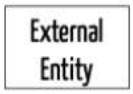
CodeMash 2025

Hands-On Threat Modeling Workshop (Pre-Compiler) - January 14, 2025

Robert Hurlbut

Handout (Page 1 of 3)

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

CodeMash 2025

Hands-On Threat Modeling Workshop (Pre-Compiler) - January 14, 2025

Handout (Page 2 of 3)

Four-Question Frame for Threat Modeling

1. **What are we working on?**
2. **What could go wrong?**
3. **What are we going to do about it?**
4. **Did we do a good enough job?**

General Questions to Help Identify Threats Using a DFD

1. **Who's interested in apps and data (threat agents)?**
2. **What goals (assets)?**
3. **What attack methods (how)?**
4. **Are there any attack surfaces (trust boundaries) exposed?**
5. **Are there any input/output (data flows) missing?**
6. **What do we worry most about the system?**

CodeMash 2025

Hands-On Threat Modeling Workshop (Pre-Compiler) - January 14, 2025

Robert Hurlbut

Handout (Page 3 of 3)

DFD Example