STRIDE

Adversarial Behaviours

STRIDE

Adversarial Behaviours

- **Framework** for thinking, discussing and classify threats developed by Kohnfelder and Garg at Microsoft.
- Designed with the aim of getting software developers to **consider common threats**.
- STRIDE is designed to largely be a resource to support software development. The approach can be considered an **elicitation** technique of the perceived threats, rather than specific discovery.
- STRIDE is **not a modelling technique** and would not be used to understand the **anatomy of a cyber attack**.

STRIDE

Adversarial Behaviours

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

STRIDE

Adversarial Behaviours

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privileges

STRIDE

Adversarial Behaviours

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

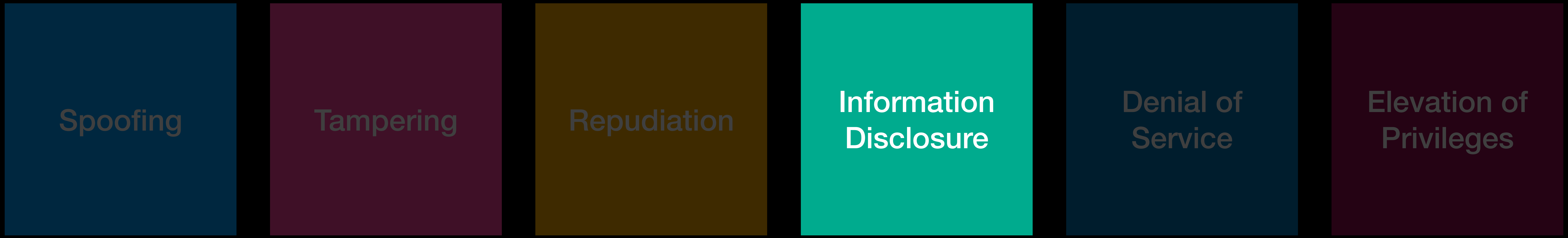
STRIDE

Adversarial Behaviours

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

STRIDE

Adversarial Behaviours



Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privileges

STRIDE

Adversarial Behaviours

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- **Denial of Service**
- Elevation of Privileges

STRIDE

Adversarial Behaviours

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

STRIDE

Adversarial Behaviours

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privileges

STRIDE

Adversarial Behaviours

Spoofing

STRIDE

- Spoofing refers to the concept of masquerading as something itself.
- An attacker could pretend to a process, file, machine or another person.
- Consider a website that masquerades or pretends to be an official website.
- Consider a social engineering phone call pretending to be an official or organisation.

Spoofing

Tampering

STRIDE

- Tampering can be consider an attack that modifies some data.
- Modification could occur on the cyber system, both on disk or memory, as well as over the network.

Tampering

STRIDE

- Attacker could add additional nefarious packets to the network rather than alter existing ones.
- Recall, many designs may start from just getting things working rather than what is optimal in terms of security.

Tampering

Repudiation

STRIDE

- Repudiation refers to rejection of responsibility of actions.
- An interesting aspect of STRIDE as it more an enterprise issue, than a technology issue.

Repudiation

Repudiation

STRIDE

- Non-repudiation is crucial to ensure another entity or individual cannot reject responsibility.
- Transactions and actions require confidence between both parties.

Repudiation

Information Disclosure

STRIDE

- Information disclosure means that information was consumed or revealed to unauthorised parties.
- Essentially meaning that an individual or entity was not meant or should not have access to the information.

Information Disclosure

Information Disclosure

STRIDE

- Can consider this from very small to very large information disclosure.
- An error message revealing structure of system or even recovery implementations.

Information Disclosure

Denial of Service

STRIDE

- Denial of service attacks effectively consume resources to the detriment to others.
- Such attacks can be considered active or persistent attacks.
- Denial of service attacks can also be considered in terms of amplification.

Denial of Service

Elevation of Privileges

STRIDE

- Elevation of privileges is an entity executing at level that is not permitted.
- Consider an entry-level individual executing processes on a cyber system restricted to administrators.
- An external entity with no privileges executing processes remotely on cyber systems.

Elevation of Privileges

Elevation of Privileges

STRIDE

- Horizontal escalation refers to accessing function available to other users on the same tier.
- Name misleading, but essentially stealing username/password access similar functions.
- Vertical escalation refers to accessing functions that are the preserve of entity with different privileges.

Elevation of Privileges

STRIDE

Adversarial Behaviours

Spoofing

Tampering

Repudiation

Information Disclosure

Denial of Service

Elevation of Privileges

STRIDE

Adversarial Behaviours

- STRIDE is **not a modelling technique** and would not be used to formulate the **anatomy of a cyber attack**.
- STRIDE is designed to largely be a resource to support software development. The approach can be considered an **elicitation** technique of the perceived threats, rather than specific discovery.
- Using STRIDE to model or formulate understanding of campaigns or complex attacks may actually result in ignoring aspects of the attack.

STRIDE

Adversarial Behaviours