



Threat Modeling Microsoft STRIDE

Prof Federica Paci

Threat Modeling

- Techniques used
 - to model and analyze technology systems and services
 - to understand how that system or service might be attacked,
 - the measures or controls needed to manage the risk posed by such attacks
- Threat modelling techniques are best applied to inform the design and development phases of a technology system or service life cycle

Threat Modeling

- ~~What are we working on?~~
- ~~What can go wrong?~~
- ~~What are we going to do about it?~~
- ~~Did we do a good enough job?~~

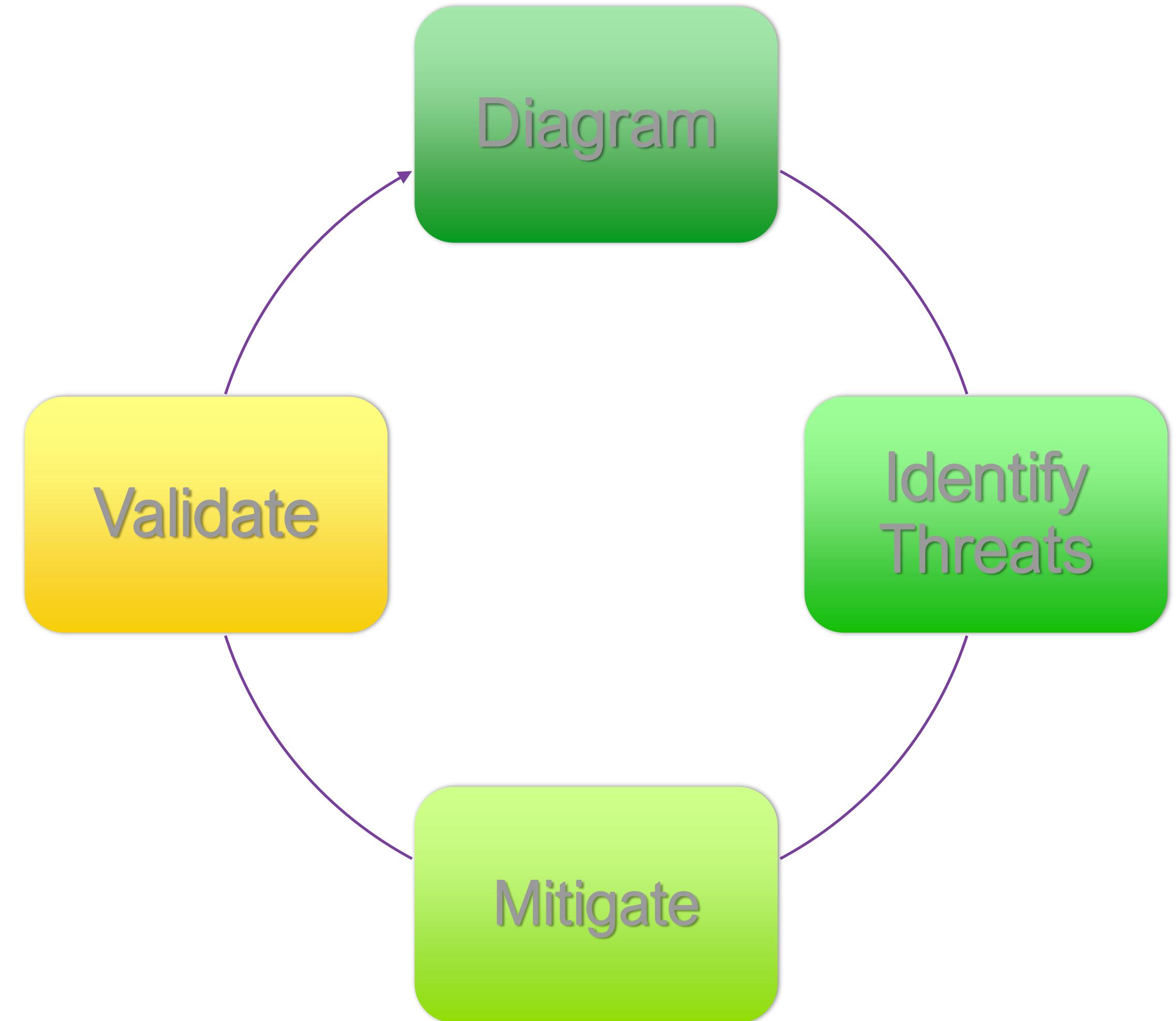
STRIDE

→ fornisce strumenti per identificare attacchi al sistema o componenti di esso
senza avere spiccate conoscenze in quel campo

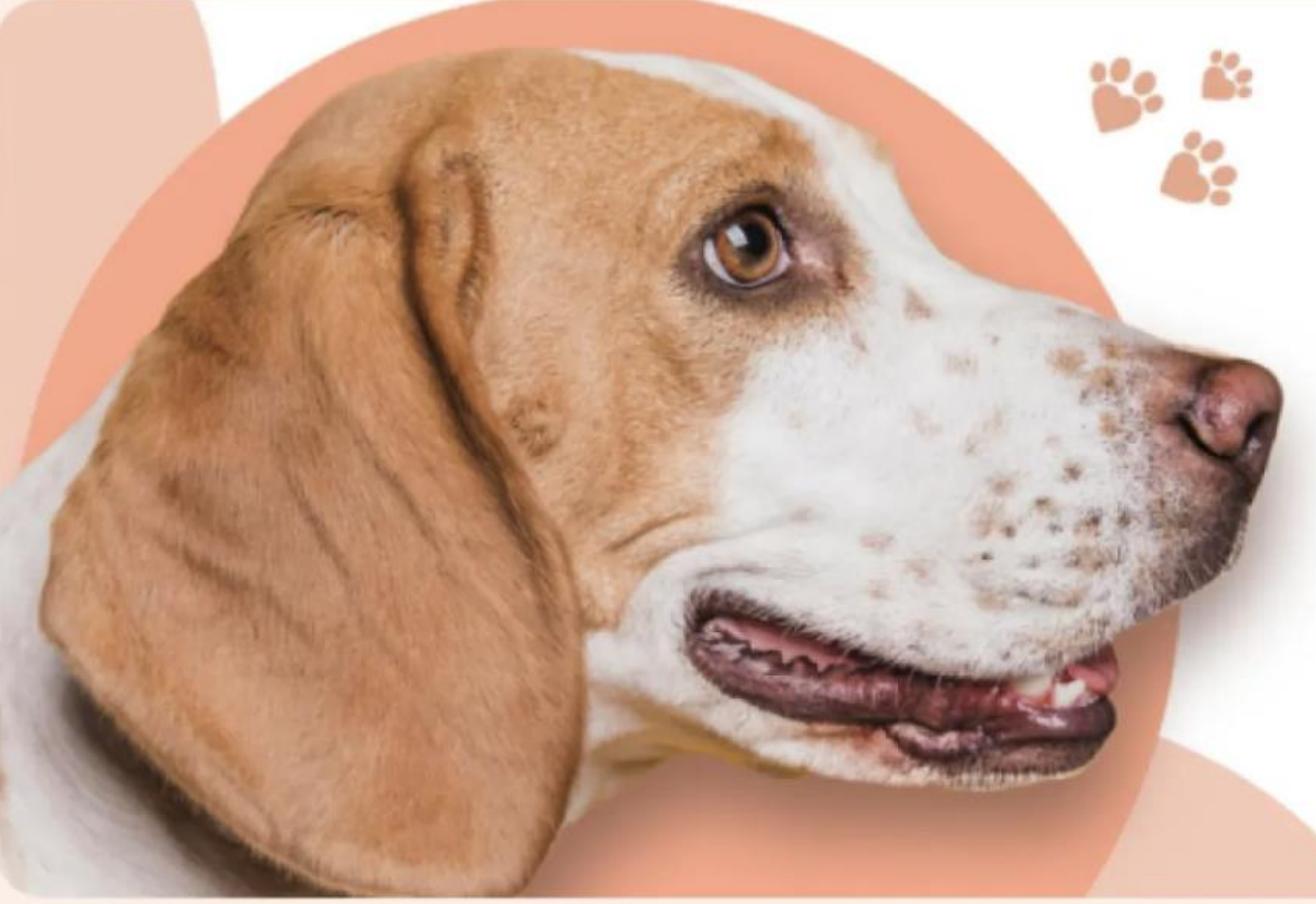
- Popular threat modeling technique by Microsoft
- Focus on what an attacker is trying to achieve
- Endorsed by Security Touchpoints, OWASP's CLASP and Microsoft's SDL
- Taught in security certification programs like CSSLP
- Widely used in industry
- Require little security expertise

Usato spesso con l'analisi del rischio e la modellazione delle minacce per identificare, comprendere e affrontare le possibili vulnerabilità di un sistema.

The Process in a Nutshell



Illustrative Example: PetShop



Pet Shop
Pet Food and Accessories

Lore ipsum dolor sit amet, consec tetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore.

[Read More](#)

 Pet Food Delivery

 Pet Clinic & Salon

 Pet School & Training

 Special Offer and Discount

 Shopping From Anywhere

 Various Payment Methods

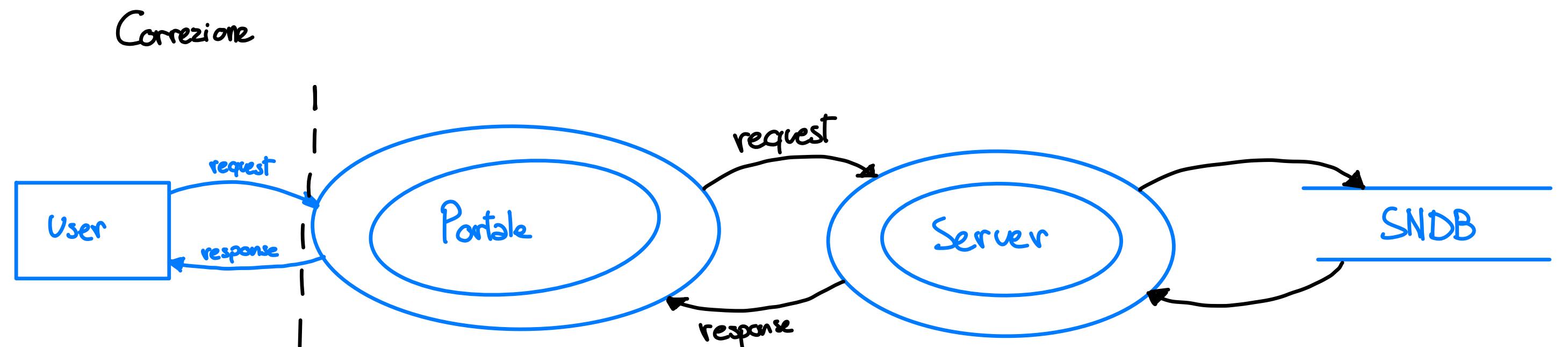
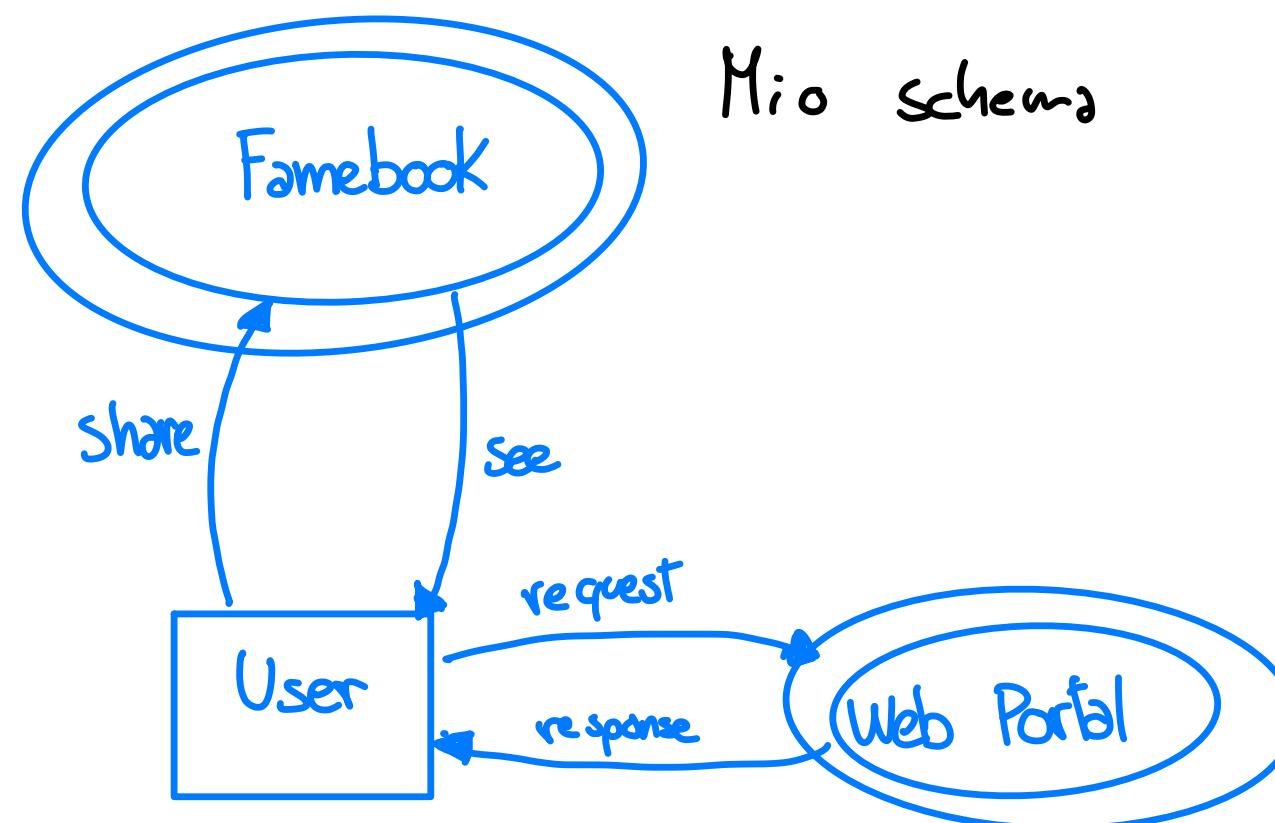
 Free Delivery All Over Bali



CAT > DOG > BIRD > RAPTILE >

Use Case: Famebook social network

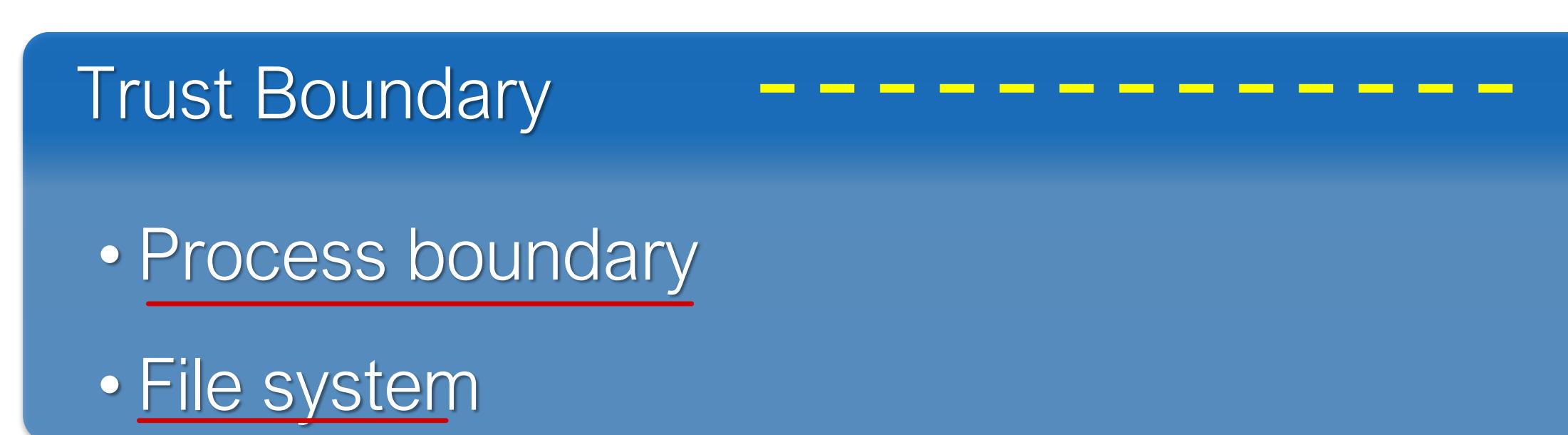
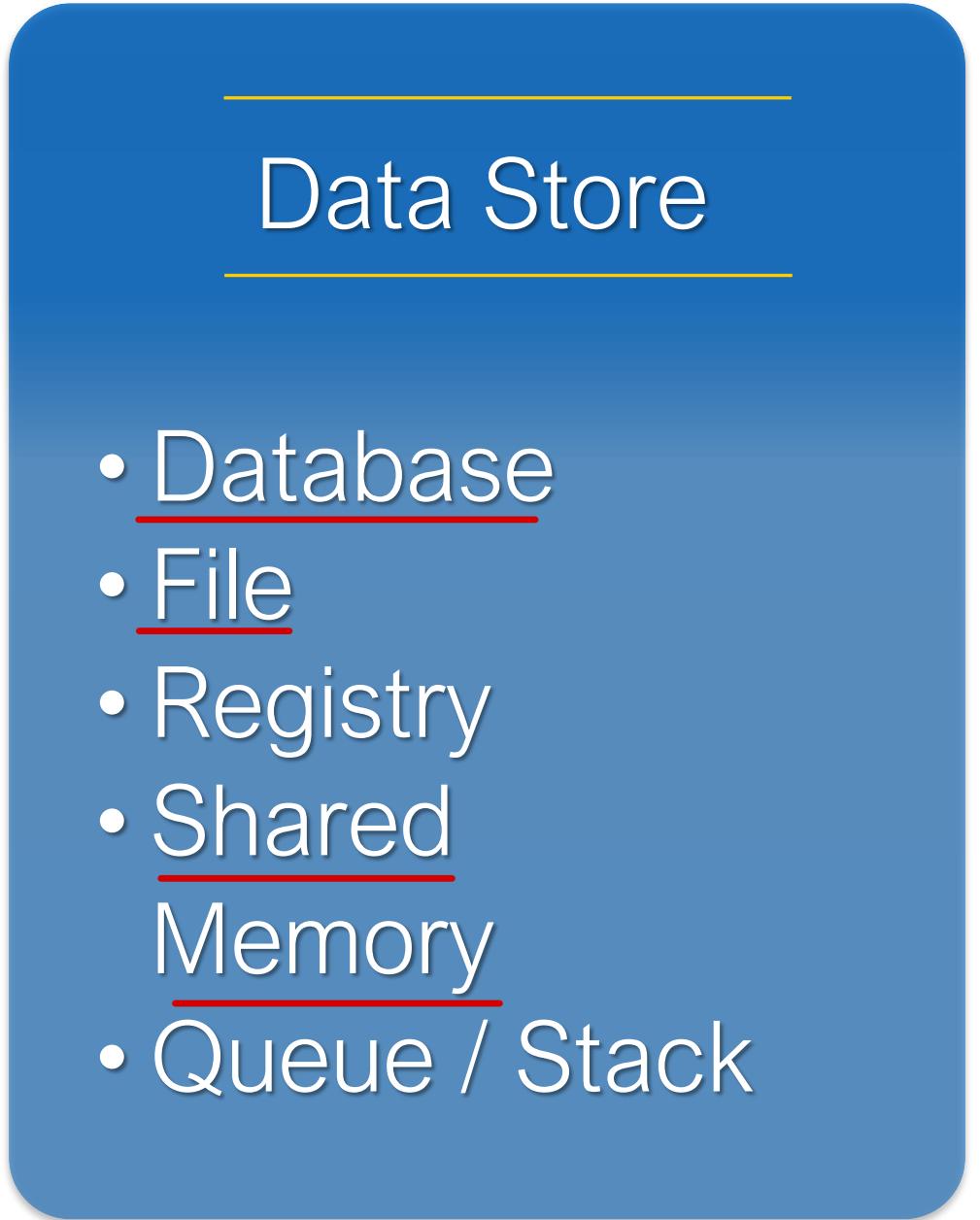
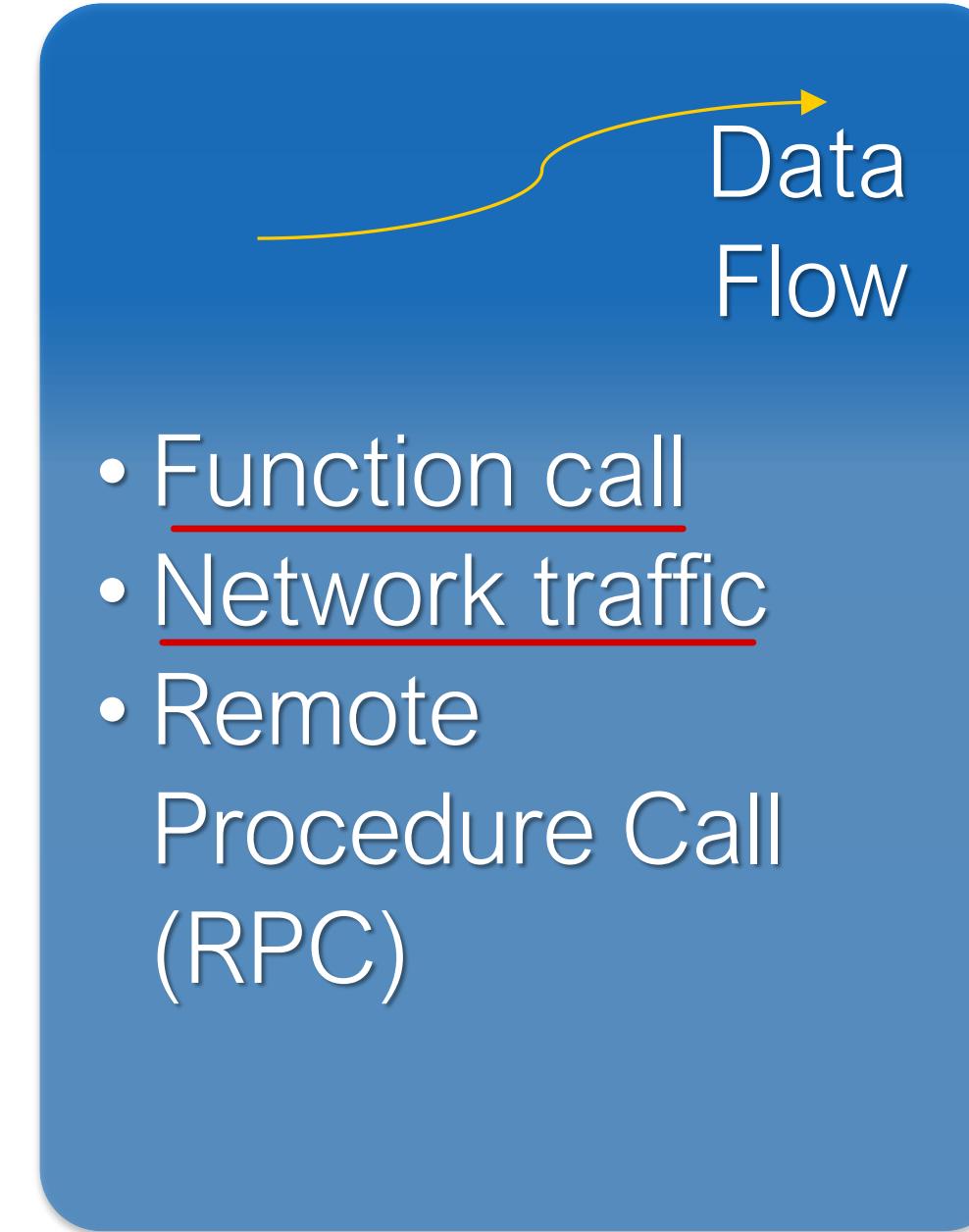
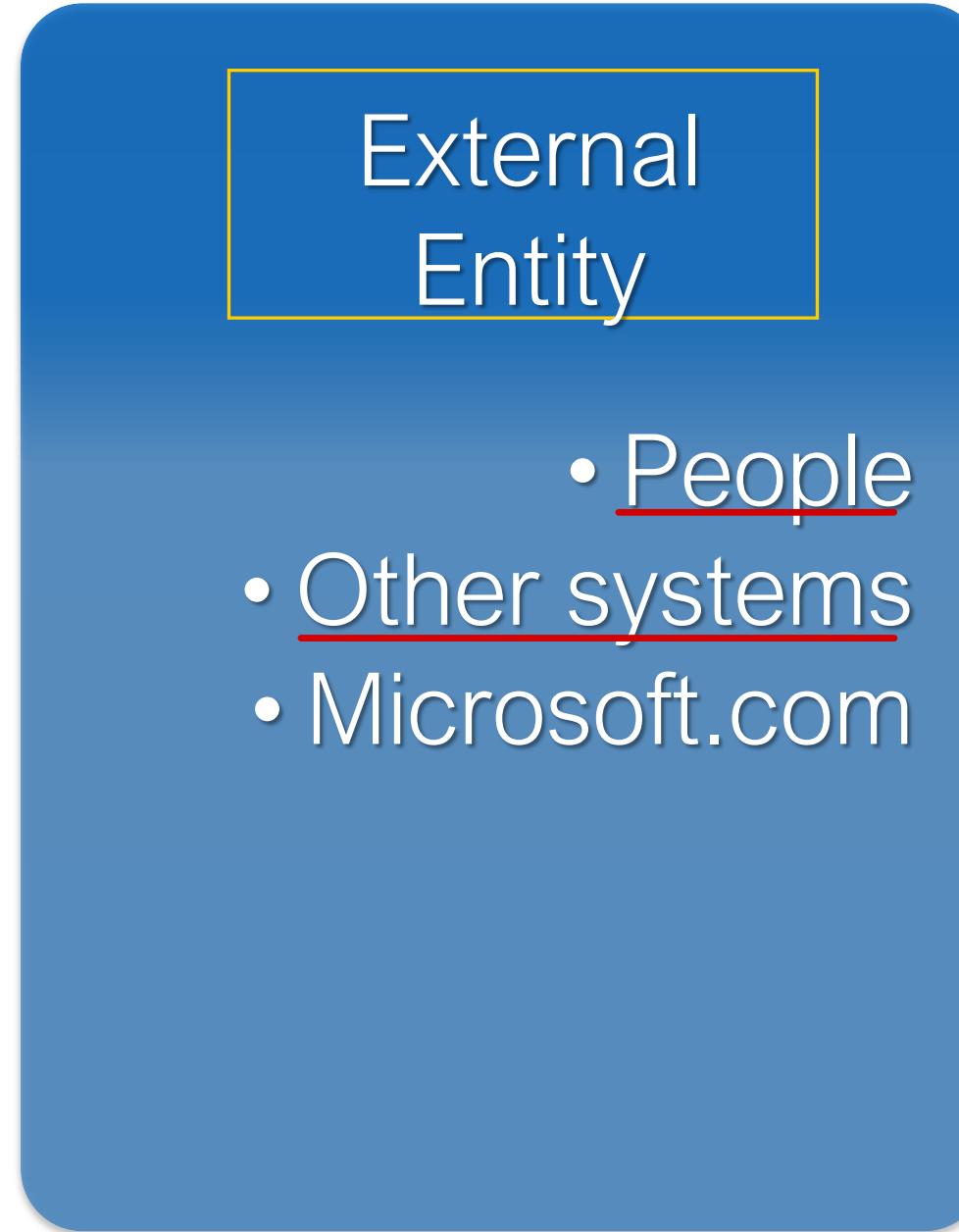
- Famebook is social network, where online users share personal information such as relationship status, pictures, and comments with their friends.
- Alice is a registered user of Famebook
- Each time Alice updates her friends list, she first connects to the social network's web portal
- The portal communicates with the social network's server, and eventually, the friendship information of Alice and all other users of that social network is stored in a database



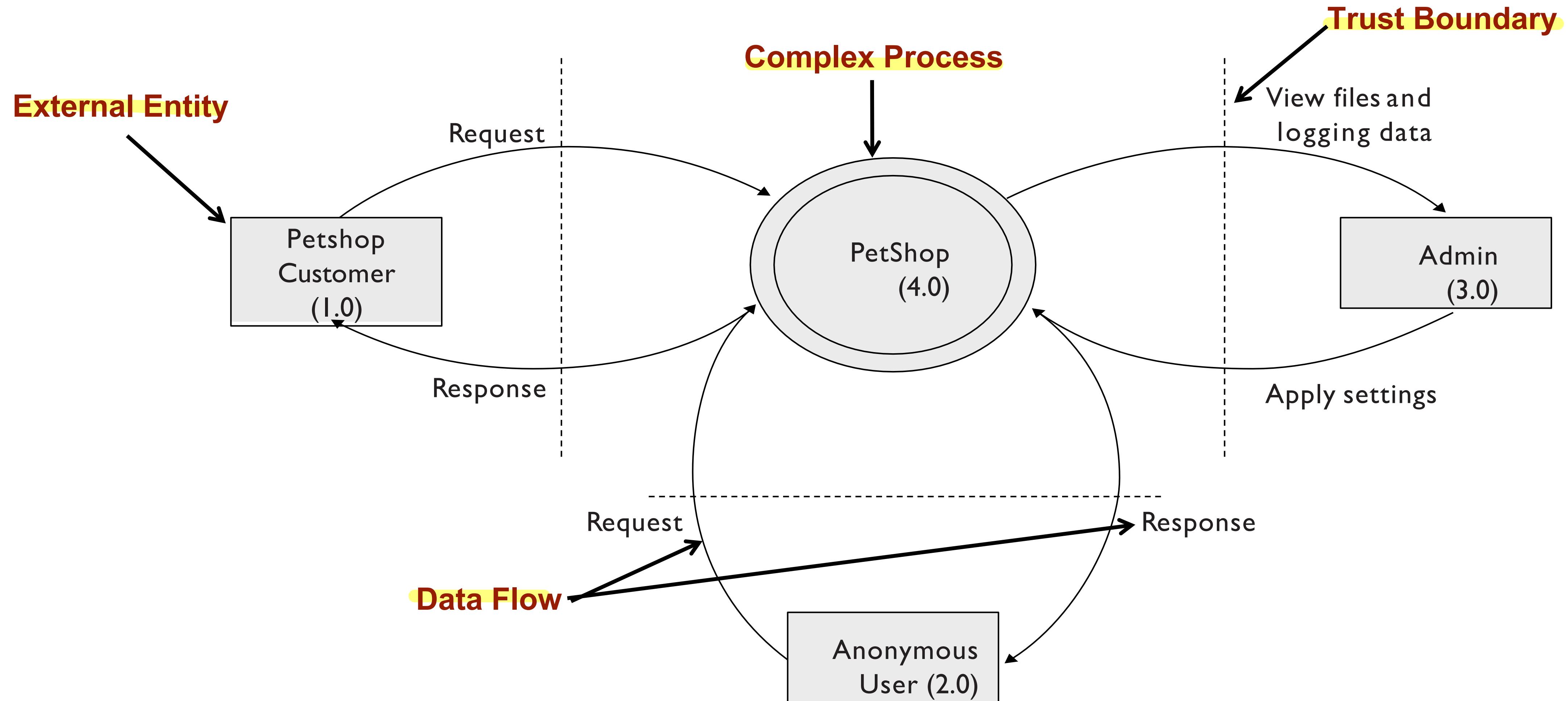
Step 1: Create Data Flow Diagrams (model the system)

- A DFD is a graphical representation of the system under review
 - Model how data enters, leaves and traverses software components
 - Shows all data sources and destinations
 - Show all relevant processes that the data goes through
- Good DFDs are critical to threat modeling!!
 - sono cruciali

Diagram Elements



Pet Shop Context Diagram

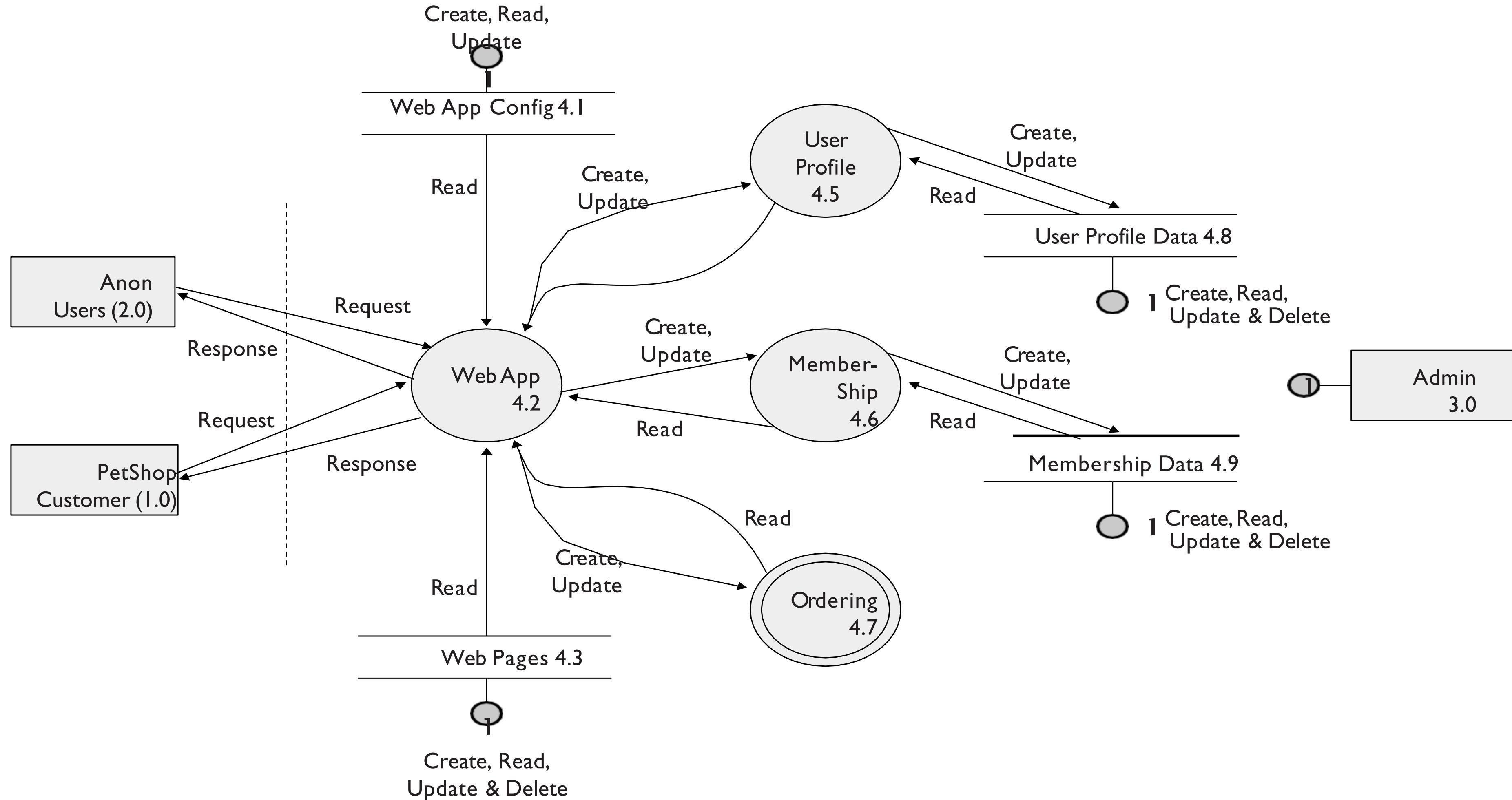


DFDs Decomposition

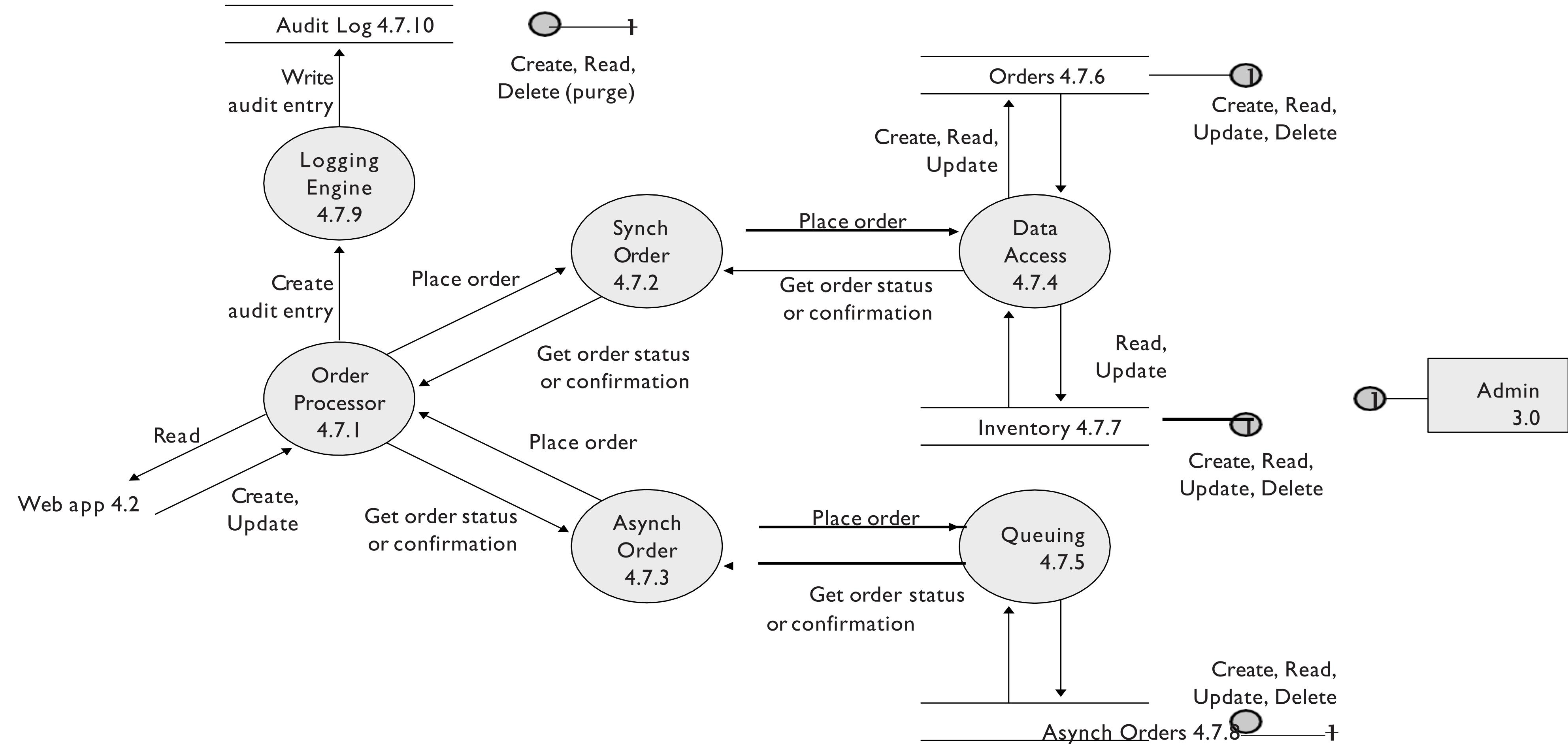
- Iterate over processes, data stores, and see where they need to be broken down
- Initially draw a **context diagram**
 - Very high-level; software and external entities interacting with it
- Then, draw a **level 1 diagram**
 - High level; major business processes
- Then processes can be further decomposed in **level 2 diagrams**
- And so on till no further decomposition is possible

Pet Shop Level 1 Diagram

major business process



Pet Shop Level 2 Diagram



Exercise 1 – Step 1- Create the data flow diagram

- Build the DFD of the Famebook social network
- Time: 10 minutes

Step 2: Identify Threats

Experts can brainstorm

How to do this without being an expert?

Use STRIDE to step through the diagram elements

Get specific about threat manifestation

Analizzo le 6 principali categorie di minacce

Threat

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privilege

Property we want

Authentication

Integrity

Nonrepudiation

Confidentiality

Availability

Authorization

Threat: Spoofing

Threat

Property

Definition

Example

Spoofing

Authentication

Impersonating something or someone else

Pretending to be any of billg, microsoft.com, or ntdll.dll

attaccante cerca di falsificare
la propria identità per apparire come
un utente legittimo

Threat: Tampering

Threat

Property

Definition

Example

Tampering

Integrity

Modifying data or code

Modifying a DLL on disk or DVD, or a packet as it traverses the LAN

Modifiche non autorizzate o alterazione dei dati
del software o dell'ambiente operativo di un
sistema

Threat: Repudiation

Threat

Property

Definition

Example

Repudiation

Non-Repudiation

Claiming to have not performed
an action

"I didn't send that email," "I didn't modify that
file," "I certainly didn't visit that Web site, dear!"

utente cerca di negare l'avvenimento di un'azione
o di un evento, spesso cercando di eludere
la registrazione o la tracciabilità.

Threat: Information Disclosure

Threat

Property

Definition

Example

Information Disclosure

Confidentiality

Exposing information to someone not authorized to see it

Allowing someone to read the Windows source code; publishing a list of customers to a Web site

d'informazioni sensibili e riservate
di informazioni sensibili e riservate

Threat: Denial of Service

Threat

Property

Definition

Example

Denial of Service

Availability

Deny or degrade service to users

Crashing Windows or a Web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole

Tentativo di rendere un sistema
un servizio o un'applicazione inaccessibile
o non operativo per gli utenti legittimi

Threat: Elevation of Privilege

Un attaccante cerca di aumentare
il proprio livello di autorizzazione o
privilegi di accesso al sistema

Threat

Elevation of Privilege (EoP)

Property

Authorization

Definition

Gain capabilities without proper authorization

Example

Allowing a remote Internet user to run commands is the classic example, but going from a “Limited User” to “Admin” is also EoP

Map STRIDE to DFD Elements

ELEMENT	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store	✓	?		✓	✓	
Data Flow	✓			✓	✓	

Map STRIDE to DFD Elements: An Example

Threat Type	DFD Elements
Spoofing	External Entities: Pet Shop Customer... Processes: Web application, Order processor
Tampering	Processes: Web application, Order processor Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,....
Repudiation	External Entities: Pet Shop Customer...
Information Disclosure	Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,...
Denial of Service	Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,....
Elevation of Privileges	Processes: Web application, Order processor

Exercise 2 – Step 2 - Identify Threats

- Work in pairs
- List the elements of the following DFD diagram
- Use the table to map elements to STRIDE threat types
 - The table is meant to support you in the identification of the threat that apply to a specific DFD element type
 - Ask yourself if a threat type is applicable to the DFD element in the system you are analysing
- Time: 10 min

Spoofing: EE User P: portable, server

Tampering: P: portable, server, SNDB DF: user to portable

Repudiation: P: portable

Information Disclosure: P: portable, server, SNDB DF: user to portable

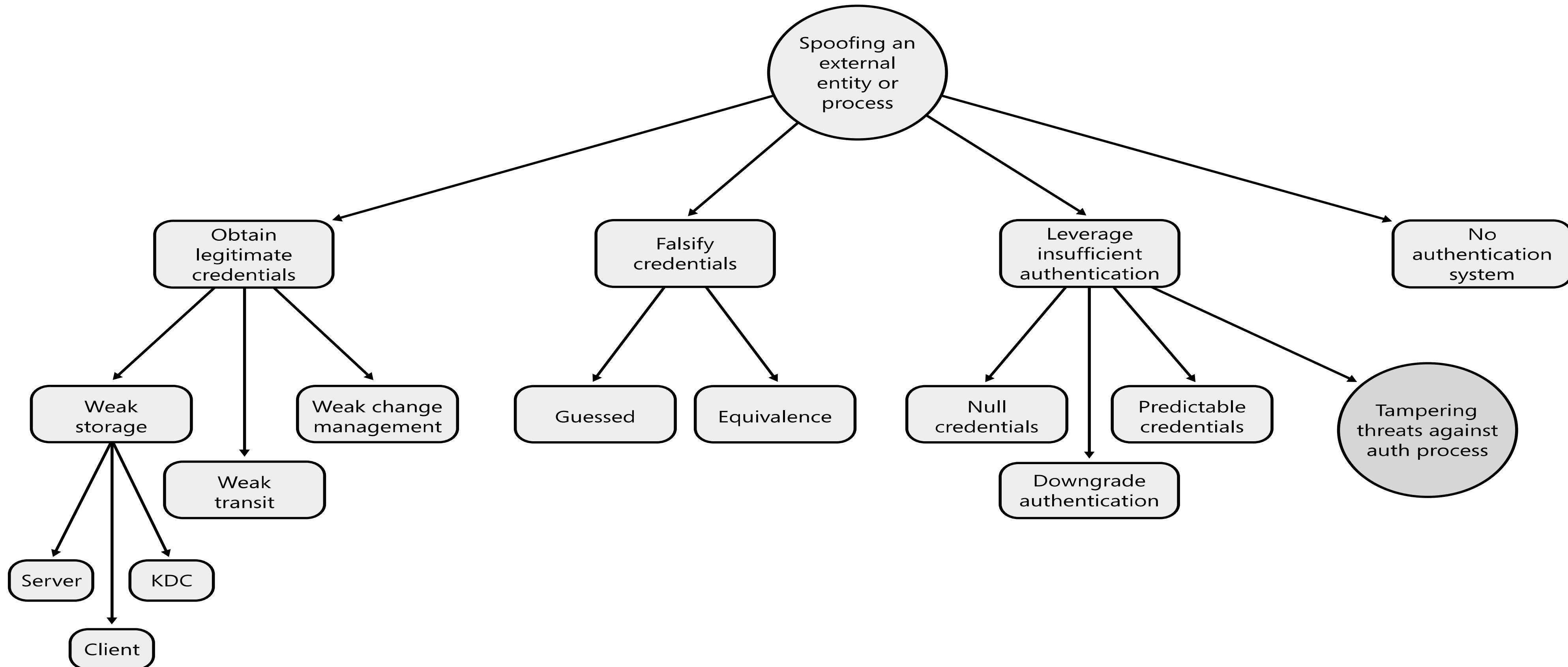
Denial of Service: P: portable, server, SNDB DF: user to portable

Elevation of privilege P: Portable, Server

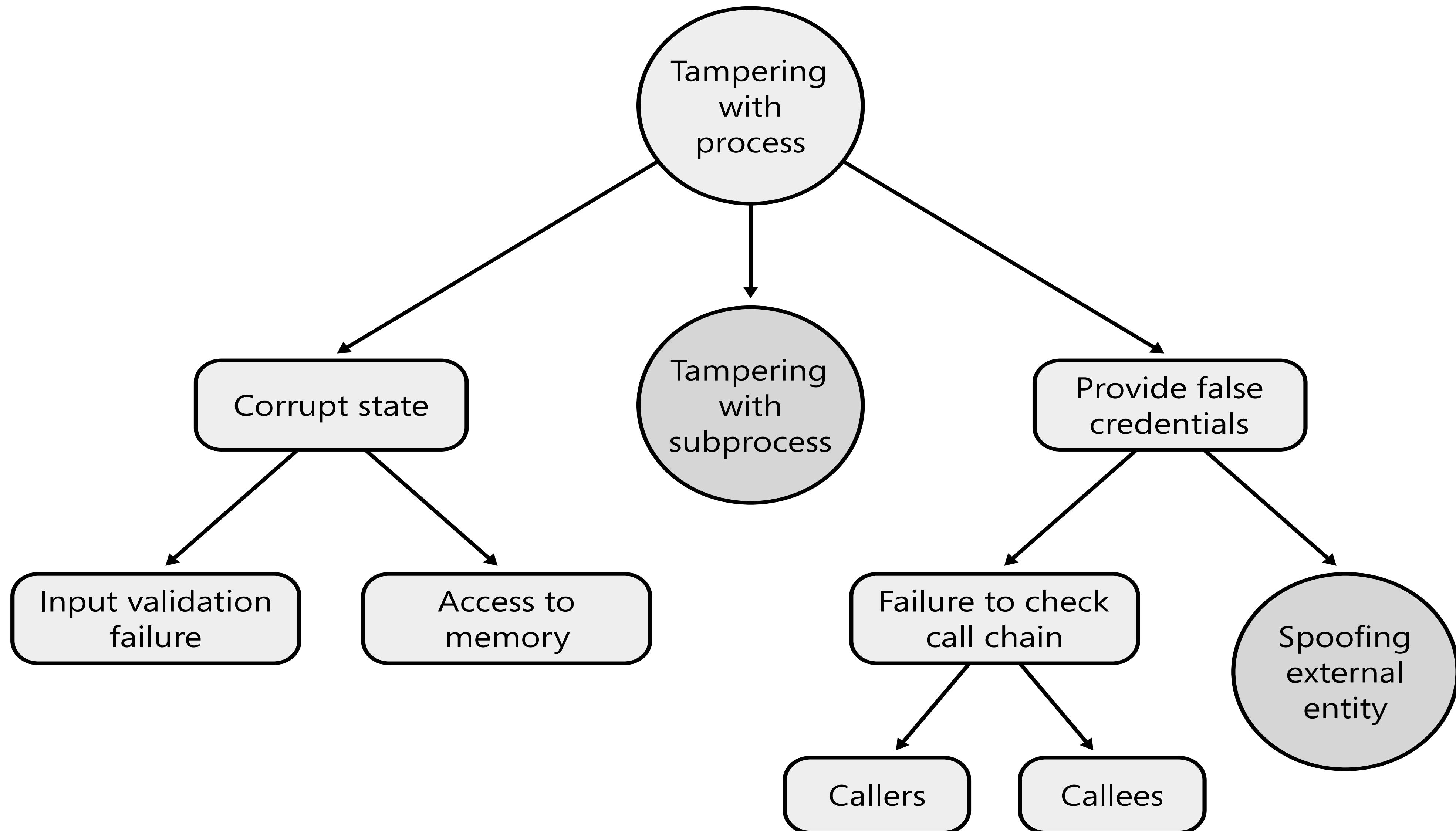
Step 2: Refine threats with tree threat patterns

- Generic threat types are refined into concrete threats via trees
- AND/OR composition of threats
- STRIDE provides 12 threat tree patterns
 - 1 threat tree for Spoofing
 - 3 threat trees for Tampering
 - 1 threat trees for Repudiation
 - 3 threat trees for Information Disclosure
 - 3 threat trees for Denial of Service
 - 1 threat tree for Elevation of Privileges

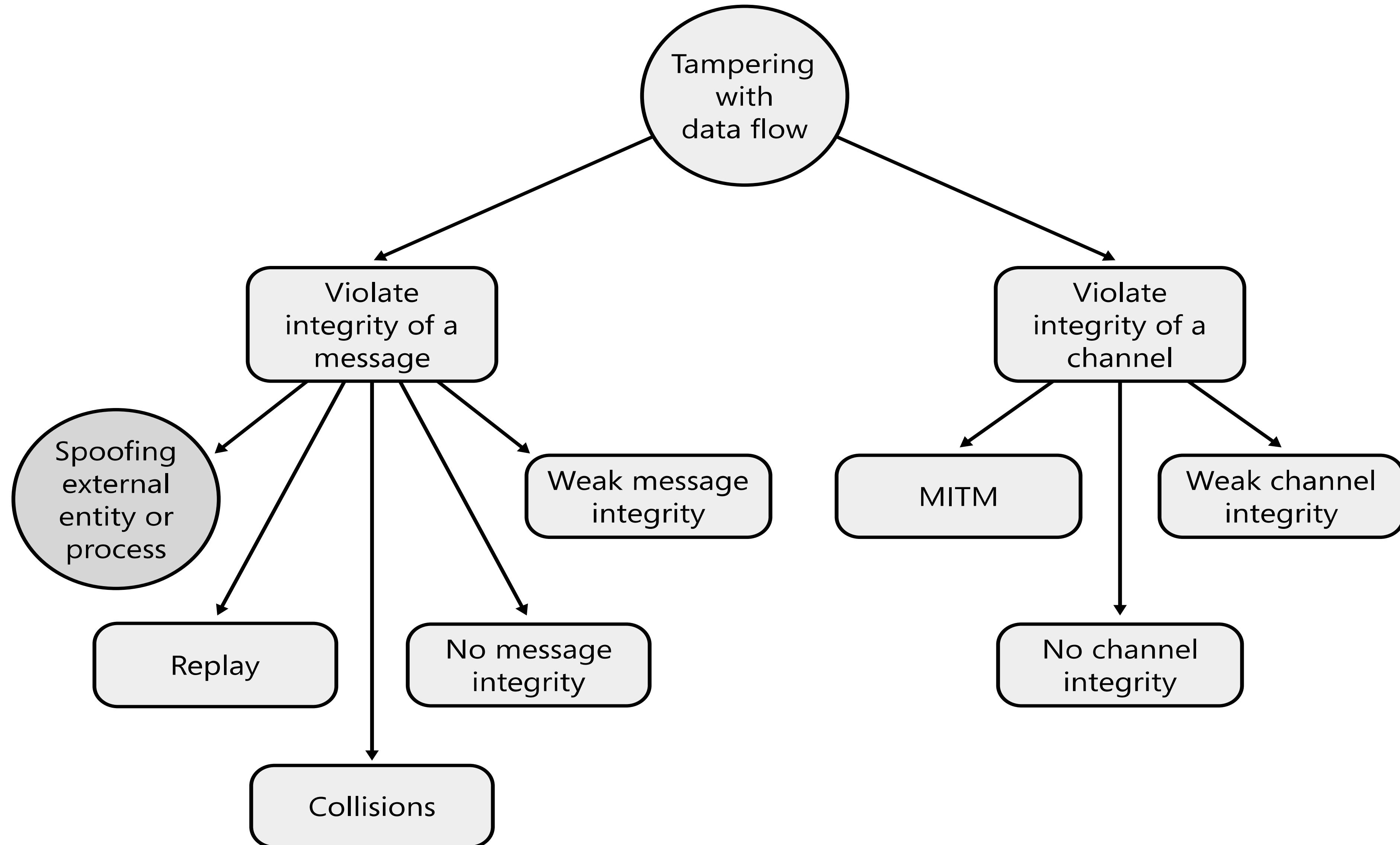
Spoofing an External Entity or Process



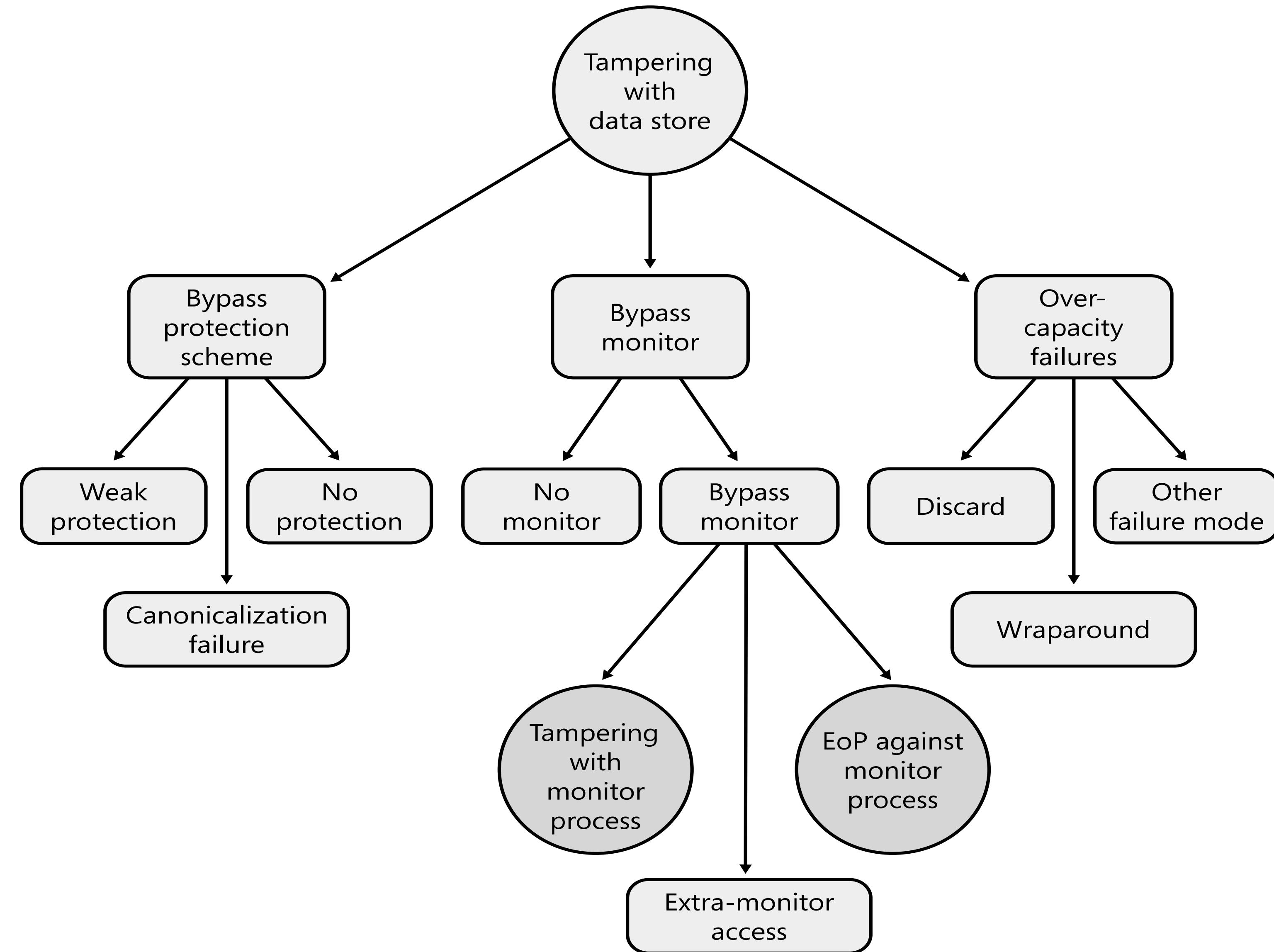
Tampering with a Process



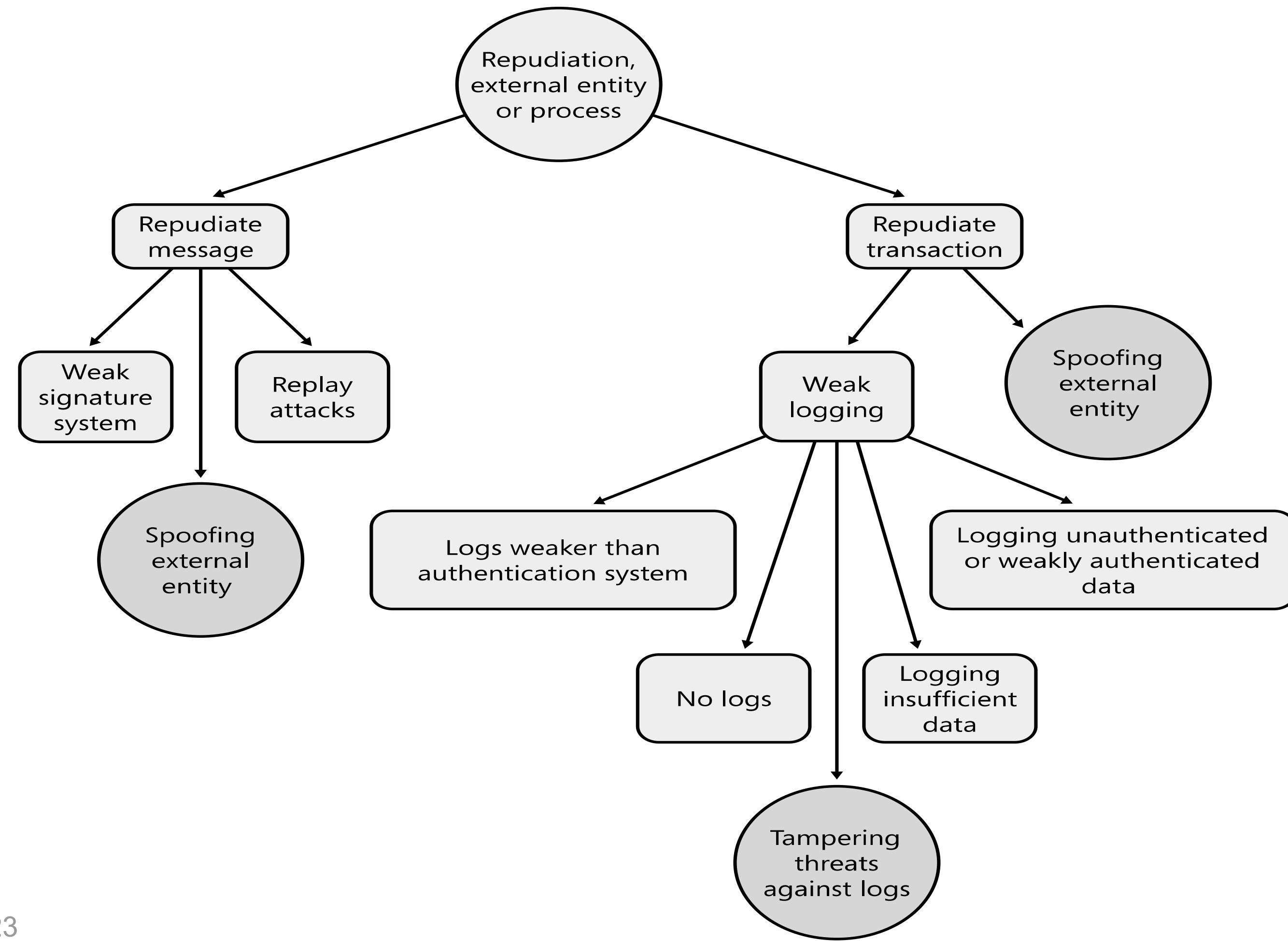
Tampering with a Data Flow



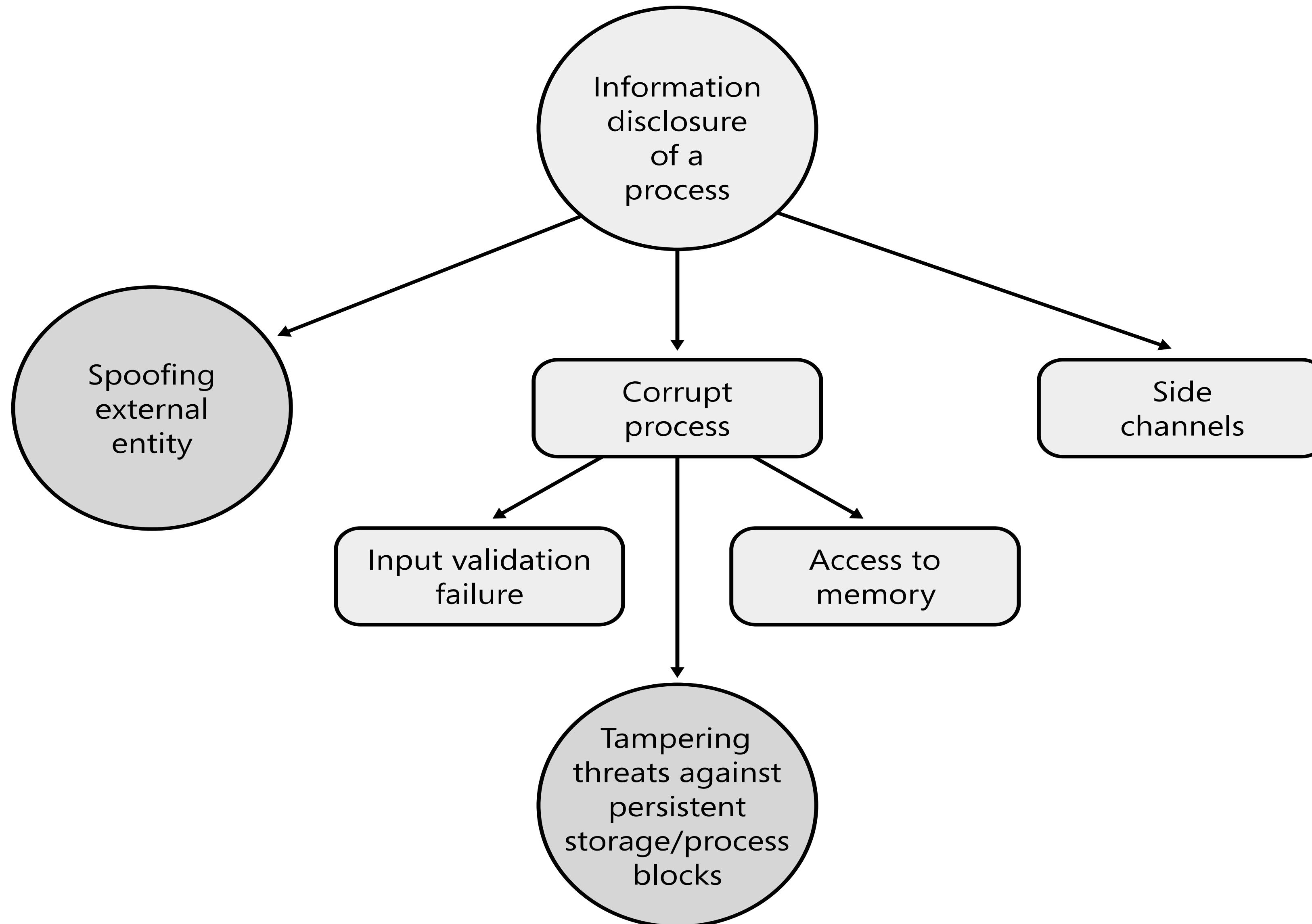
Tampering with a Data Store



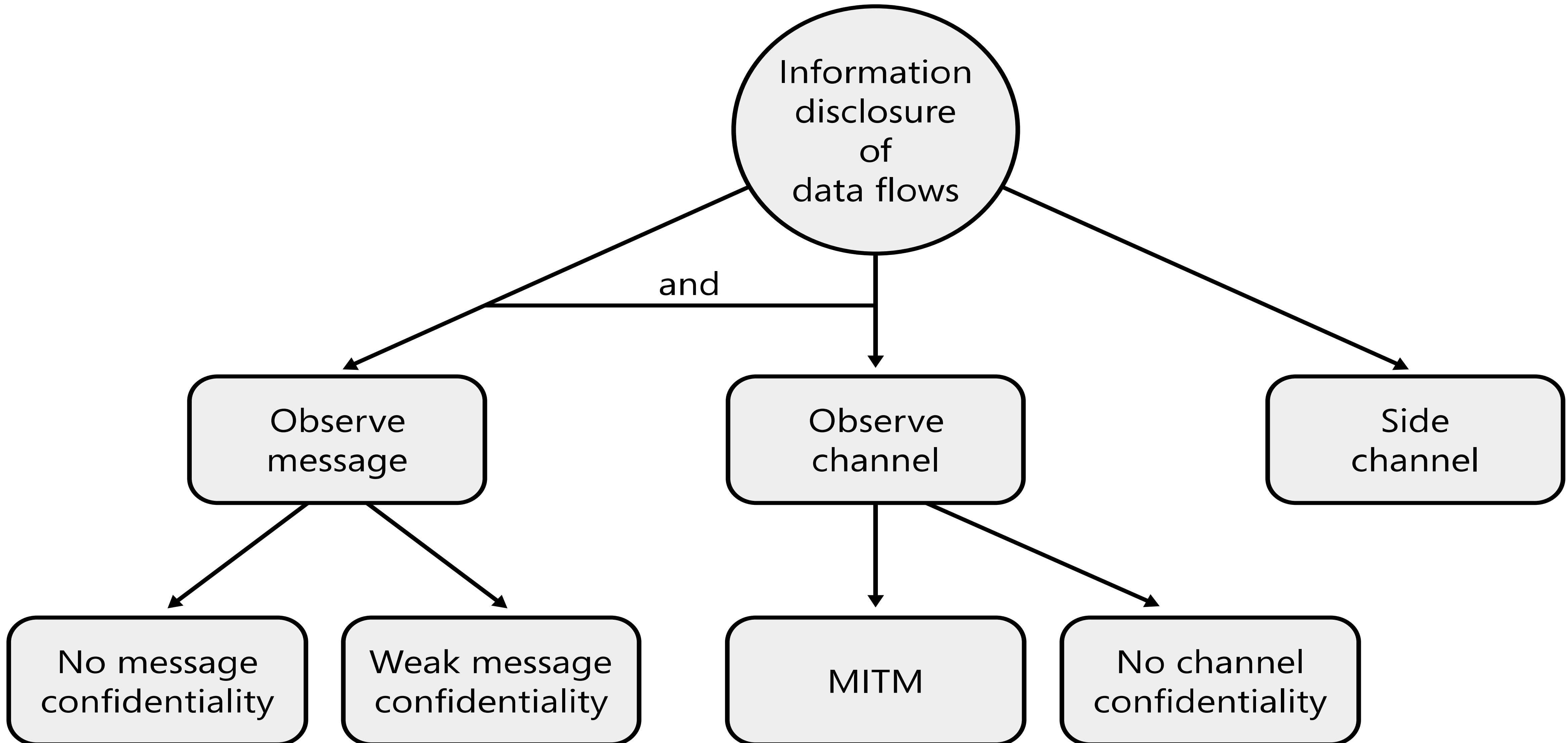
Repudiation



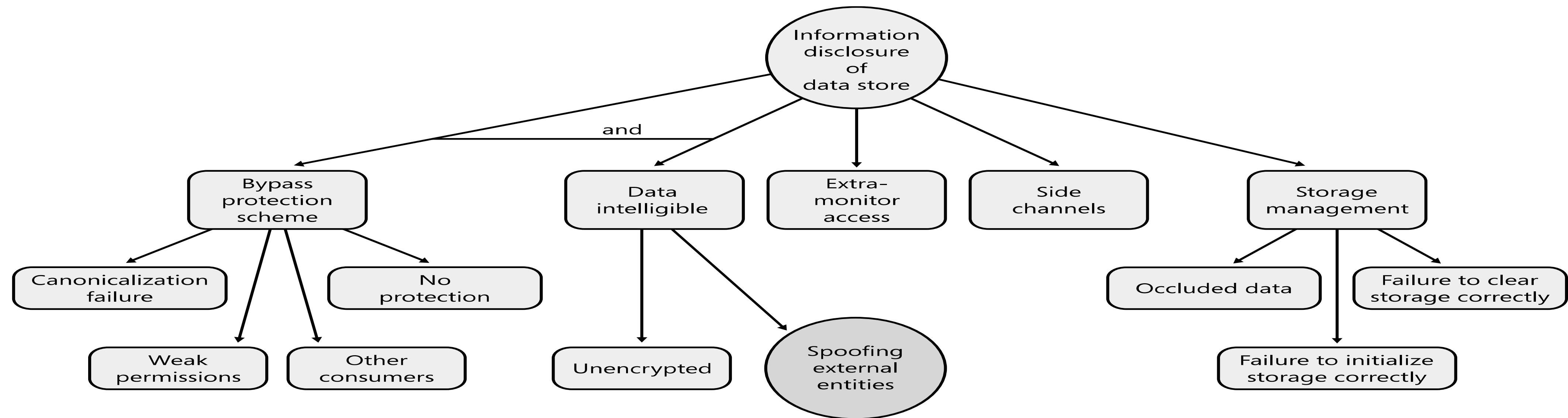
Information Disclosure of a Process



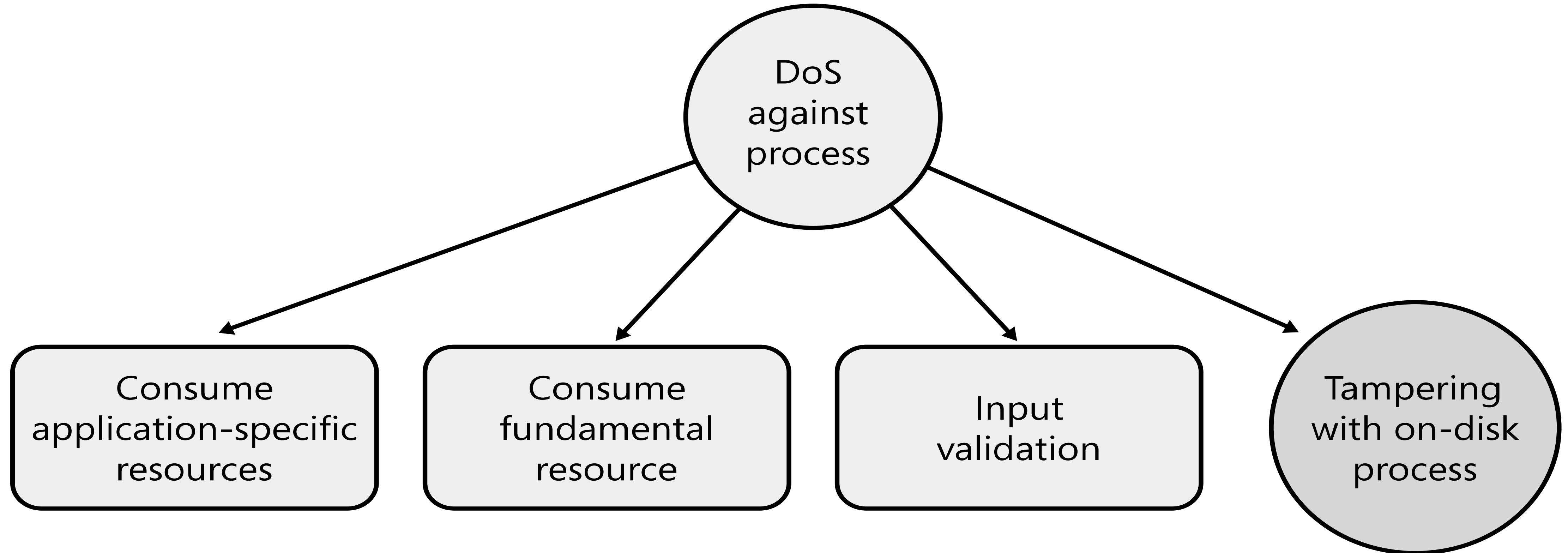
Information Disclosure of a Data Flow



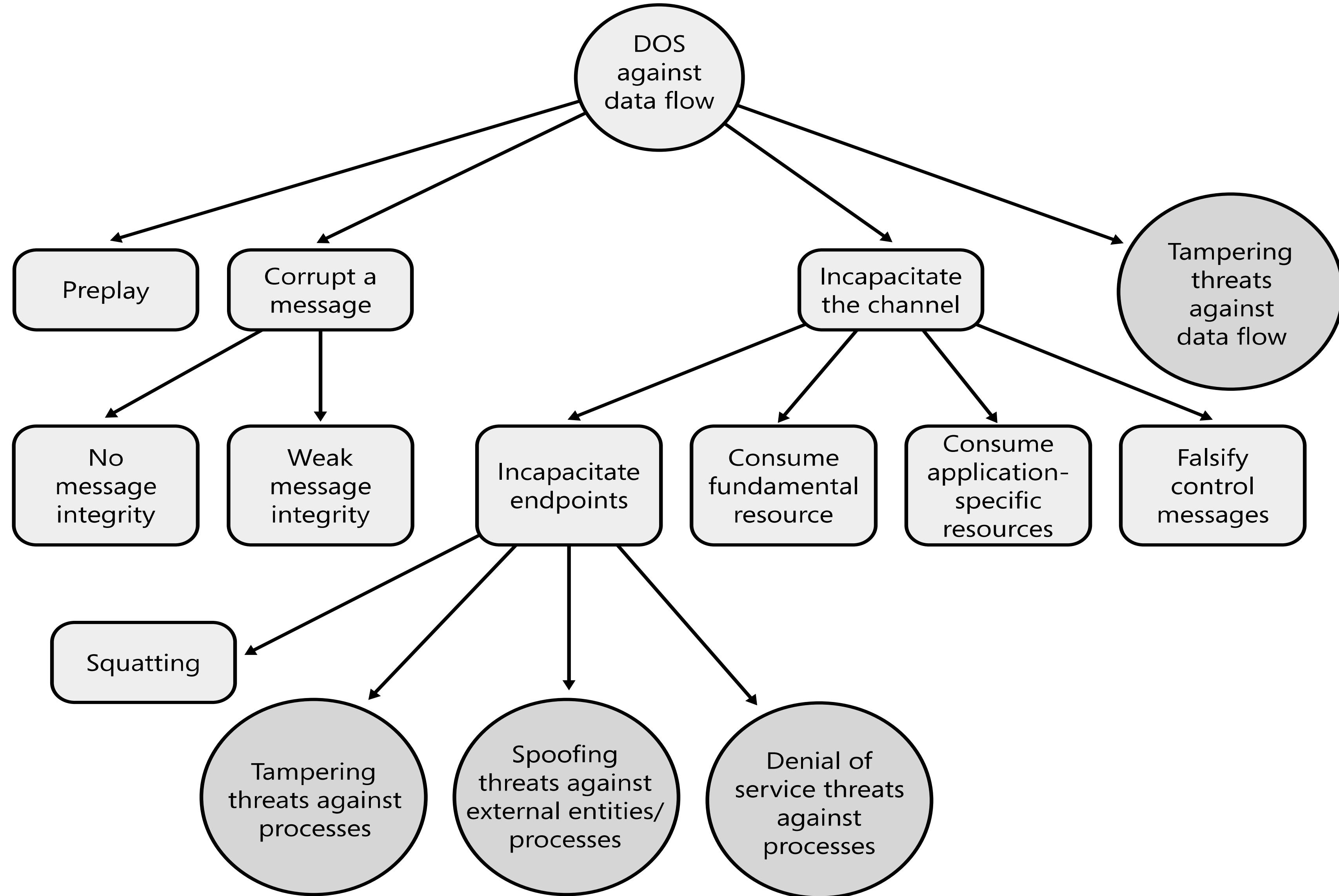
Information Disclosure of a Data Store



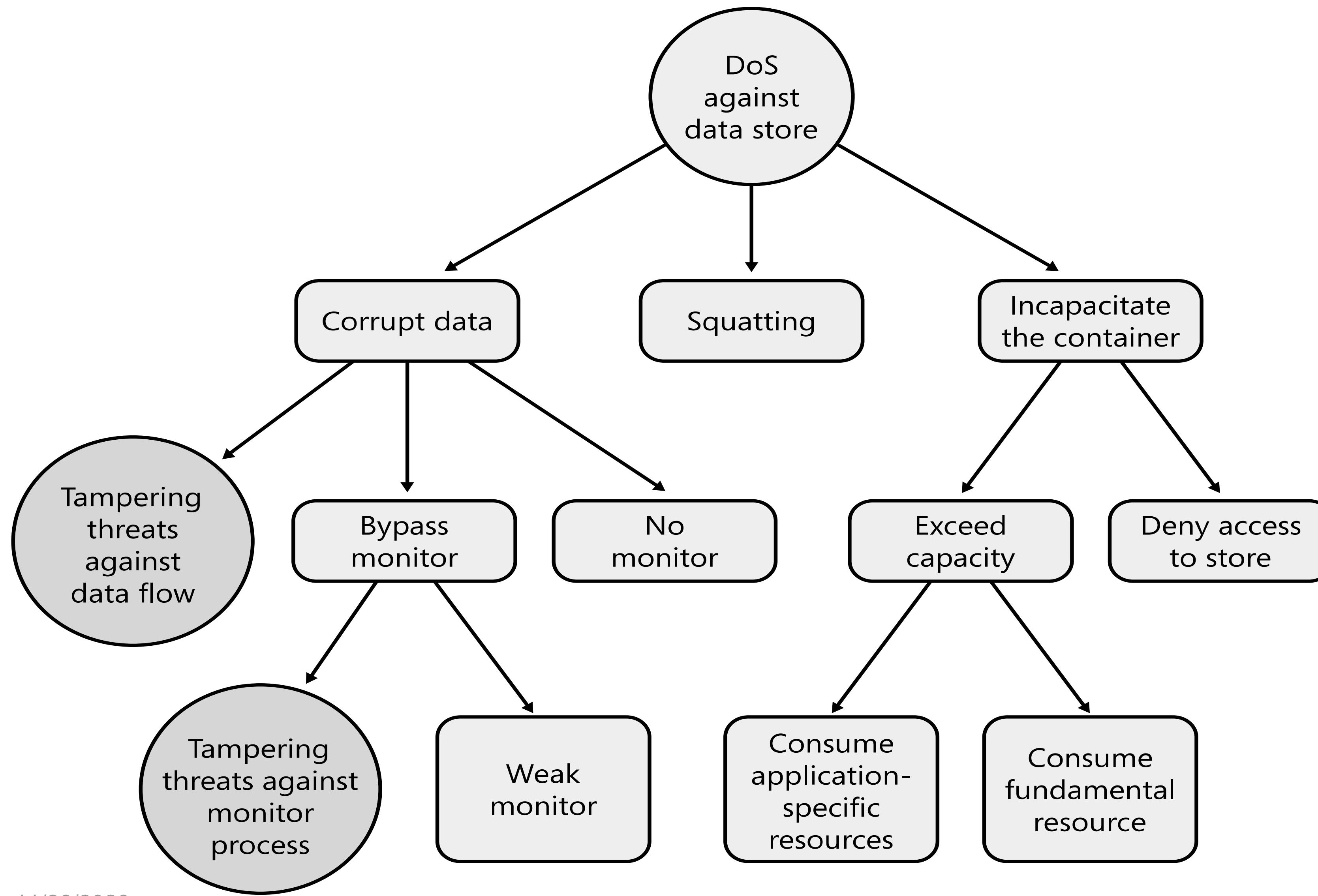
DoS against a Process



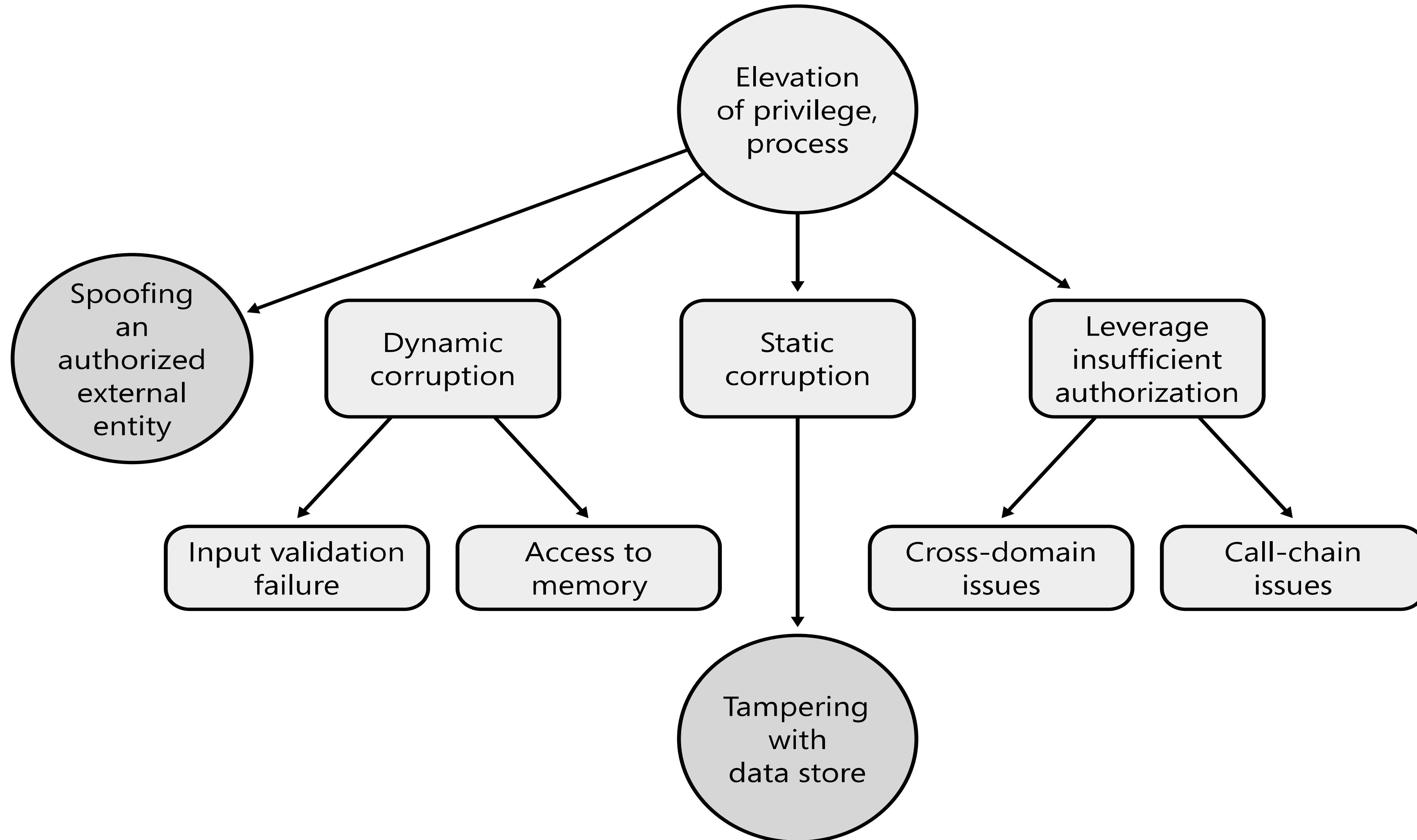
DoS against a Data Flow



DoS against a Data Store



Elevation of Privilege



Refining threats – An Example

DFD Element	Threat Type	Threat
Pet Shop Customer to Web application	Information Disclosure (I)	Observe message – No Message Confidentiality
Audit Log Data Store	Tampering (T)	Tampering with Data Store – Weak Protection
Order Processor	Elevation of Privileges (EoP)	Leverage Insufficient Authorization

Step 2: Assess the Risks

- Risk level given by the combination of likelihood and impact
- 4 Possible Risk Levels
 - 1 very high must be fixed during development phase
 - 2 high must be fixed during development phase
 - 3 medium must be fixed before the product becomes a release candidate
 - 4 low should be fixed only if time permits

How do you assess the risks?

- Microsoft SDL Requirement phase requires to specify **bug bars**
- A *bug bar* classifies threats based on the impact that they have
- First the bug is assigned a STRIDE threat category
- Then a risk level is associated with the threat based on
 - Server application versus client application.
 - Local versus remote accessibility
 - Accessibility to anonymous versus authenticated users
 - Accessibility to authenticated users versus administrators
 - The degree of user interaction required
 - In the case of an information disclosure threat, whether the data is personally identifiable information (PII) or is sensitive data
 - In the case of a DoS attack, whether the application continues service or is non functional once an attack stops

Assessing the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Spoofing	Client	Ability for attacker to present a UI that is different from but visually identical to the UI that users must rely on to make valid trust decisions in a default/common scenario	2
	Server	Computer connecting to server is able to masquerade as a different user or computer of his or her choice <i>using a protocol</i> that is designed and marketed to provide strong authentication.	2

Assessing the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Spoofing	Client	Ability for attacker to present a UI that is different from but visually identical to the UI that users are accustomed to trust in a specific scenario.	3
	Server	Client user or computer is able to masquerade as a different, random user or computer using a protocol that is designed and marketed to provide strong authentication.	3

Assign the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Tampering/Repudiation	Client/Server	Permanent modification of any user data or data used to make trust decisions in a common or default scenario that persists after restarting the OS/application.	2
	Server	Temporary modification of data in a common or default scenario that does not persist after restarting the OS/application.	3
	Client	Temporary modification of any data that does not persist after restarting the OS/application.	4

Assessing the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Information Disclosure	Client/Server	Disclosure of PII (email addresses, phone numbers, credit card information)	2
	Client/Server	Attacker can locate and read information from anywhere on the system	2
	Client/Server	Attacker can locate and read information from known locations	3
	Client Server	Any untargeted information disclosure including runtime data	4

Assessing the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Denial of Service	Client	Requires reinstallation of system and/or components	2
	Client	Requires cold reboot or causes Blue Screen/Bug Check	3
	Client	Temporary DoS: restart of application	4
	Server	Anonymous user sends a small amount of data	2
	Server	Authenticated permanent DoS	3

Assessing the risk level

STRIDE Threat Type	Client/Server	Scope	Risk Level
Elevation of Privilege	Client/Server	Remote user with the ability to execute arbitrary code	1
	Client	Local, low-privilege user can elevate himself to another user, administrator or local system	2
	Server	Local authenticated user has the ability to execute arbitrary code or obtain more privilege than intended	2

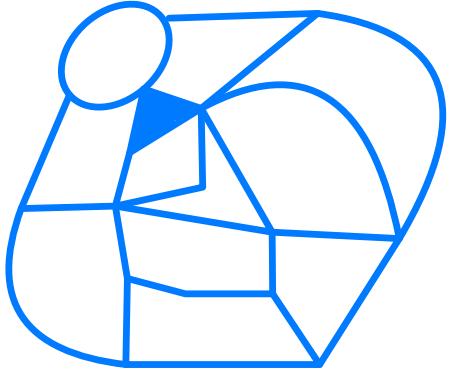
Assessing Risks: An example

DFD Element	Threat Type	Threat	Risk Level
Pet Shop Customer to Web application	Information Disclosure (I)	<ul style="list-style-type: none">Observe message – No MessageConfidentiality	1
Audit Log Data Store	Repudiation(R)	<ul style="list-style-type: none">Tampering with Data Store –Weak Protection	1
Order Processor	Elevation of Privileges (EoP)	<ul style="list-style-type: none">Leverage Insufficient Authorization	1

Exercise4: Part 2 – Refine Threats and Assess Risks

1. For each identified threat type to a DFD element

1. Refine into a concrete threat
2. Assess the risk of the threat (from 1 to 4)



Time: 10 minutes

User

Spoofing

Guessed

1

SN DB

Tampering
Information Disclosure
Denial of Service

Step 3: Plan for Mitigations

- Four ways to address threats
 1. Do Nothing
 2. Remove the feature
 3. Accept vulnerability in design
 4. Counter the threats with technology
 - ✓ Use list of mitigation technologies

Standard Mitigations

Threat	Property	
<u>Spoofing</u>	<u>Authentication</u>	<p>To authenticate principals:</p> <ul style="list-style-type: none">• MFA• Kerberos authentication• PKI systems, such as SSL or TLS and certificates• IPSec• Digitally signed packets <p>To authenticate code or data:</p> <ul style="list-style-type: none">• Digital signatures• Message authentication codes• Hashes

Standard Mitigations

Threat	Property	Mitigation
<u>Tampering</u>	<u>Integrity</u>	<ul style="list-style-type: none">• Windows Vista mandatory integrity controls• ACLs• Digital signatures• Message authentication codes

Standard Mitigations

Threat

Repudiation

Property

Nonrepudiation

- Strong authentication
- Secure logging and auditing
- Digital signatures
- Secure time stamps
- Trusted third parties

Standard Mitigations

Threat

Information Disclosure

Property

Confidentiality

- Encryption
- ACLs

Standard Mitigations

Threat

Denial of Service

Property

Availability

- ACLs
- Filtering
- Quotas
- Authorization
- High-availability designs

Standard Mitigations

Threat

Elevation of
Privilege

Property

Authorization

- ACLs
- Group or role membership
- Privilege ownership
- Permissions
- Input validation

Example – Step 3 - Plan for Mitigations

DFD Element	Threat Type	Threat	Mitigation
Pet Shop Customer to Web application	I	Observe message	SSL/TLS
Audit Log Data Store	R	Bypass protection scheme	ACL and MAC
Order Processor	EoP	Leverage Insufficient Authorization	ACL

Step 4: Validating Threat Models

- Validate the whole threat model
 - Does diagram match final code?
 - Are threats enumerated?
 - Minimum: STRIDE per element that touches a trust boundary
 - Is each threat mitigated?
 - Are mitigations done right?

Summary

- Threat modeling helps to find and proactively mitigate security design flaws before the system is built
- Microsoft STRIDE is a systematic process to identify and mitigate security design flaws
- It can be used by non security experts
 - taxonomy of threats
 - threats tree patterns
 - standard mitigations for threats

Recommended Readings

- Threat modeling
<https://www.ncsc.gov.uk/collection/risk-management/threat-modelling>
- M. Howard and S. Lipner. The Security Development Life Cycle, 2006. Chapters 9 and 22
- Threat Modeling Available at:
https://www.owasp.org/index.php/Application_Threat_Modeling
- Threat Modeling Lessons from Star Wars (and Elsewhere): Available at:
<https://www.youtube.com/watch?v=KLpgaoD8ySM>