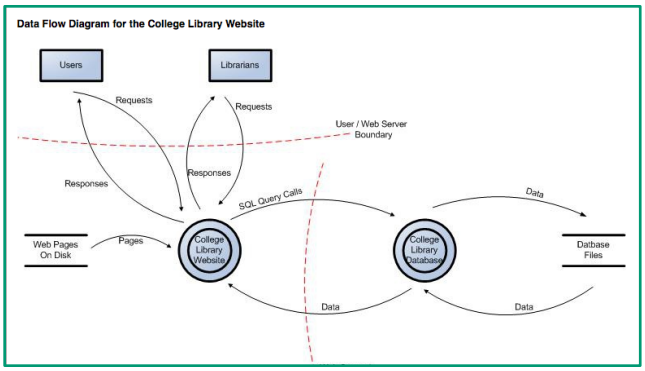
Threat Modeling



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

Laurie Williams
laurie_williams@ncsu.edu

Slides adapted from John Slankas, MS Threat Modeling, Adam Shostack's "Threat Modeling"

Computer Science
NC STATE UNIVERSITY

What is a threat? A threat model?

- Threat = potential event that will have an unwelcome consequence
- Threat model = model you employ to address or mitigate potential threats

Computer Science
NC STATE UNIVERSITY

What is software security threat modeling?

- Set of techniques aimed at identifying threats to a system based upon how it is architected and how it supposed to behave
- Process of decomposing a system architecture:
  - Key structural elements
  - Assets
  - Attack surface
  - Data and control flow
  - Security mechanisms
  - Trust boundaries

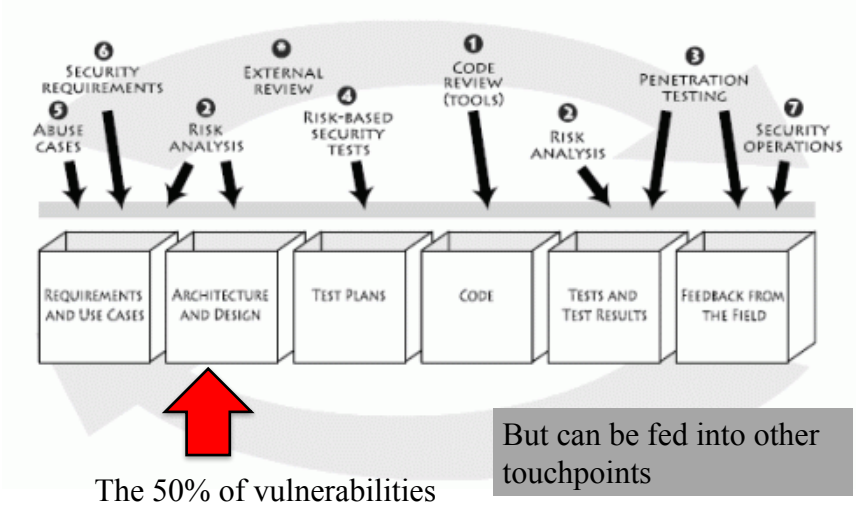
Computer Science
NC STATE UNIVERSITY

Who

- Building a threat model
  - Program Manager (PM) owns overall process
  - Testers
    - Identify threats in analyze phase
    - Use threat models to drive test plans
  - Developers create diagrams
  - Business analysts
- Customers for threat models
  - Your team
  - Other features, product teams
  - Customers, via user education
  - "External" quality assurance resources, such as pen testers
- You'll need to decide what fits to your organization

Computer Science
NC STATE UNIVERSITY

When: Security Touchpoints



The 50% of vulnerabilities related to design flaws

But can be fed into other touchpoints

http://www.cigital.com/justiceleague/wp-content/uploads/2007/07/touchpoints.gif

Computer Science NC STATE UNIVERSITY

Why

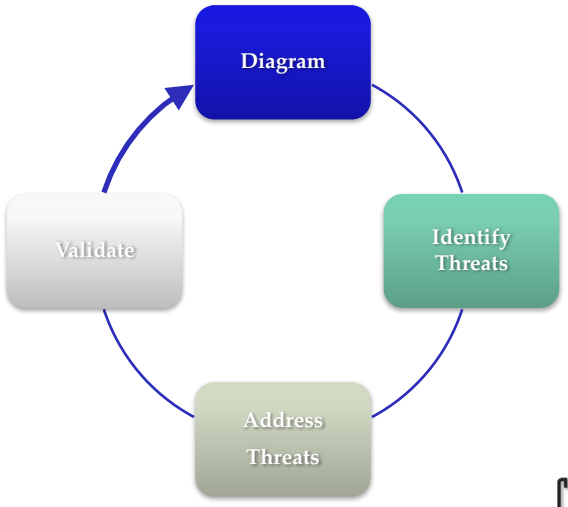
- Produce software that's secure by design
  - Improve designs the same way we've improved code
- Because attackers think differently
  - Creator blindness/new perspective
- Allow you to predictably and effectively find security problems early in the process
- Understand your security requirements

Computer Science NC STATE UNIVERSITY

How?

Computer Science
NC STATE UNIVERSITY

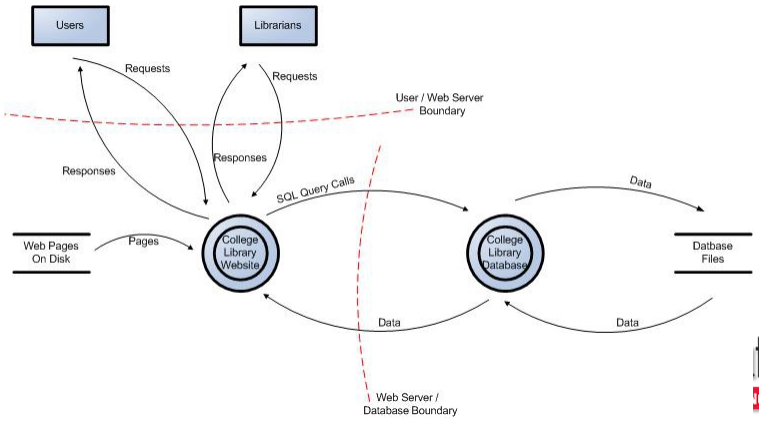
The Process



Computer Science
NC STATE UNIVERSITY

Diagram

- Sketch high level view of system
- Most commonly a Data Flow Diagram (DFD)
  - Sketching DFD ➔ Understand the system
  - Analyzing DFD ➔ Understand the threats



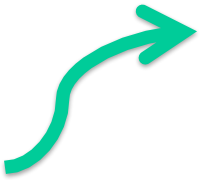
Data Flow Diagram (DFD): Symbols

External Entity / Interactor

Process

Data store

Trust boundary



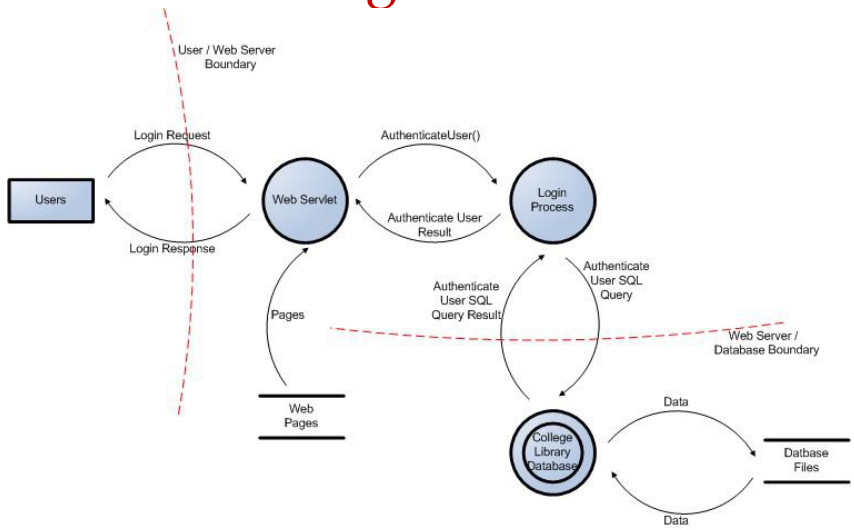
Data flow

DFD Elements: Examples

External Entity	People, other systems
Process	DLLS, Components, Services, Web Services
Data Flow	Function call, Network traffic, Remote procedure call
Data Store	Database, file, registry, shared memory, queue
Trust Boundary	Process boundary, file system, system boundary

Computer Science
NC STATE UNIVERSITY

Data Flow Diagram – Detailed

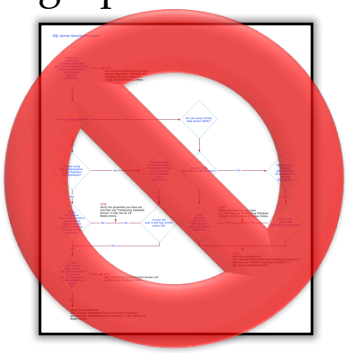


https://www.owasp.org/index.php/Application_Threat_Modeling

Computer Science
NC STATE UNIVERSITY

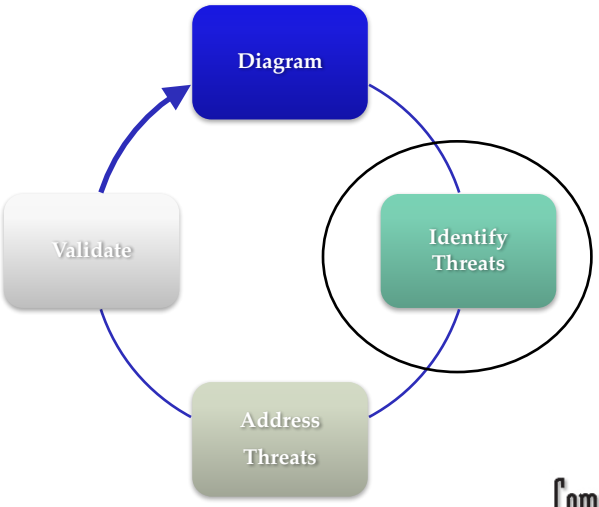
Diagrams Should Not Resemble

- Flow charts
- Class diagrams
- Call graphs



Computer Science
NC STATE UNIVERSITY

The Process: Identify Threats



Computer Science
NC STATE UNIVERSITY

Identify Threats

- Use a systematic approach to identify the application exposure to threats

  1. Analyze DFD via (Microsoft's) STRIDE
  2. Abuse and misuse cases
  3. Attack trees
  4. Attack libraries, common vulnerabilites (implementation bugs & design flaws)
  5. Elevation of Privilege game
  6. ~~Unstructured Brainstorm~~

- Outcome: List of threats relevant to the application environment, the hosts, and the application tiers

Computer Science
NC STATE UNIVERSITY

(Microsoft) STRIDE

Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Computer Science
NC STATE UNIVERSITY

Threat: Spoofing

Threat	Spoofing
Property	Authentication
Definition	Impersonating something or someone else
Example	Pretending to be any of billg, microsoft.com, or ntdll.dll

Computer Science
NC STATE UNIVERSITY

Threat: Tampering

Threat	Tampering
Property	Integrity
Definition	Modifying data or code
Example	Modifying a DLL on disk or DVD, or a packet as it traverses the LAN

Computer Science
NC STATE UNIVERSITY

Threat: Repudiation

Threat	Repudiation
Property	Non-Repudiation
Definition	Claiming to have not performed an action
Example	"I didn't send that email," "I didn't modify that file," "I certainly didn't visit that Web site, dear!"

Computer Science
NC STATE UNIVERSITY

Threat: Information Disclosure

Threat	Information Disclosure
Property	Confidentiality
Definition	Exposing information to someone not authorized to see it
Example	Allowing someone to read the Windows source code; publishing a list of customers to a Web site

Computer Science
NC STATE UNIVERSITY

Threat: Denial of Service

Threat	Denial of Service
Property	Availability
Definition	Deny or degrade service to users
Example	Crashing Windows or a Web site, sending a packet and absorbing seconds of CPU time, or routing packets into a black hole

Computer Science
NC STATE UNIVERSITY

Threat: Elevation of Privilege

Threat	Elevation of Privilege (EoP)
Property	Authorization
Definition	Gain capabilities without proper authorization
Example	Allowing a remote Internet user to run commands is the classic example, but going from a “Limited User” to “Admin” is also EoP

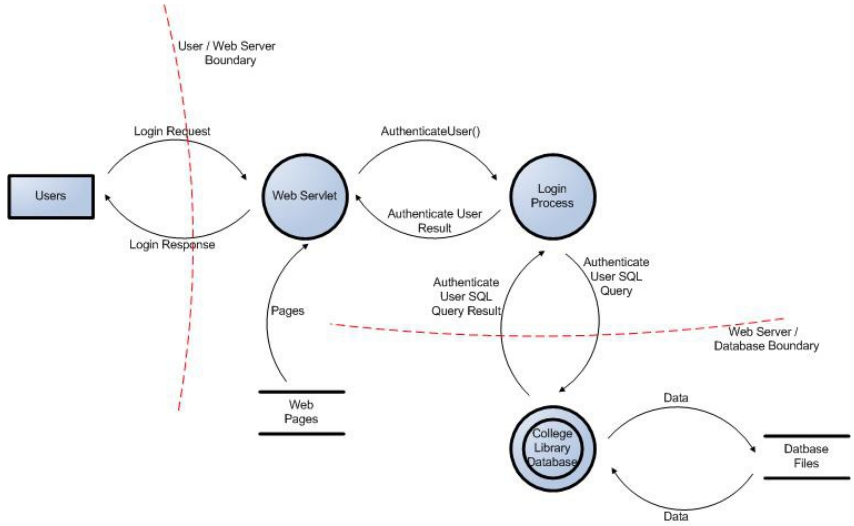
Computer Science
NC STATE UNIVERSITY

Different Threats Affect Each Element Type

ELEMENT	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store		✓	?	✓	✓	
Data Flow		✓		✓	✓	

Computer Science
NC STATE UNIVERSITY

What STRIDE Threats Exist?



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

Computer Science
NC STATE UNIVERSITY

Use the Trust boundaries

- Trusted/ high code reading from untrusted/low
  - Validate everything for specific and defined uses
- High code writing to low
  - Make sure your errors don't give away too much

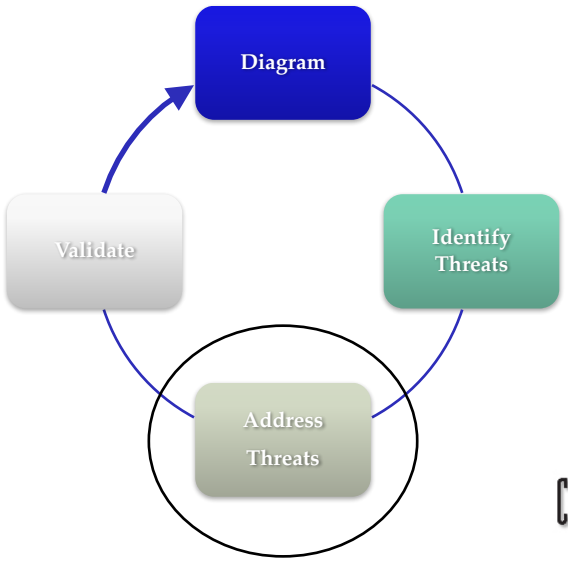
Computer Science
NC STATE UNIVERSITY

STRIDE: Review

Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Computer Science
NC STATE UNIVERSITY

The Process: Address Threats



Computer Science
NC STATE UNIVERSITY

Addressing Threats is the Point of Threat Modeling

- Protect customers
- Design secure software
- Why bother if you:
  - Create a great model
  - Identify lots of threats
  - Stop
- So, find problems and fix them

Computer Science
NC STATE UNIVERSITY

Address Threats: META

For each threat,

- Mitigate

  What have similar software packages done and how has that worked out for them?

- Eliminate

  Redesign

- Transfer

  Another part of the system or entity

- Accept

- "wait and see"

Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Spoofing	Authentication	To authenticate principals: • Basic authentication • Digest authentication • Cookie authentication • Windows authentication (NTLM) • Kerberos authentication • PKI systems, such as SSL or TLS and certificates • IPSec • Digitally signed packets To authenticate code or data: • Digital signatures • Message authentication codes • Hashes

Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Tampering	Integrity	• Windows Vista mandatory integrity controls • ACLs • Digital signatures • Message authentication codes

Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Repudiation	Nonrepudiation	• Strong authentication • Secure logging and auditing • Digital signatures • Secure time stamps • Trusted third parties

Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Information Disclosure	Confidentiality	• Encryption • Access Control Lists (ACLs)

Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Denial of Service	Availability	• ACLs • Filtering • Quotas • Authorization • High-availability designs

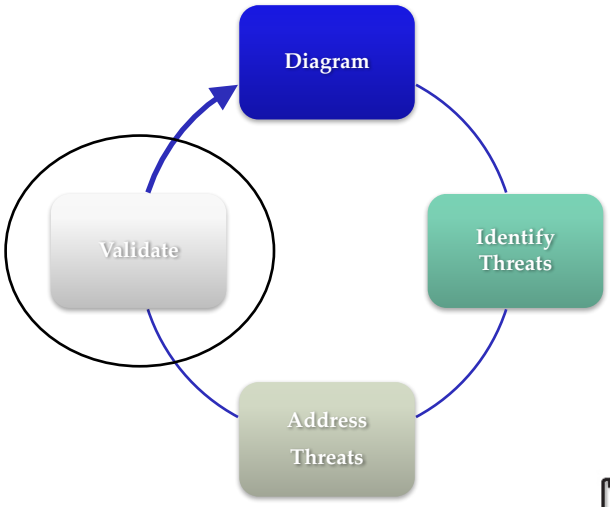
Computer Science
NC STATE UNIVERSITY

STRIDE: Standard Mitigations

Threat	Property	
Elevation of Privilege	Authorization	• ACLs • Group or role membership • Privilege ownership • Permissions • Input validation • Least Privilege

Computer Science
NC STATE UNIVERSITY

The Process: Validate



Computer Science
NC STATE UNIVERSITY

Validate DFDs

1. Can we tell a story without changing the diagram?
2. Can we tell that story without using words such as "sometimes" or "also"?
3. Can we look at the diagram and see exactly where the software will make a security decision?
4. Does the diagram show all the trust boundaries, such as where different accounts interact? Do you cover all user roles, all application roles, and all network interfaces?
5. Does the diagram reflect the current or planned reality of the software?
6. Can we see where all the data goes and who uses it?
7. Do we see the processes that move data from one data store to another?

Computer Science
NC STATE UNIVERSITY

Validate Threats

1. Have we looked for each of the STRIDE threats?
2. Have we looked at each element of the diagram?
3. Have we looked at each data flow in the diagram?
4. For each threat: Does it:
   - Describe the attack
   - Describe the context
   - Describe the impact

Computer Science
NC STATE UNIVERSITY

Validate "Addressing Threats"

- Is there a proposed/planned/implemented way to address each threat?
- Is the mitigation correctly implemented?
  - Test cases?
  - Software passed tests?

Computer Science
NC STATE UNIVERSITY

Validate Information Captured

- Dependencies
  - What other code are you using?
  - What security functions are in that other code?
  - Are you sure?
- Assumptions
  - Things you note as you build the threat model
    - "HTTP.sys will protect us against SQL Injection"
    - "LPC will protect us from malformed messages"
    - GenRandom will give us crypto-strong randomness

Computer Science
NC STATE UNIVERSITY

Summary

- Threat models helps you **find and proactively mitigate security design flaws before the system is built**
- Threat models help you understand your application better and find bugs.
- Threat models help new team members (and other teams) understand the application in detail.
- Threat models can be used by testers to plan test cases.

Computer Science
NC STATE UNIVERSITY

41