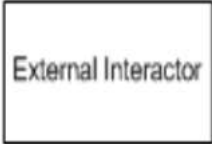






DFD and STRIDE Cheat Sheet

Type of Attack	Example Threats	What to target	Property we want	Example Controls
Spoofing	Pretending to be someone else	<ul style="list-style-type: none"> Person/role Machine File Process 	Identity Assurance	<ul style="list-style-type: none"> Authentication based on key exchange Single-factor, 2FA, multi-factor authentication Offload authentication to another provider Restrict authentication to certain IP ranges
Tampering	Modifying data that should not be modifiable	<ul style="list-style-type: none"> File / data Memory Network Process 	Integrity	<ul style="list-style-type: none"> Cryptographic integrity mechanisms Enumerated authorized users modify data
Repudiation	Claiming someone didn't do something	<ul style="list-style-type: none"> Logs Database Location of logs 	Non-Repudiation	<ul style="list-style-type: none"> Maintain logs Digital signature
Information Disclosure	Exposing information	<ul style="list-style-type: none"> Data stores Data in transit Data in memory Data within a process Data within a file/device 	Confidentiality	<ul style="list-style-type: none"> Authorized users only see files/database Authorized users only see communication
Denial of Service	Preventing a system from providing service	<ul style="list-style-type: none"> Process Data store Data flow Network 	Availability	<ul style="list-style-type: none"> Rate limiting or throttling access to service Real-time monitoring of log files / resources
Elevation of Privilege	Doing things that one isn't supposed to do	<ul style="list-style-type: none"> Compromising a process Circumventing authorization Tampering data 	Least Privilege	<ul style="list-style-type: none"> System has centralized authorization engine Strong ACLs Limits to writing data to higher integrity levels Roles / accounts or permissions

Data Flow Diagram Stencils

	External Interactor / Entity – systems, users, - “static” elements (“We don’t own or control”)
	Process (single circle) or Complex Process (double circle) – handles/processes/moves data (“We own or control”)
	Data Flow – direction data flows
	Data Store – data storage such as databases, file systems, caches
	Trust Boundary – change of trust levels