Threat Modeling

A Primer

Disclaimer

This Presentation describes a simplified version of Threat Modeling

References

- OWASP Threat Modeling Cheat Sheet
- OWASP Attack Surface Analysis Cheat Sheet
- Wikipedia Information Security
- Wikipedia STRIDE
- MSDN STRIDE

Information Security

The **CIA Triad** of security attributes/goals.

- **Confidentiality**
  An Information must not be available or be disclosed to unauthorized individuals, entities or processes.
- **Integrity**
  Accuracy and completeness of an information must be assured over its lifetime.
- **Availability**
  An Information must be avaiblabe when needed.

More Information Security

Secondary/derived security attributes/goals

- **Authenticity**
  Correctness/Trustworthiness can be verified*.
- **Non Repudiation**
  Operations cannot be denied by any party.
- **Accountability**
  Operators can be clearly identified.
- **Anonymity**
  Operators cannot be identified.

FYI: The term **Verification implies provability, this demands more than just a simple review which would be just **Validation**.*

Even More Informatin Security

GDPR (DSGVO) security attributes/goals

- **Resilience**
  Robustness against surveillance and sabotage.

More or less a combination of all others because... EU lawyers, i guess...

STRIDE

A model of threats developed by Praerit Garg and Loren Kohnfelder at Microsoft.

	Threat	Security Goal
S	Spoofing Identities	Authenticity
T	Tampering with Data	Integrity
R	Repudiation	Non-Repudiation
I	Information Disclosure	Confidiality
D	Dinial of Service	Availability
E	Elevation of Privilege	Confidiality, Integrity, Availability

STRIDE Threats

	Threat	Short Definition
S	Spoofing Identities	Successfully identify with another identity.
T	Tampering with Data	Intentional modification of data.
R	Repudiation	Sucessfully deny performing an action.
I	Information Disclosure	Disclosure of information to unauthorized parties.
D	Dinial of Service	Prevent legitimate use of a service/resource.
E	Elevation of Privilege	Gain elevated access to otherwise protected resources.

Spoofing Identities

- Successfully identify with another identity.

Example

TODO

Tampering with Data

- Intentional modification of data.

Example

TODO

Repudiation

- Sucessfully deny performing an action.

Example

TODO

Information Disclosure

- Disclosure of information to unauthorized parties.

Example

TODO

Dinial of Service

- Prevent legitimate use of a service/resource.

Example

TODO

Elevation of Privilege

- Gain elevated access to otherwise protected resources.

Example

TODO

Example

Thanks!