Threat Modeling

MODIO
Secure & efficient energy information

What are you protecting?

MODIO
Secure & efficient energy information

What are you protecting?

Assets

- Personal data
- CC numbers

Treat User Data as Toxic Waste

https://www.schneier.com/blog/archives/2008/01/data_as_polluti.html

MODIO
Secure & efficient energy information

What are you protecting?

Systems:

- Machines
- Services
- Protocols

MODIO
Secure & efficient energy information

Against what?

Against what?

- Brownout
- Datacenter fire
- Hard drive loss
- Forgotten laptop
- Malicious actor

More examples?

Building a model

What are the requirements

(What should it do)

Necessary access

Users, roles,

Data and its flow

Use cases

Combines data + user

MODIO
Secure & efficient energy information

Architecture

The Components

Architecture

Different services (And elevation levels)

MODIO
Secure & efficient energy information

Architecture

External dependencies

S.T.R.I.D.E.

MODIO
Secure & efficient energy information

S.T.R.I.D.E.

Spoofing (Identity, data)

MODIO
Secure & efficient energy information

S.T.R.I.D.E.

Tampering

(Data, Code)

MODIO
Secure & efficient energy information

S.T.R.I.D.E.

Repudiation

MODIO
Secure & efficient energy information

S.T.R.I.D.E.

Information Disclosure

MODIO
Secure & efficient energy information

S.T.R.I.D.E.

Denial of Service

S.T.R.I.D.E.

Elevation of Privilege

MODIO
Secure & efficient energy information

And then?

Look at the edges and borders

Identify risks

Countermeasures

Resources: Wikipedia

https://en.wikipedia.org/wiki/Threat_model

Resources: OWASP

https://www.owasp.org/index.php/Application_Threat_Modeling

Resources: SDL

http://www.microsoft.com/en-us/download/details.aspx?id=29884