Universidade do Minho
Departamento de Informática

Tecnologias de Segurança

João Marco Silva
joaomarco@di.uminho.pt

Threat Modelling

- What is a threat?

A category of objects, people, or other entities that represents a danger to the security properties of an asset

Threat Modelling

- What is threat modelling?
  - an analysis process to figure out what might be wrong with the thing you’re building
  - a set of idealised attackers
  - abstracting threats into classes
    - *e.g.*, tampering, spoofing…
  - the use of abstractions to aid in thinking about risks

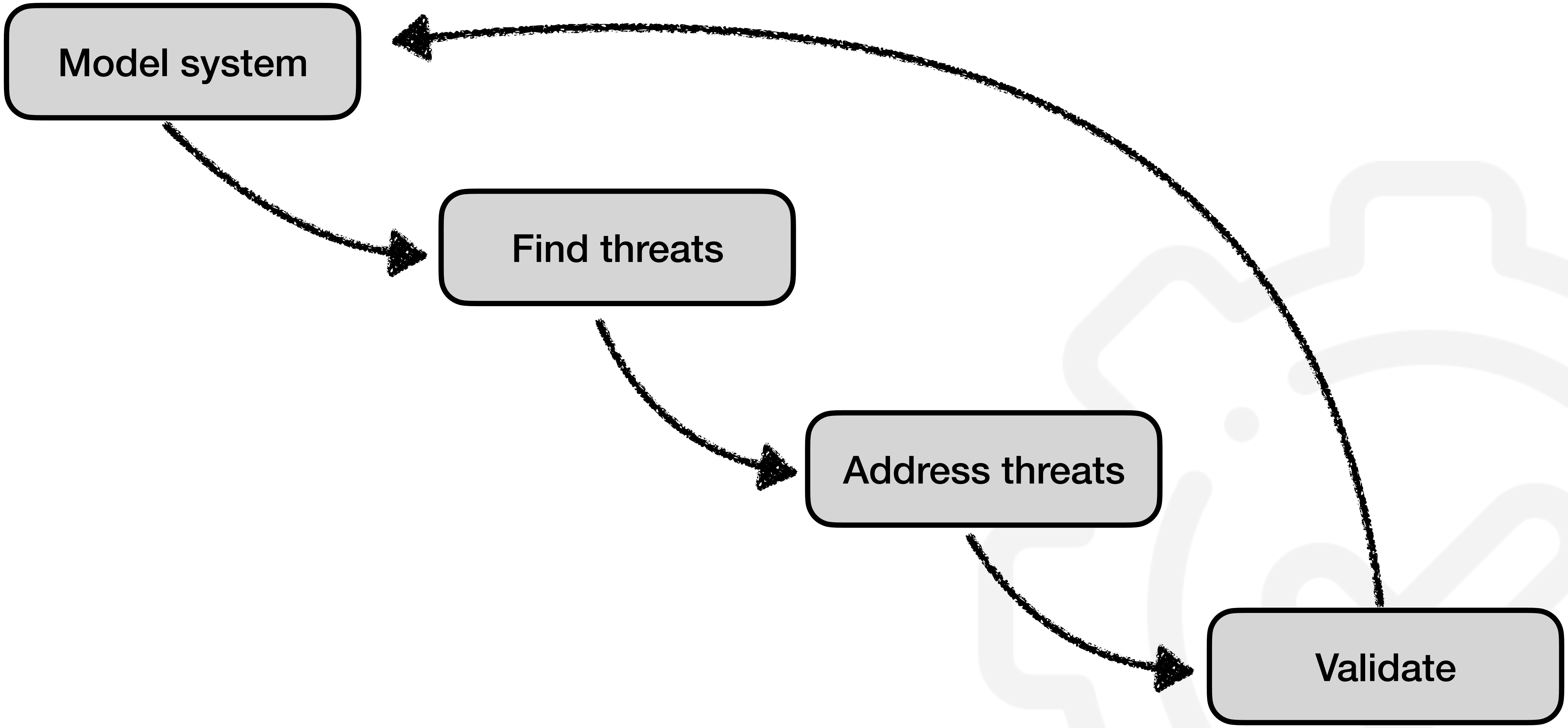
Threat Modelling

- Reasons to threat model
    - find security issues early
        - the early you find problems, the easier it is to fix them
    - understand your security requirements
    - engineer and deliver better products

A good model helps address classes or groups of attacks and deliver a more secure product.

Threat Modelling

- The four-steps framework



Threat Modelling

- Initial remarks
    - there’s more than one way to threat model
    - the right way is the way that finds relevant threats
    - threat modelling is an iterative process
    - it requires both techniques and repertoire

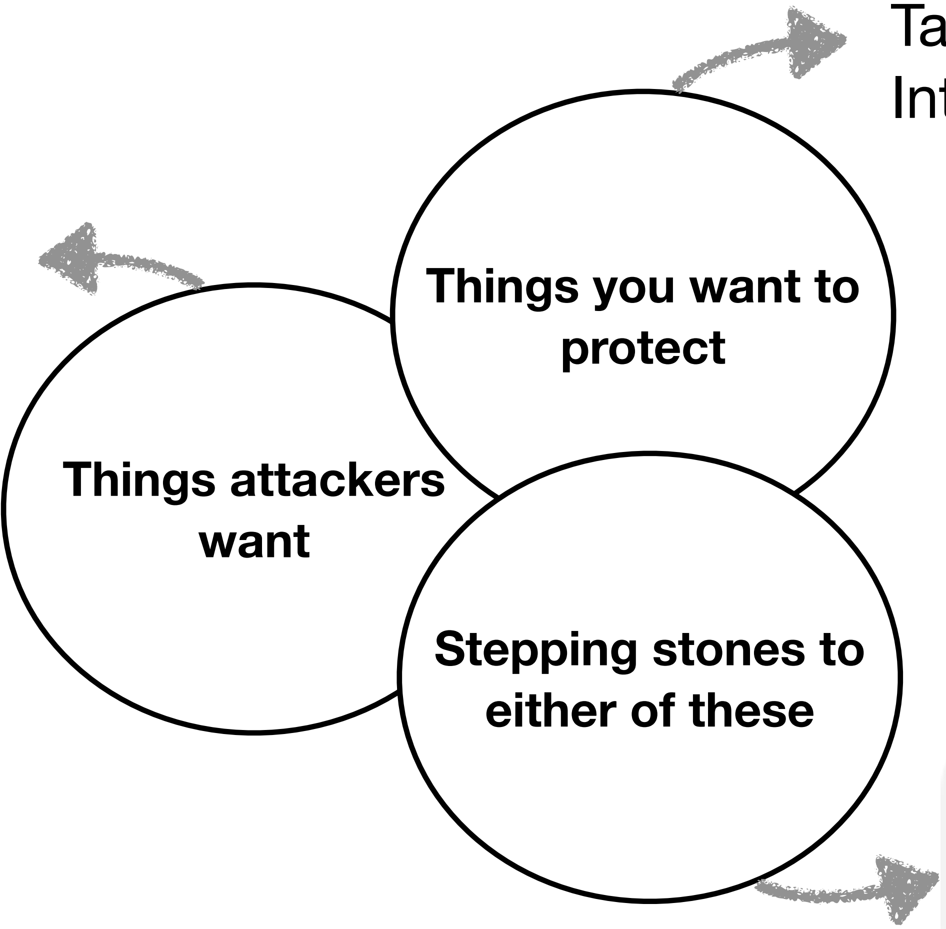
Threat Modelling

- Strategies
  - Unstructured
    - brainstorming
    - literature review
  - Structured
    - focusing on assets
    - focusing on attackers
    - focusing on software

Strategies

- Focusing on Assets

User passwords or keys
Credit card numbers
Confidential business data


Things attackers want
Things you want to protect
Stepping stones to either of these

Tangible things attackers want
Intangible assets

- reputation
- things that matters to customers

Firewall
VPN Service
Authentication system

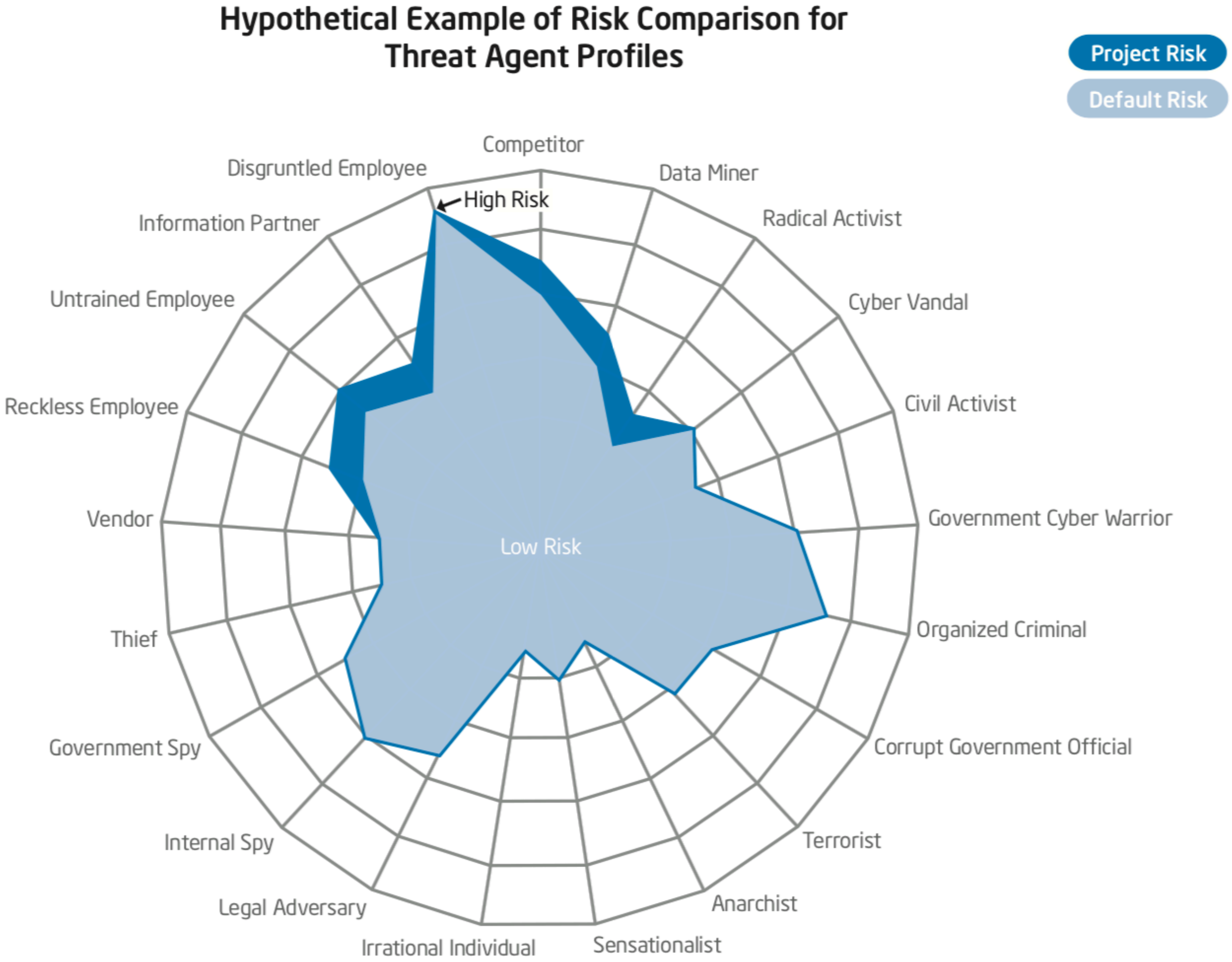
Strategies

- Focusing on attackers
  - useful to explain who might attack an asset and why
  - Common sets of attackers
    - Barnard’s List
      - Intrusion Detection Systems, 1988 ISBN:978075064278
    - Verizon’s List
      - Verizon Data Breach Intelligence Report

Strategies

- Focusing on attackers
  - Common sets of attackers
    - OWASP - The Open Web Application Security Project
      - https://www.owasp.org/index.php/Category:Attack
    - Intel TARA - Threat Agent Risk Assessment
      - Threat Agent Library

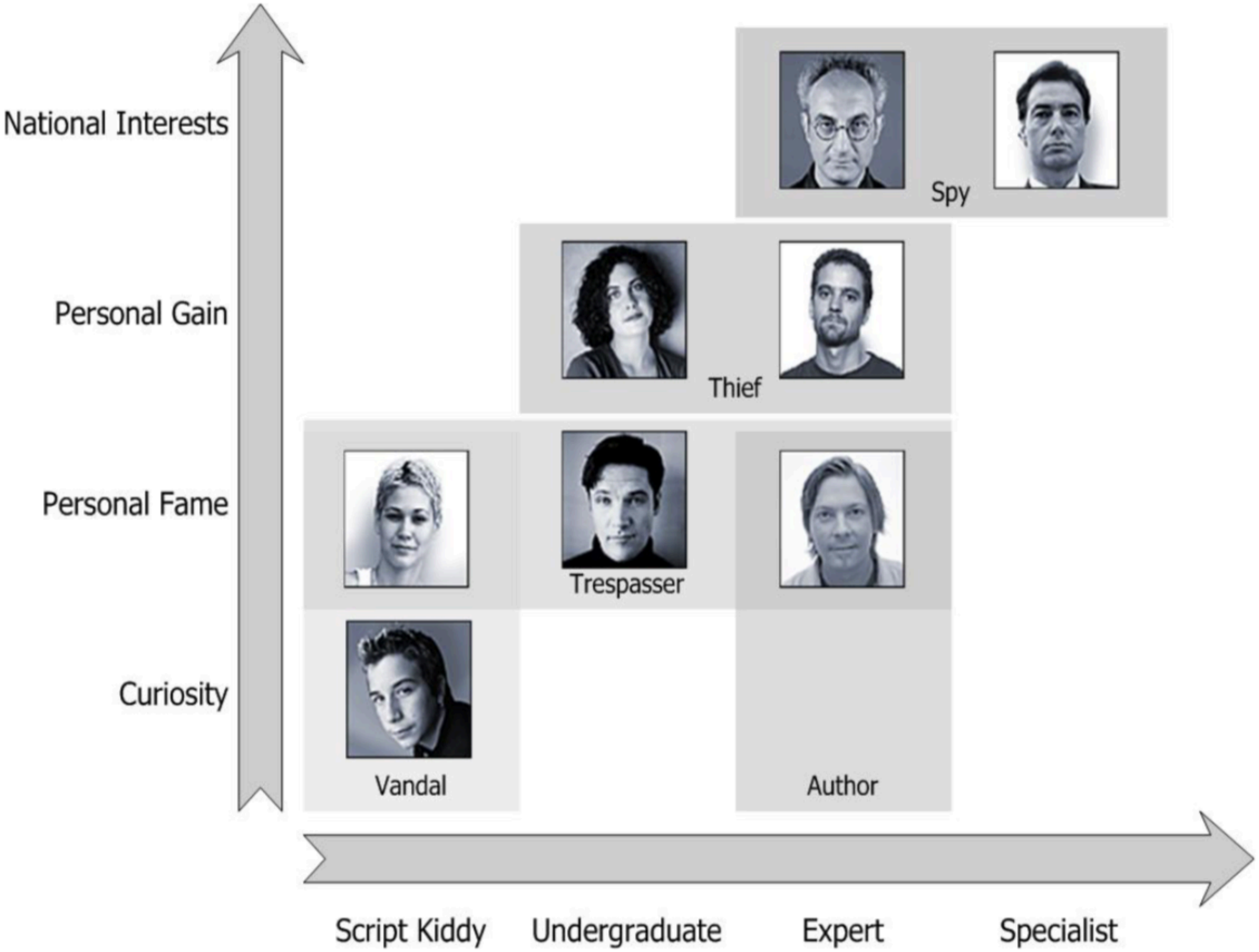
Strategies



Source: Prioritizing information security risks with threat agent risk assessment (TARA)

Strategies

- Personas and Archetypes



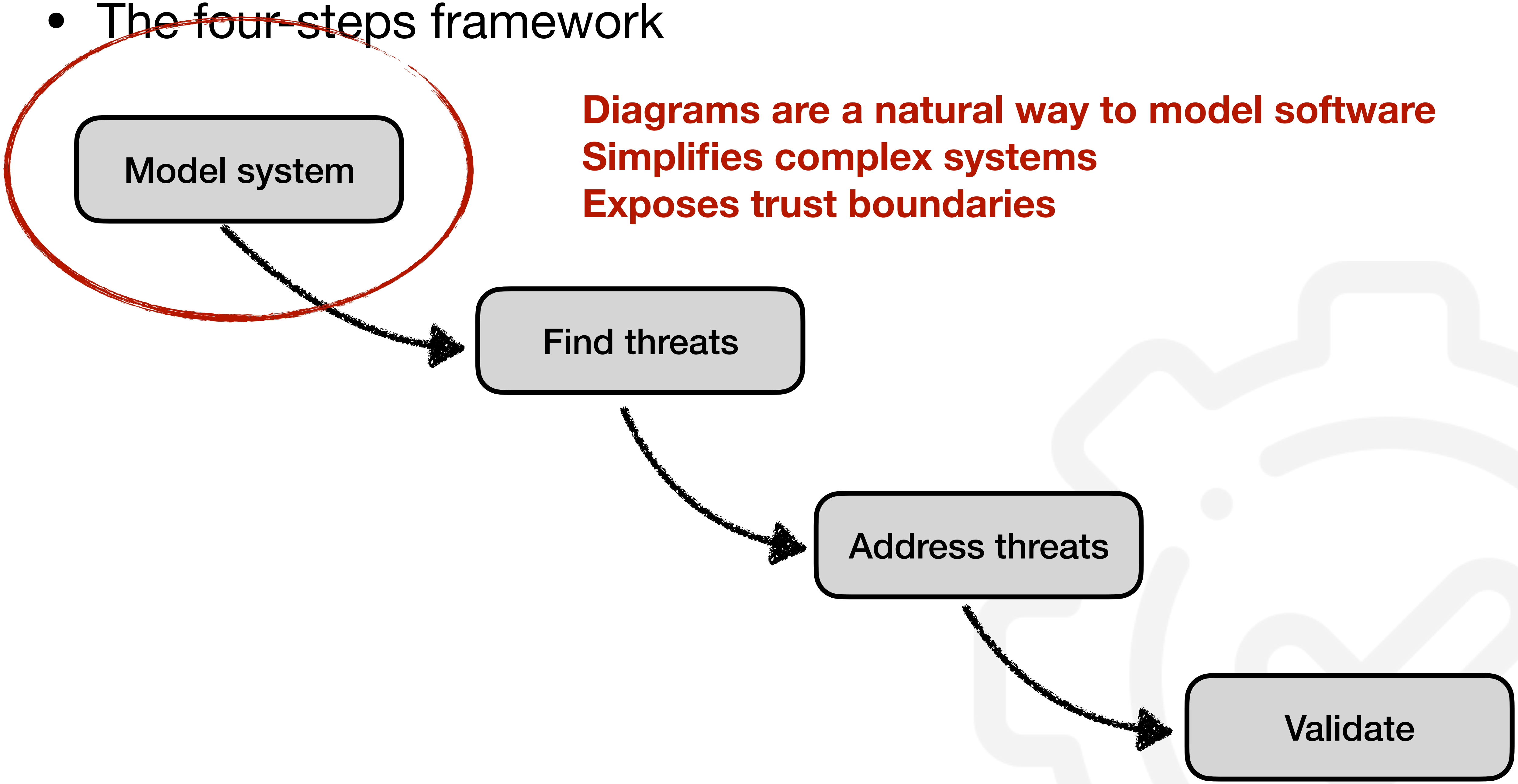
Motivation vs Skill: Based on FBI analysis of cyber-attack data

Strategies

- Focusing on software
  - suitable for large and complex projects
  - can use diverse document models as input
    - UML diagrams, architecture, or APIs
  - can be applied to all sorts of software
    - it doesn’t depend on the business or deployment model
  - developers understand the software they’re developing

Threat Modelling

- The four-steps framework



Diagrams are a natural way to model software
Simplifies complex systems
Exposes trust boundaries

System modelling

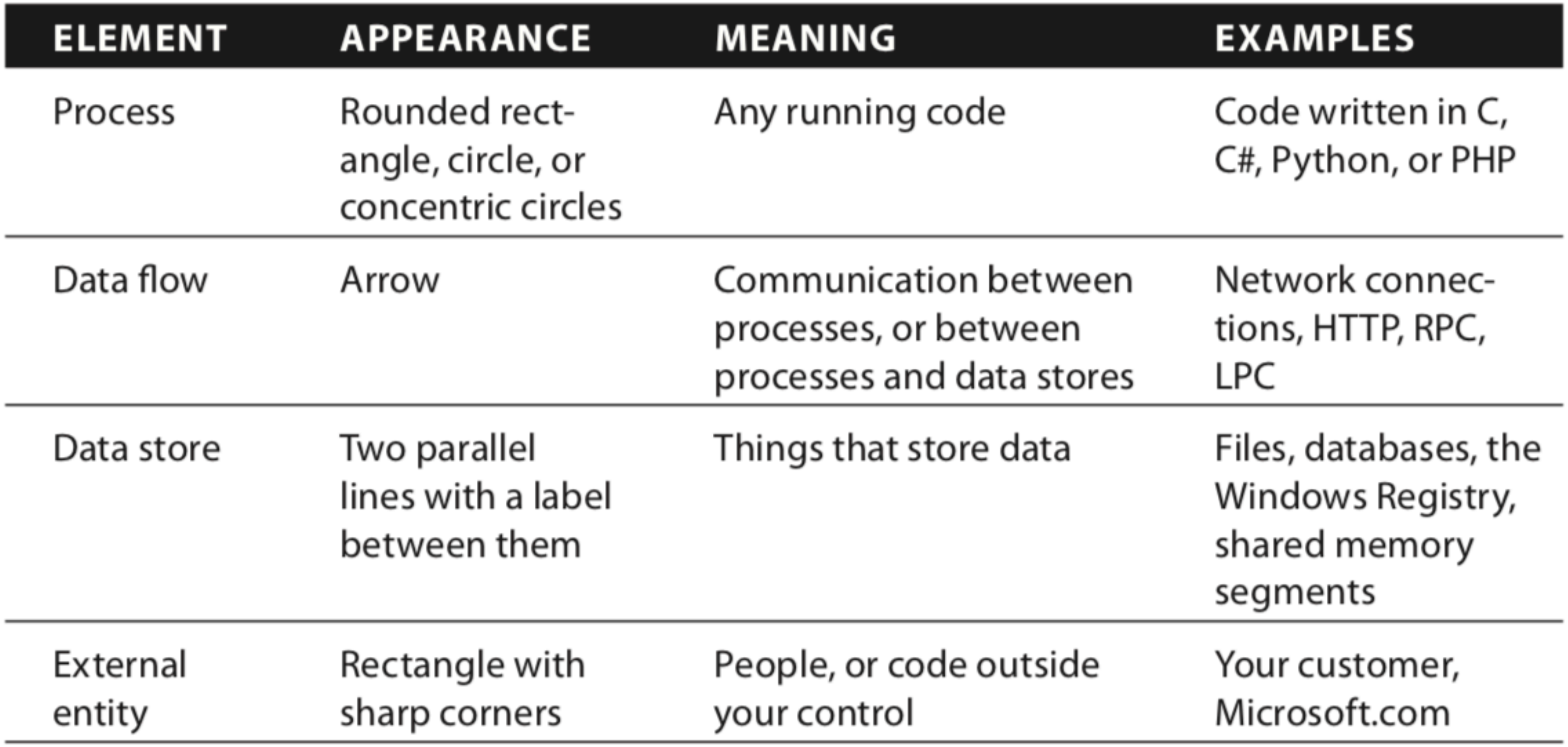
- Types of diagrams
  - Data Flow Diagrams - DFDs
  - UML
  - Swim Lane Diagrams
  - State Diagrams
- Trust boundaries

System modelling

- DFD - Data Flow Diagram
  - commonly used for network or architected systems
  - suitable for threats that tend to follow the data flow, not the control flow
  - also called “threat model diagrams.”

System modelling

- DFD - Data Flow Diagram

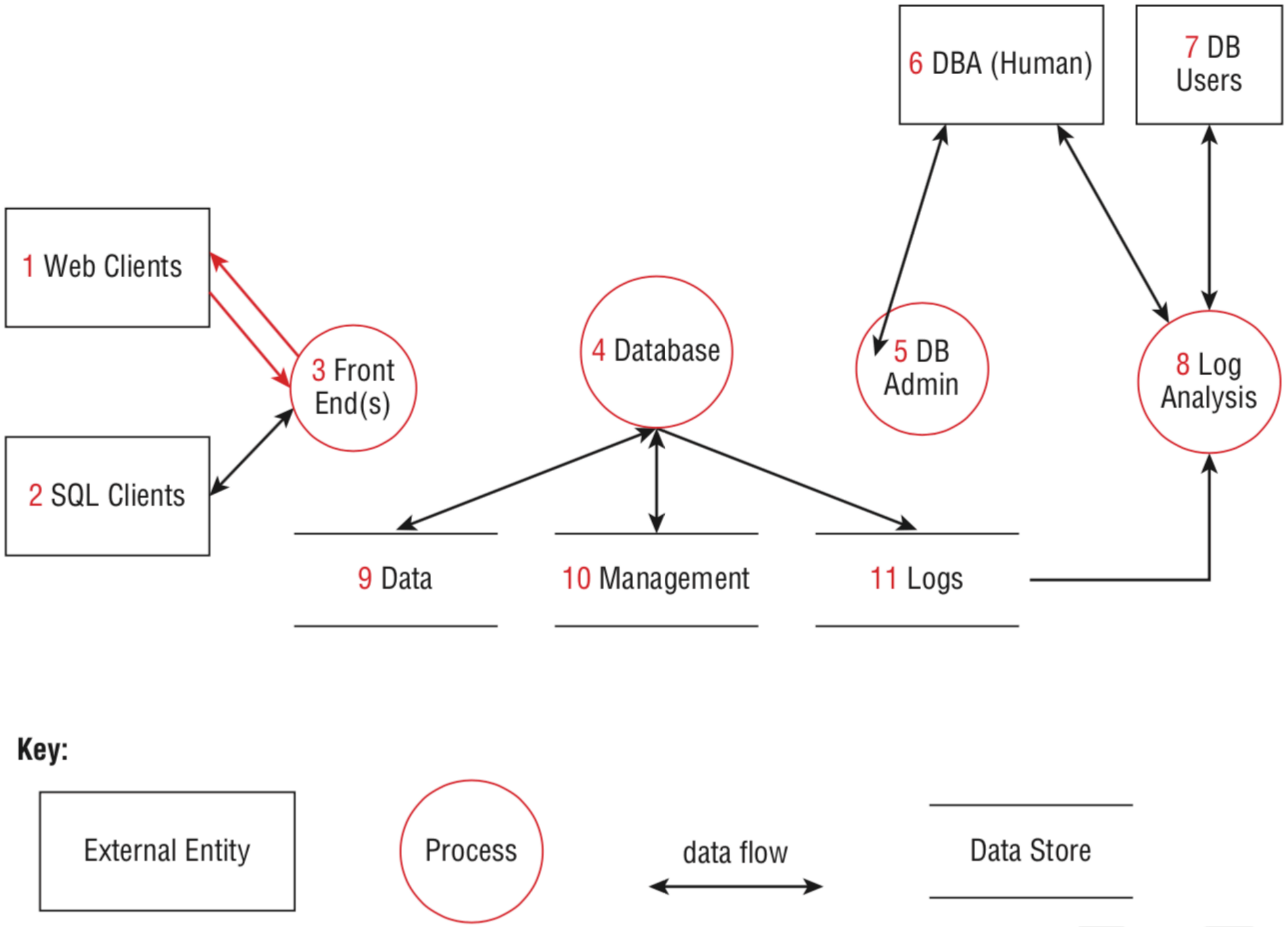


ELEMENT	APPEARANCE	MEANING	EXAMPLES
Process	Rounded rectangle, circle, or concentric circles	Any running code	Code written in C, C#, Python, or PHP
Data flow	Arrow	Communication between processes, or between processes and data stores	Network connections, HTTP, RPC, LPC
Data store	Two parallel lines with a label between them	Things that store data	Files, databases, the Windows Registry, shared memory segments
External entity	Rectangle with sharp corners	People, or code outside your control	Your customer, Microsoft.com

Elements of a DFD

System modelling

- DFD - Data Flow Diagram



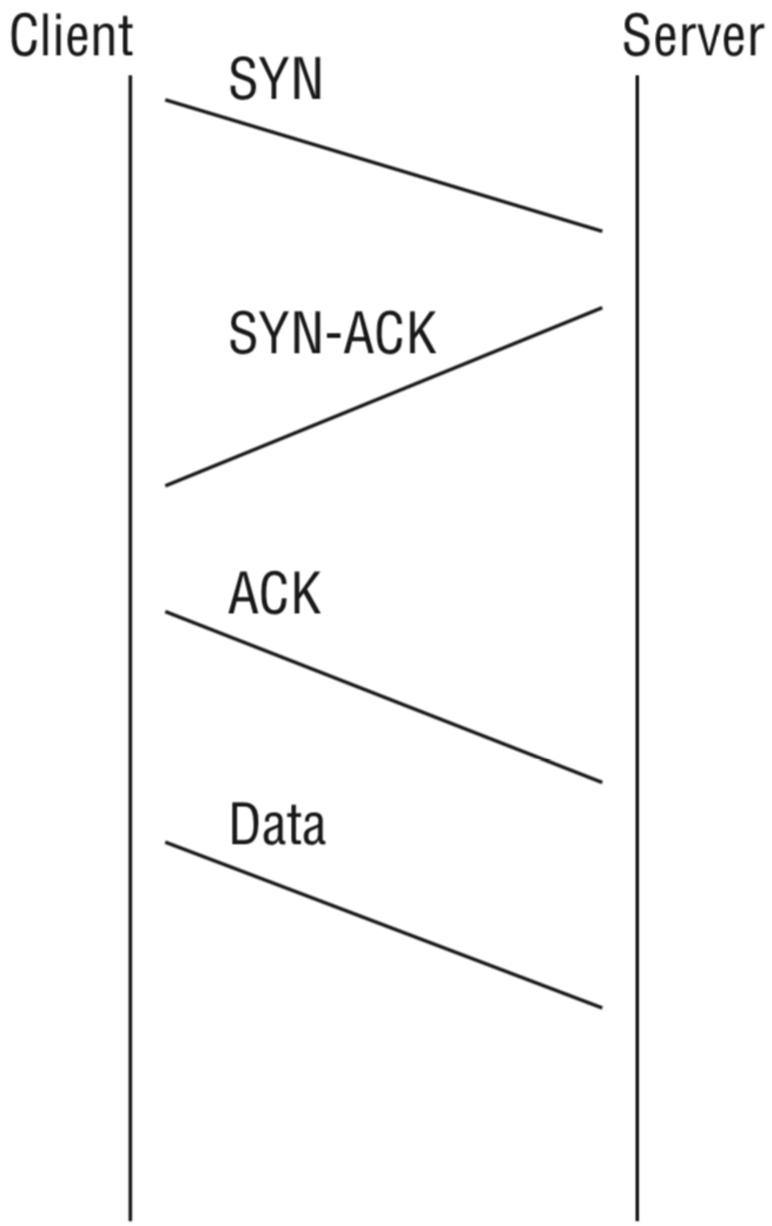
An example of DFD

System modelling

- Swim Lane Diagrams
  - a common way to represent flows between various participants
  - suitable for protocols
  - components
    - entities; messages; time
  - unclear for representing computation done by the entities

System modelling

- Swim Lane Diagrams



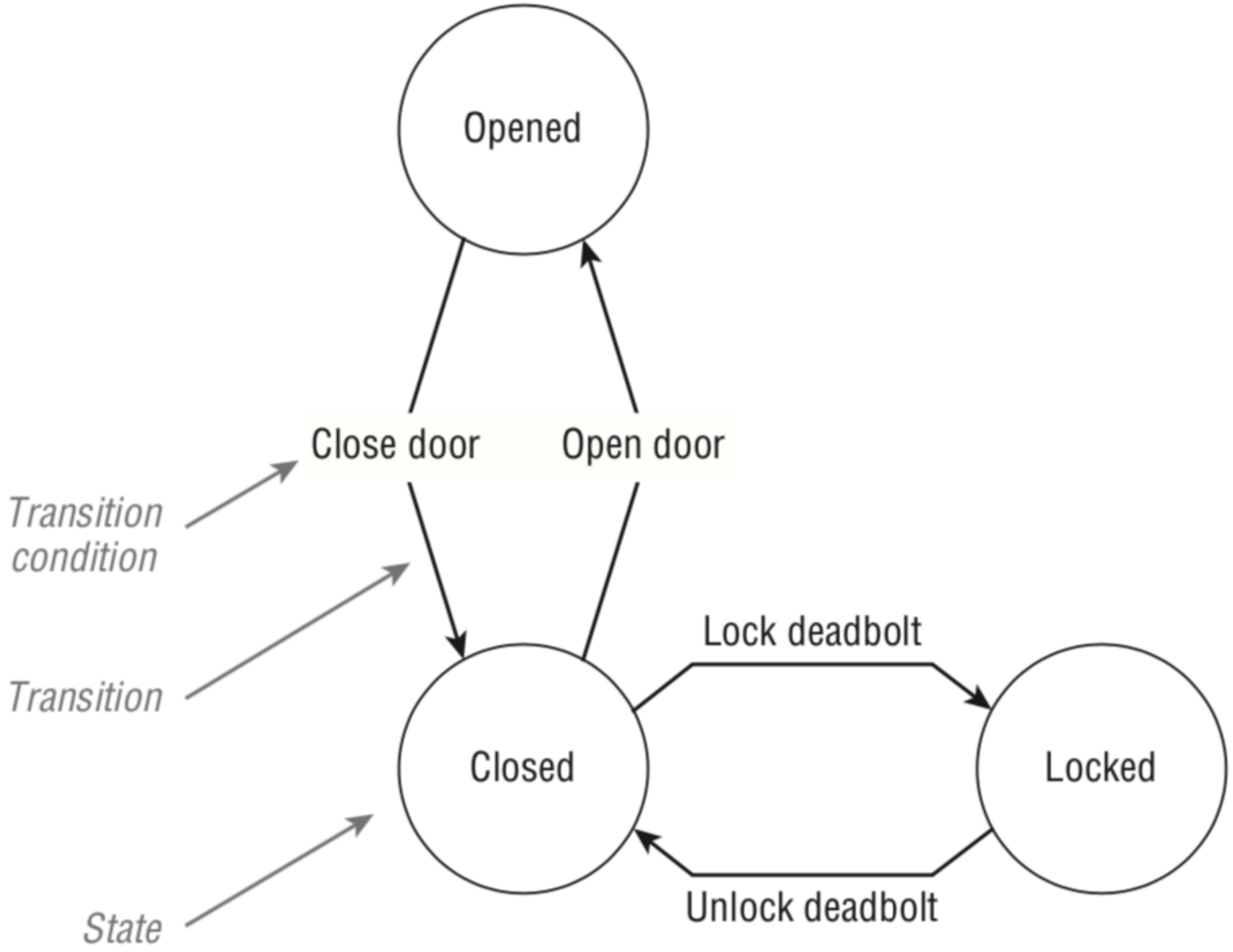
Swim lane diagram - The start of a TCP connection

System modelling

- State Diagram
  - represents the various states a system can be in, and the transmission between those states
  - components - for a computer system
    - state; memory; rules
  - in threat modelling
    - used to check whether each transition complies with the appropriate security validation

System modelling

- State Diagram



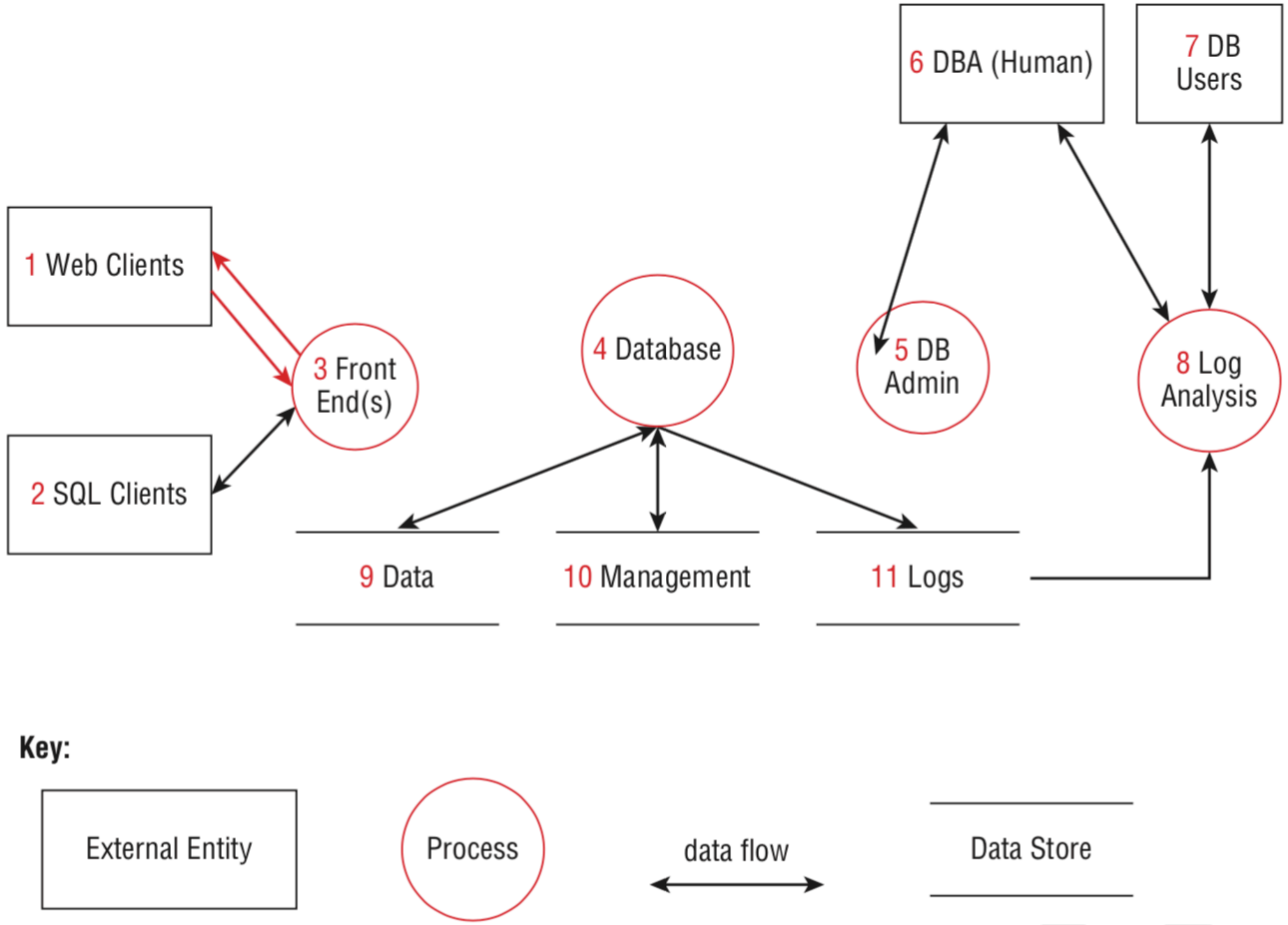
A state machine diagram

System modelling

- Trust boundaries
  - describe the edge where a program data or execution changes its level/domain of trust
  - usually added after the software model
  - iterative processes
  - examples
    - unix UIDs; Windows sessions; machines; network segments; subsystems

System modelling

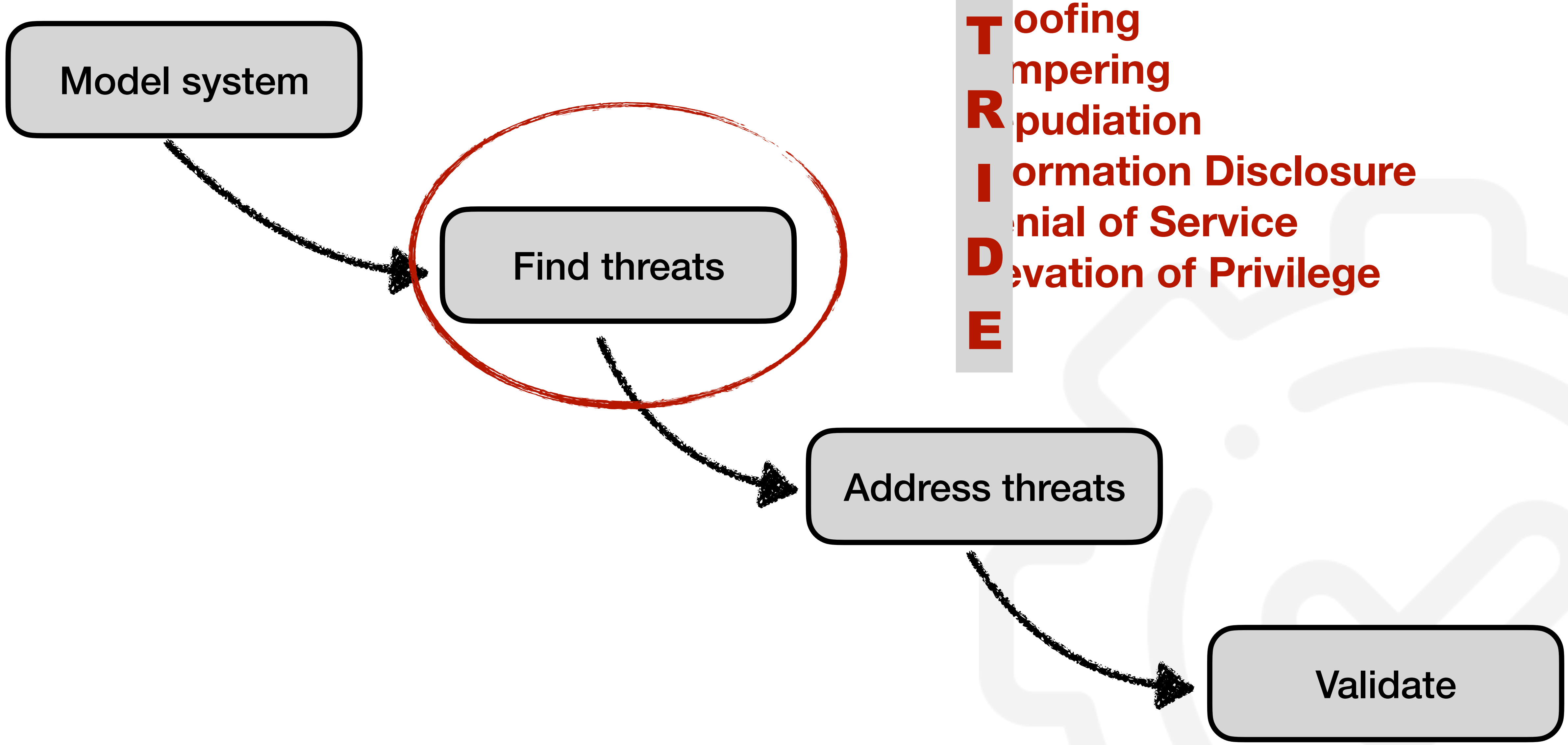
- Trust boundaries



An example of DFD with trust boundaries

Threat Modelling

- The four-steps framework



S

T **oofing**

mpering

R **pudiation**

I **ormation Disclosure**

nial of Service

D **evation of Privilege**

E

STRIDE

- Spoofing
  - Pretending to be something or someone other than yourself - Impersonating a system or a person
  - Property violated: Authentication
  - Typical victims: processes; external entities; people
  - Examples
    - email spoofing - changing email header
    - DNS spoofing

STRIDE

- Tampering
  - Modifying data on disk, on a network, or in memory
  - Property violated: Integrity
  - Typical victims: data stores; data flows; processes
  - Examples
    - adding or removing packets traversing a network
    - changing values in a DB

STRIDE

- Repudiation
  - The act of refusing authoring of something that happened
  - Property violated: Non-Repudiation
  - Typical victims: processes; people
  - Examples
    - neutralize the logging system
    - using untrusted certificates

STRIDE

- Information Disclosure
  - Disclosing information to an entity not authorised to have access to it
  - Property violated: Confidentiality
  - Typical victims: processes; data stores; data flows
  - Examples
    - data remanence
    - file name and path disclosure

STRIDE

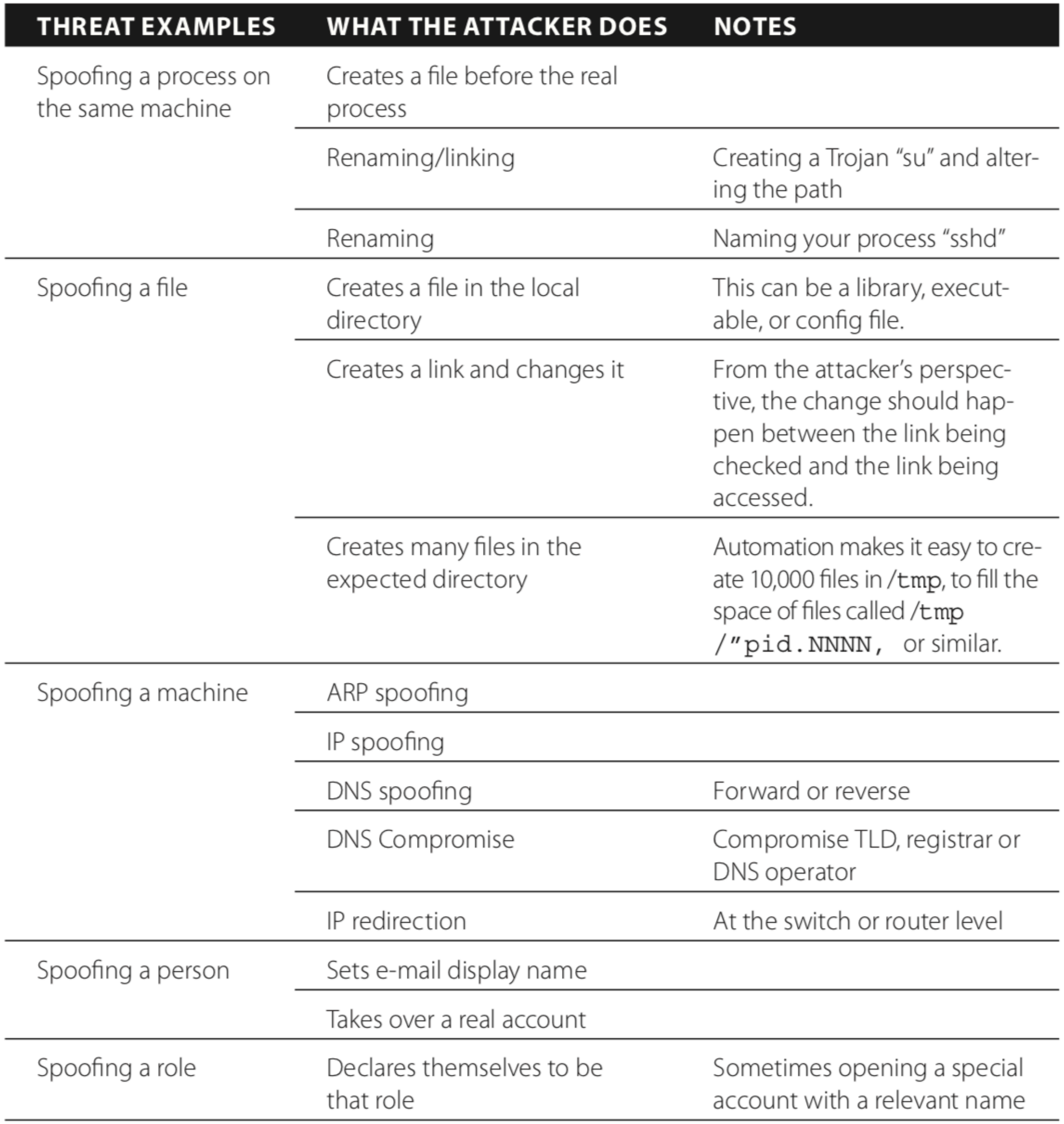
- Denial of Service - DoS
  - Absorbing resources needed to provide a service
  - Property violated: Availability
  - Typical victims: processes; data stores; data flows
  - Examples
    - a process that fills up the disk
    - massive requests to a DNS

STRIDE

- Elevation of Privilege - EoP
  - Allowing an entity to do something it’s not authorised to do
  - Property violated: Authorisation
  - Typical victims: processes
  - Examples
    - a normal user executing code as admin
    - allowing a remote person without any privileges to run code

STRIDE

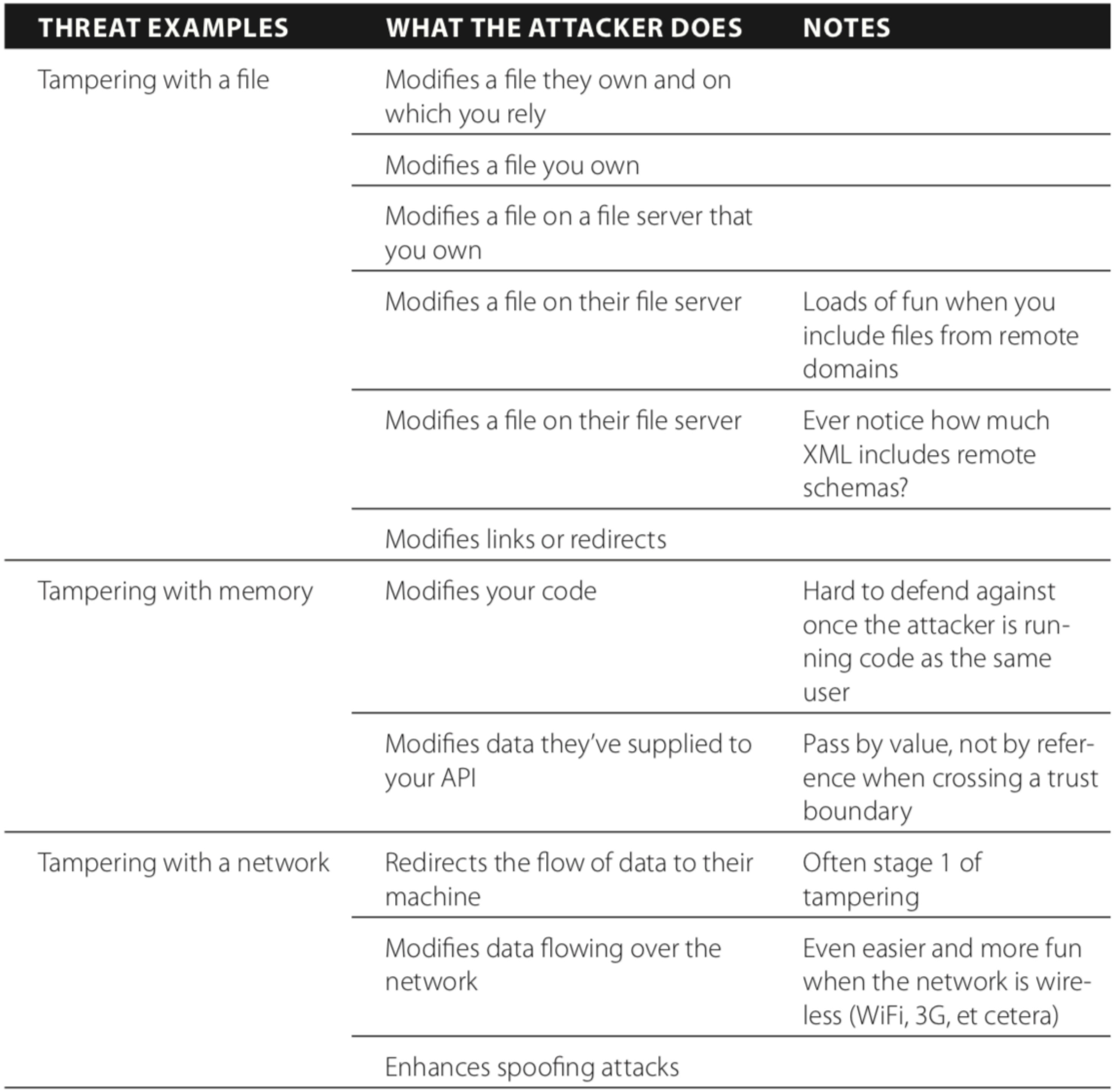
- A more detailed view - Spoofing threats



THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Spoofing a process on the same machine	Creates a file before the real process	
	Renaming/linking	Creating a Trojan "su" and altering the path
	Renaming	Naming your process "sshd"
Spoofing a file	Creates a file in the local directory	This can be a library, executable, or config file.
	Creates a link and changes it	From the attacker's perspective, the change should happen between the link being checked and the link being accessed.
	Creates many files in the expected directory	Automation makes it easy to create 10,000 files in `/tmp`, to fill the space of files called `/tmp /"pid.NNNN,` or similar.
Spoofing a machine	ARP spoofing	
	IP spoofing	
	DNS spoofing	Forward or reverse
	DNS Compromise	Compromise TLD, registrar or DNS operator
	IP redirection	At the switch or router level
Spoofing a person	Sets e-mail display name	
	Takes over a real account	
Spoofing a role	Declares themselves to be that role	Sometimes opening a special account with a relevant name

STRIDE

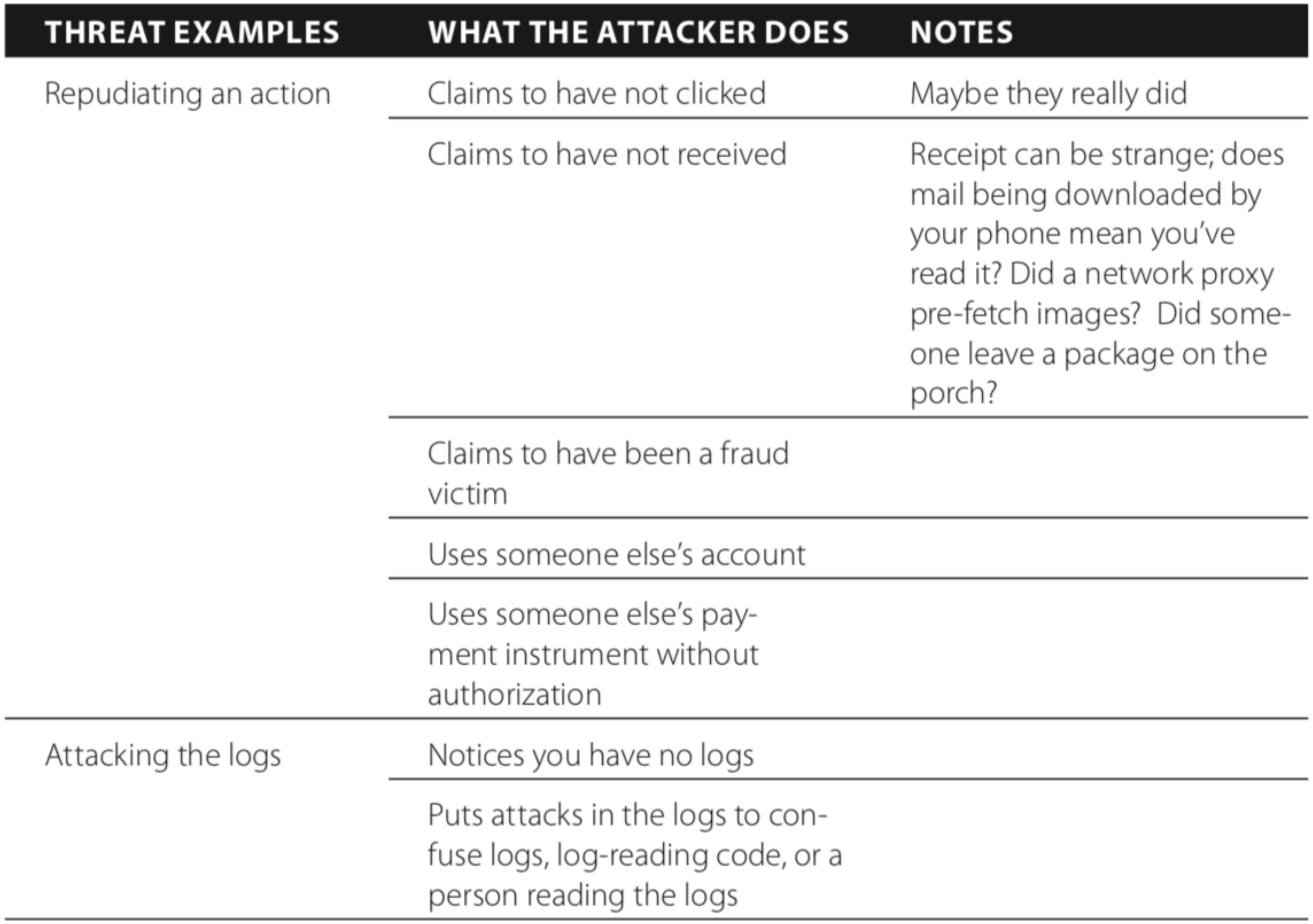
- A more detailed view - Tampering threats



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	
	Modifies a file on their file server	Loads of fun when you include files from remote domains
	Modifies a file on their file server	Ever notice how much XML includes remote schemas?
	Modifies links or redirects	
Tampering with memory	Modifies your code	Hard to defend against once the attacker is running code as the same user
	Modifies data they've supplied to your API	Pass by value, not by reference when crossing a trust boundary
Tampering with a network	Redirects the flow of data to their machine	Often stage 1 of tampering
	Modifies data flowing over the network	Even easier and more fun when the network is wireless (WiFi, 3G, et cetera)
	Enhances spoofing attacks	

STRIDE

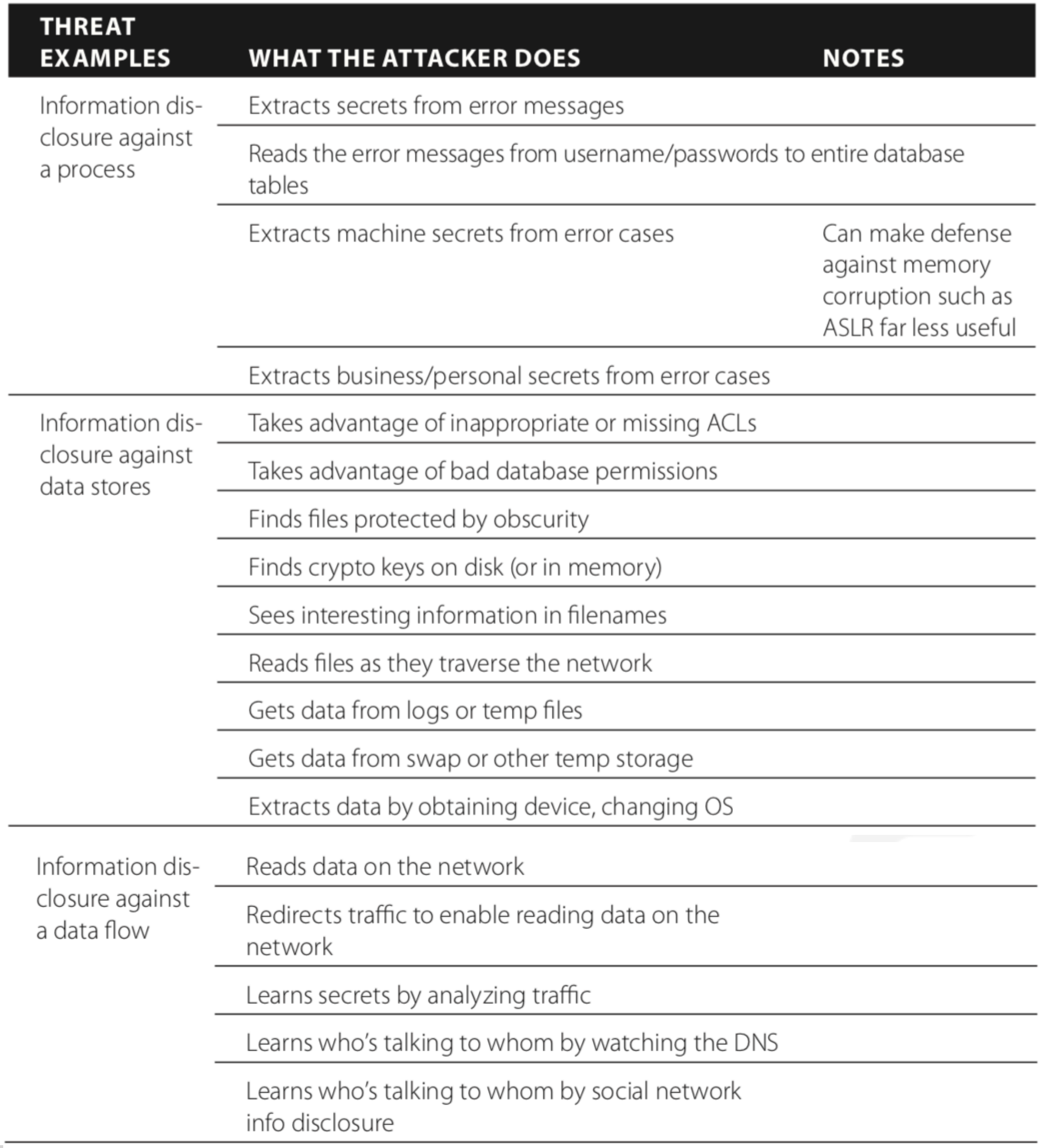
- A more detailed view - Repudiation threats



THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Repudiating an action	Claims to have not clicked	Maybe they really did
	Claims to have not received	Receipt can be strange; does mail being downloaded by your phone mean you've read it? Did a network proxy pre-fetch images? Did someone leave a package on the porch?
	Claims to have been a fraud victim	
	Uses someone else's account	
	Uses someone else's payment instrument without authorization	
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	

STRIDE

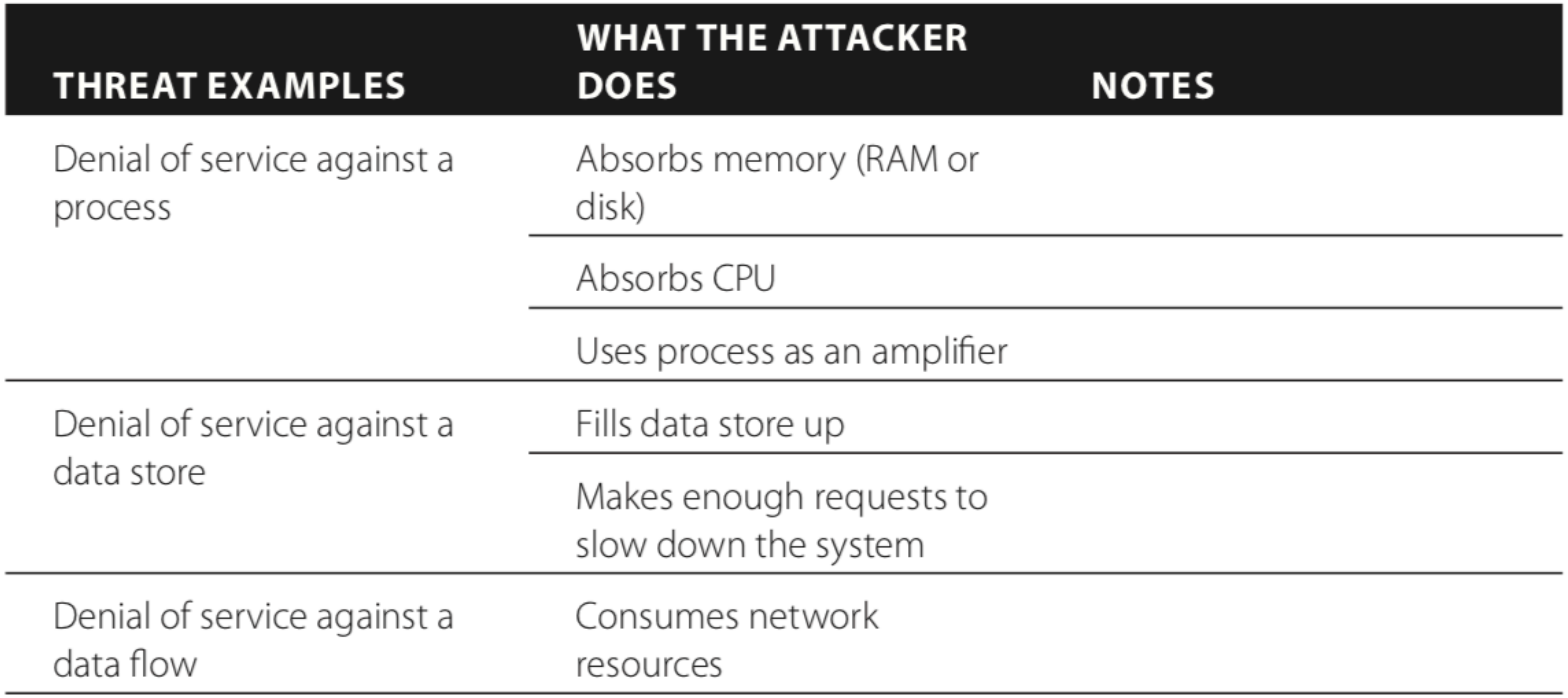
- A more detailed view - Information disclosure threats



THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Information disclosure against a process	Extracts secrets from error messages	
	Reads the error messages from username/passwords to entire database tables	
	Extracts machine secrets from error cases	Can make defense against memory corruption such as ASLR far 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 files protected by obscurity	
	Finds crypto keys on disk (or in memory)	
	Sees interesting information in filenames	
	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, 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 analyzing traffic	
	Learns who's talking to whom by watching the DNS	
	Learns who's talking to whom by social network info disclosure	

STRIDE

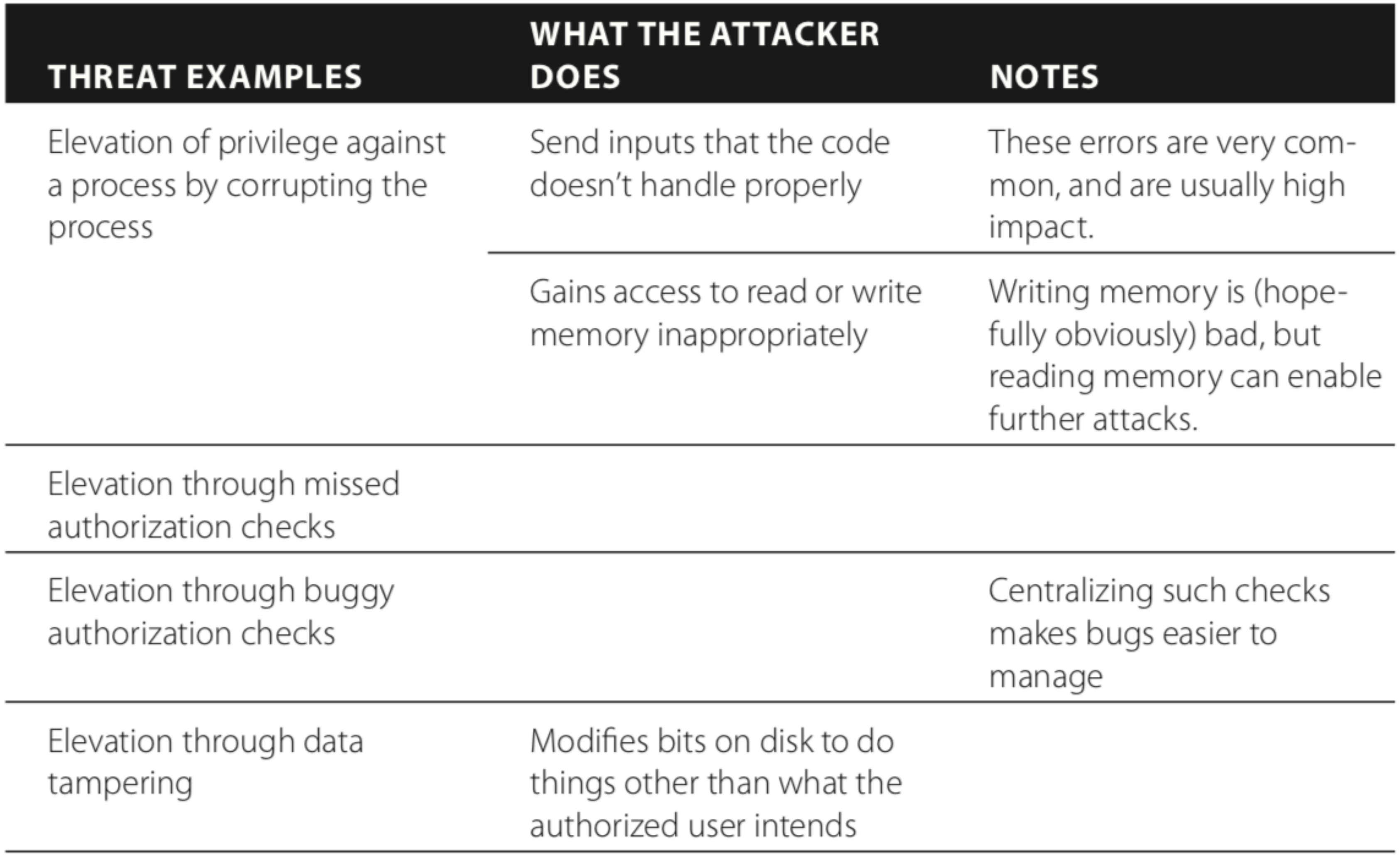
- A more detailed view - Denial-of-Service threats



THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Denial of service against a process	Absorbs memory (RAM or disk)	
	Absorbs CPU	
	Uses process as an amplifier	
Denial of service against a data store	Fills data store up	
	Makes enough requests to slow down the system	
Denial of service against a data flow	Consumes network resources	

STRIDE

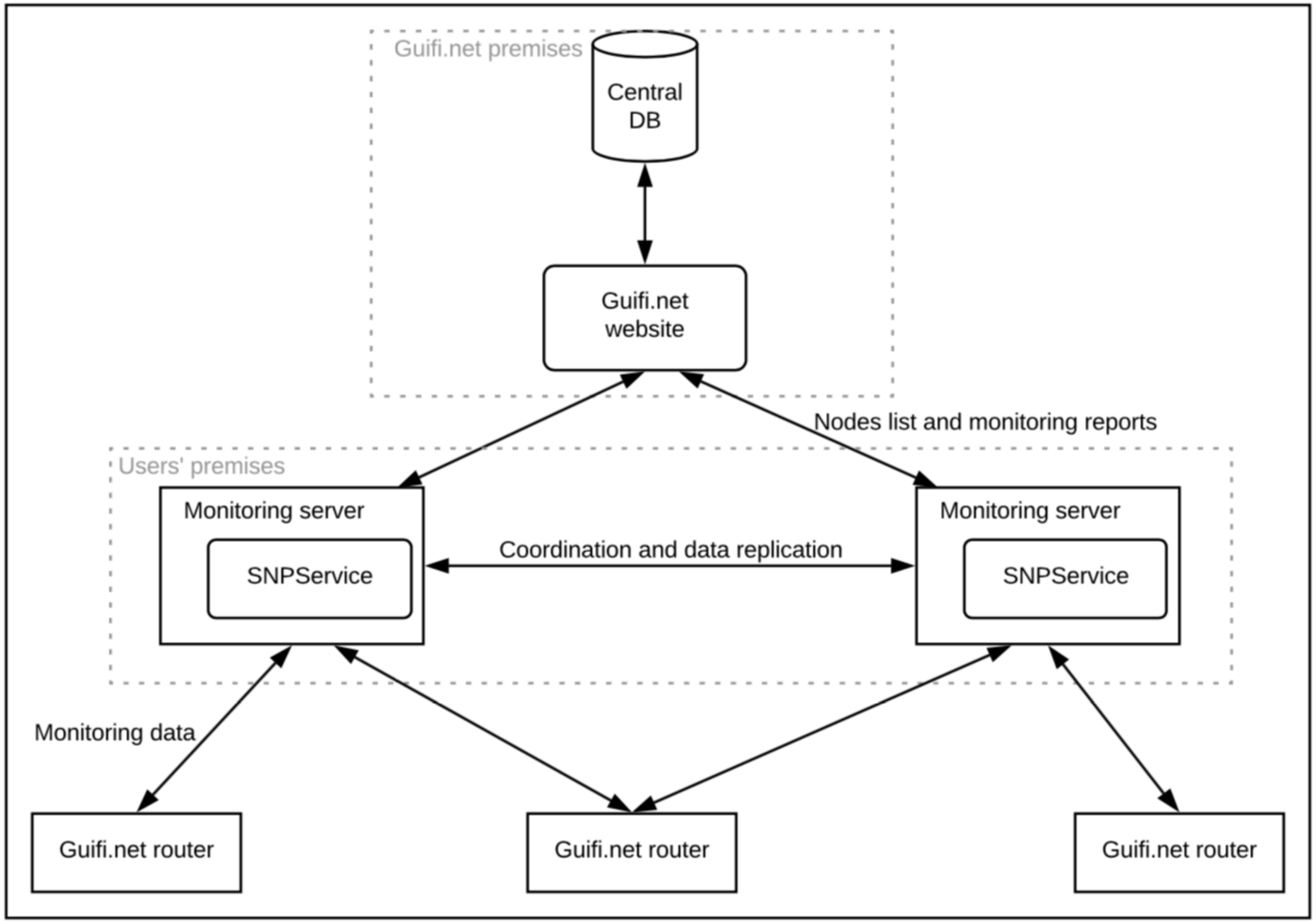
- A more detailed view - Elevation of Privilege threats



THREAT EXAMPLES	WHAT THE ATTACKER DOES	NOTES
Elevation of privilege against a process by corrupting the process	Send inputs that the code doesn't handle properly	These errors are very common, and are usually high impact.
	Gains access to read or write memory inappropriately	Writing memory is (hopefully obviously) bad, but reading memory can enable further attacks.
Elevation through missed authorization checks		
Elevation through buggy authorization checks		Centralizing such checks makes bugs easier to manage
Elevation through data tampering	Modifies bits on disk to do things other than what the authorized user intends	

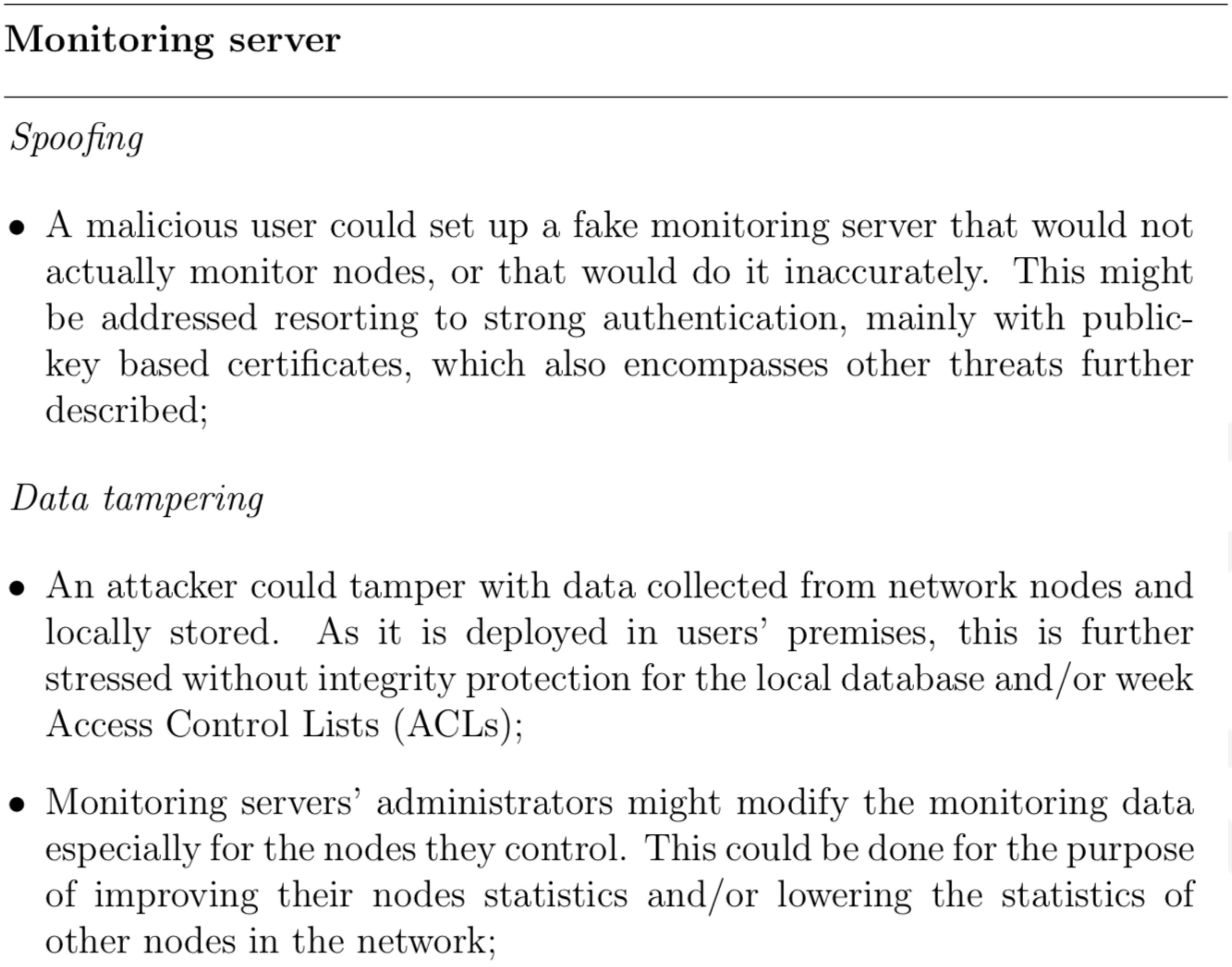
Example

- STRIDE-per-Element



DFD - Distributed network management system

Example



Monitoring server

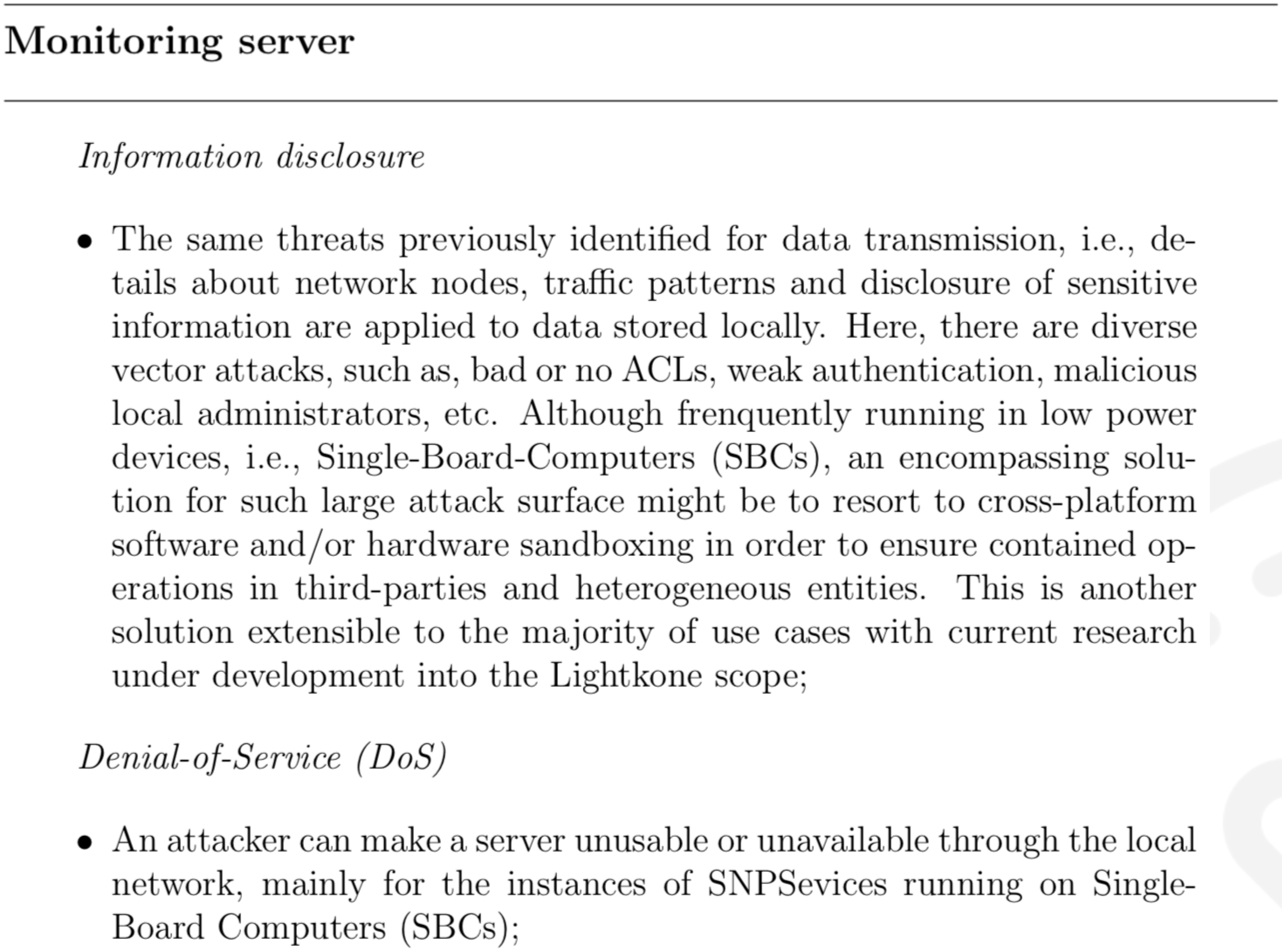
Spoofing

- A malicious user could set up a fake monitoring server that would not actually monitor nodes, or that would do it inaccurately. This might be addressed resorting to strong authentication, mainly with public-key based certificates, which also encompasses other threats further described;

Data tampering

- An attacker could tamper with data collected from network nodes and locally stored. As it is deployed in users' premises, this is further stressed without integrity protection for the local database and/or week Access Control Lists (ACLs);
- Monitoring servers' administrators might modify the monitoring data especially for the nodes they control. This could be done for the purpose of improving their nodes statistics and/or lowering the statistics of other nodes in the network;

Example



Monitoring server

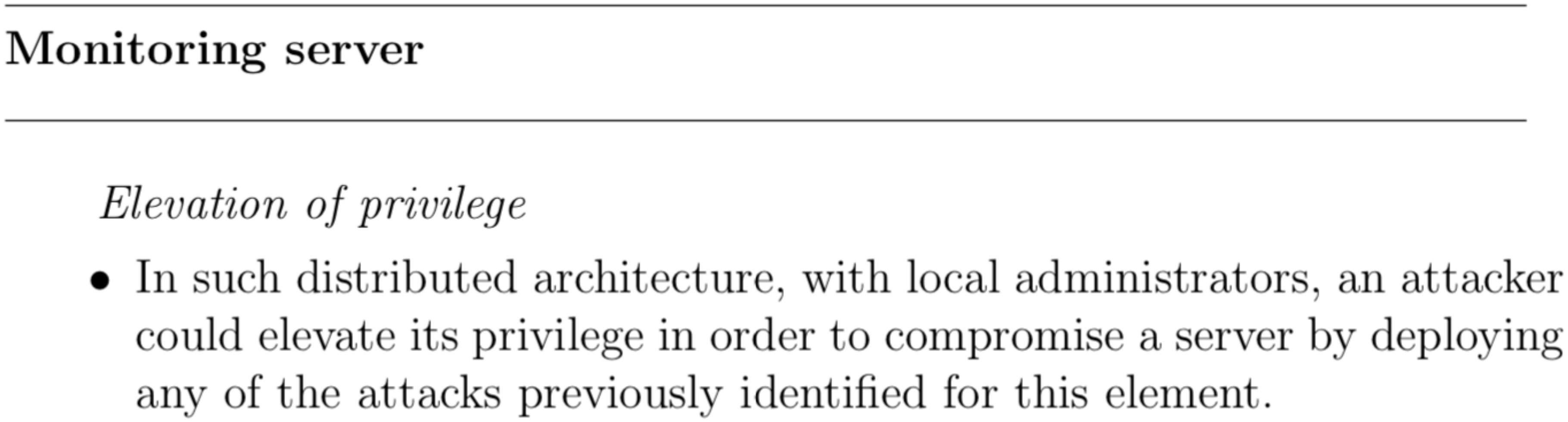
Information disclosure

- The same threats previously identified for data transmission, i.e., details about network nodes, traffic patterns and disclosure of sensitive information are applied to data stored locally. Here, there are diverse vector attacks, such as, bad or no ACLs, weak authentication, malicious local administrators, etc. Although frenquently running in low power devices, i.e., Single-Board-Computers (SBCs), an encompassing solution for such large attack surface might be to resort to cross-platform software and/or hardware sandboxing in order to ensure contained operations in third-parties and heterogeneous entities. This is another solution extensible to the majority of use cases with current research under development into the Lightkone scope;

Denial-of-Service (DoS)

- An attacker can make a server unusable or unavailable through the local network, mainly for the instances of SNPSevices running on Single-Board Computers (SBCs);

Example

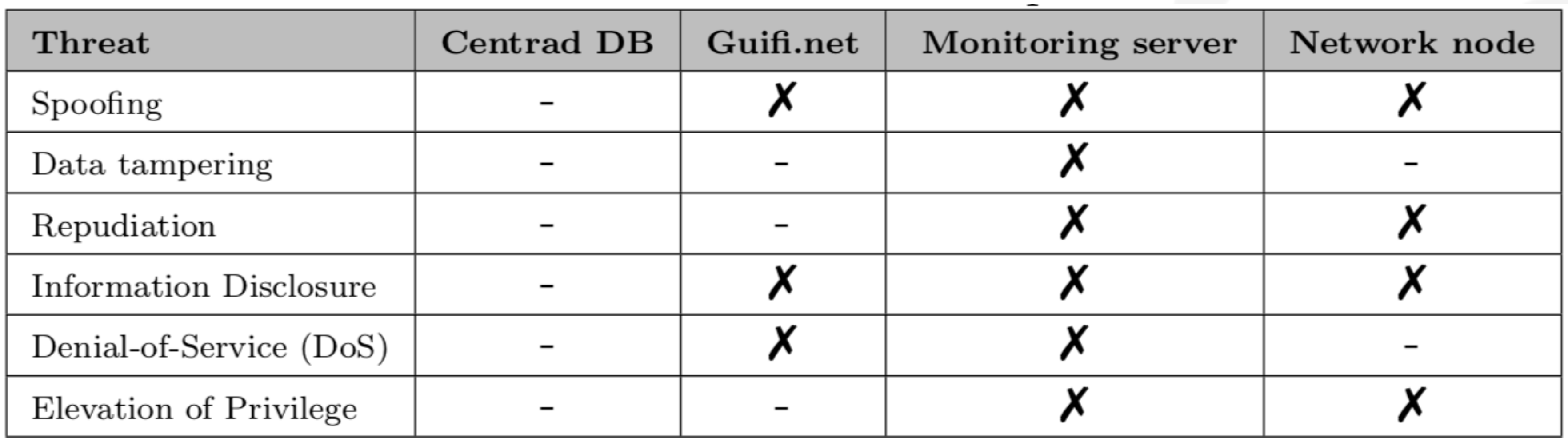


Monitoring server

Elevation of privilege

- In such distributed architecture, with local administrators, an attacker could elevate its privilege in order to compromise a server by deploying any of the attacks previously identified for this element.

Summary of threats



Threat	Centrad DB	Guifi.net	Monitoring server	Network node
Spoofing	-	✗	✗	✗
Data tampering	-	-	✗	-
Repudiation	-	-	✗	✗
Information Disclosure	-	✗	✗	✗
Denial-of-Service (DoS)	-	✗	✗	-
Elevation of Privilege	-	-	✗	✗

Hands on

- See BlackBoard - Ficha de exercício 02