundary

#### STRIDE – Definitions and Example Mitigations

Threat	Property Violated	Threat Definition	Threat Mitigations
<b>Spoofing</b>	Authentication	Pretending to be something or someone other than yourself	2FA, MFA, Another provider
<b>Tampering</b>	Integrity	Modifying something on disk, network, memory, or elsewhere	Crypto integrity, authorized users only
<b>Repudiation</b>	Non-Repudiation	Claiming you didn't do something or were not responsible; can be honest or false	Maintain logs, digital signature
<b>Information Disclosure</b>	Confidentiality	Providing information to someone not authorized to access it	Data in files, logs, etc. available to authorized users only
<b>Denial of Service</b>	Availability	Exhausting resources needed to provide service	Rate-limiting, throttling access, monitoring
<b>Elevation of Privilege</b>	Authorization	Allowing someone to do something they are not authorized to do	Central authorization, ACLs, limits on writing, roles / permissions