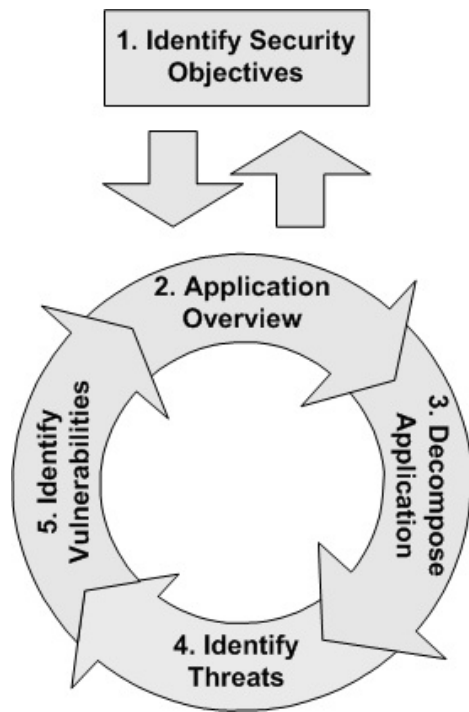


Threat Model Concepts



Vocabulary

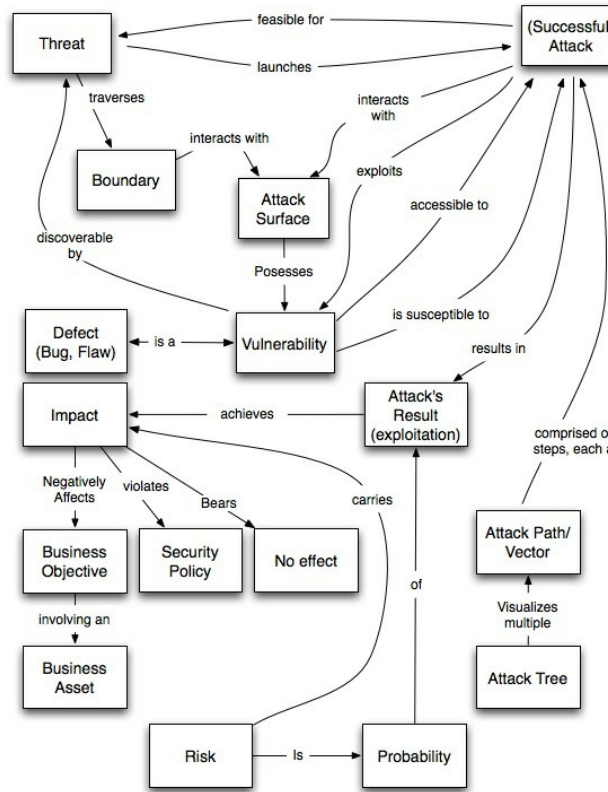


Image from <https://www.cigital.com/blog/threat-modeling-vocabulary/>

DFD Elements

External Entity

The external entity shape is used to represent any entity outside the application that interacts with the application via an entry point

Process

Represents a task that handles data within the application. The task may process the data or perform an action based on the

Multiple Process

Used to present a collection of subprocesses. The multiple process can be broken down into its subprocesses in another DFD.

Data Store

Represents locations where data is stored

Data Flow

Represents data movement within the application. The direction of the data movement is represented by the arrow.

Privilege Boundary

Represent the change of privilege levels as the data flows through the application.

Data Classification

Data Classification Wizard
Business Data Examples

HBI ☒ MBI ☐ LBI ☐ Public ☐ MY SELECTIONS

Non-User Data	Supplier or Vendor Management Data	Keys and Certificates
Personal User Data	Bank Account Numbers	Hardware or Software Tokens
Account ID	Receipts and Payment Data	Private Cryptographic Keys
Address	Sales Account Data	Product Keys (Individual)
Age	Documentation	Public Cryptographic Keys
Biometric Markers	Current Systems Configuration Data	Employee Data
Complete Geo-Location Tracking Data	Data or Software File Shares	Personal Employment Data
Credit Card and Transaction Information	Design and Functional Specifications	Sensitive Personal Employment Data
Customization Information	Future or Active Processes or Procedures	
DNA Sequences and Samples	Future or Active Sales and Marketing Plans	
Email Address	Operating Procedures or Manuals	
Facial Recognition Patterns		

image from <https://www.microsoft.com/security/data/>

STRIDE

Threat	Description	Breaks
Spoofting	Pretending to be somebody else	Authentication
Tampering	Modifying data that should not be modifiable	Integrity
Repudiation	Claiming someone didn't do something	Non-Repudiation
Information Disclosure	Exposing information	Confidentiality
Denial of Service	Preventing a system from providing service	Availability
Elevation of Privilege	Doing things that one isn't supposed to do	Authorization