Web Application Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in

Threat Modelling

STRIDE

DREAD

Thread Modeling

- ✓ **Threat modeling** is an approach for analyzing the **security** of an application.
- ✓ It is a structured approach that enables you to
  - ✓ identify,
  - ✓ quantify,
  - ✓ and address the security risks associated with an application.
- ✓ Threat modeling **is not** an approach to
  - ✓ reviewing code,
  - ✓ but it does complement the security code review process.

Threat Modelling

- ✓ The inclusion of threat modeling in the **SDLC** can help to ensure that applications are being developed with **security built-in from** the very beginning.
- ✓ This, combined with the documentation produced as part of the threat modeling process, can give the reviewer a greater understanding of the system.
- ✓ This allows the reviewer to see where the entry points to the application are and the associated threats with each entry point.

Threat Modelling

- ✓ The concept of threat modeling is not new but there has been a **clear mindset change** in recent years.
- ✓ Modern threat modeling looks at a system from a potential attacker's perspective, as opposed to a defender's viewpoint.
- ✓ Microsoft have been strong advocates of the process over the past number of years, SDL (Security Development Life Cycle)

- ✓ They have made threat modeling a **core component** of their **SDLC**, which they claim to be one of the reasons for the increased security of their products in recent years.
- ✓ When source code analysis is performed outside the SDLC, such as on existing applications, the results of the threat modeling help in reducing the complexity of the source code analysis by promoting an **in-depth first approach vs. breadth first approach.**

- ✓ Instead of reviewing all source code with equal focus, you can prioritize the security code review of components whose threat modeling has
  - ✓ ranked with high risk threats.

Step 1: Decompose the Application.

- ✓ The threat modeling process can be decomposed into 3 high level steps:
- ✓ The first step in the threat modeling process is concerned with gaining an understanding of the application and how it interacts with external entities.
- ✓ This involves creating use-cases to understand
  - ✓ how the application is used,
  - ✓ identifying entry points to see where a potential attacker could interact with the application

Step 1: Decompose the Application.

- ✓ This involves creating use-cases to understand
  - ✓ identifying assets i.e. items/areas that the attacker would be interested in, and
  - ✓ identifying trust levels which represent the access rights that the application will grant to external entities.
- ✓ This information is documented in the Threat Model document and it is also used to produce data flow diagrams (DFDs) for the application. The DFDs show the different paths through the system, highlighting the privilege boundaries.

Step 2: Determine and rank threats.

- ✓ Critical to the identification of threats is using a threat categorization methodology.
- ✓ A threat categorization such as **STRIDE (See Next Slide)** can be used, or the **Application Security Frame (ASF)** that defines threat categories such as
  - ✓ Auditing & Logging,
  - ✓ Authentication, Authorization,
    - ✓ Authentication = login + password (who you are)
    - ✓ Authorization = permissions (what you are allowed to do)

Step 2: Determine and rank threats.

- ✓ Configuration Management,
- ✓ Data Protection in Storage and
- ✓ Transit, Data Validation,
- ✓ Exception Management.

✓ The goal of the threat categorization is to help identify threats both from the **attacker (STRIDE) and the defensive perspective (ASF).**

The STRIDE Threat Model

- ✓ When you are considering threats, it is useful to ask questions such as these:
  1. How can an attacker change the authentication data?
  2. What is the impact if an attacker can read the user profile data?
  3. What happens if access is denied to the user profile database?
- ✓ You can group threats into categories to help you formulate these kinds of pointed questions.

The STRIDE Threat Model

- ✓ One model you may find useful is STRIDE, derived from an acronym for the following six threat categories:
- ✓ **Spoofing identity.** An example of identity spoofing is **illegally accessing** and then using another user's authentication information, such as username and password.

The STRIDE Threat Model

- ✓ **Tampering with data.** Data tampering involves the **malicious modification of data**. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet.
- ✓ **Repudiation.** A repudiation attack happens when an application or system does not adopt controls to properly track and log users' actions, thus permitting malicious manipulation or forging the identification of new actions.

- ✓ **Repudiation.** This attack can be used to change the authoring information of actions executed by a malicious user in order to log wrong data to log files. Its usage can be extended to general data manipulation in the name of others, in a similar manner as spoofing mail messages. If this attack takes place, the data stored on log files can be considered invalid or misleading.

The STRIDE Threat Model

- ✓ Example of Repudiation, suppose a customer sends a letter to a vendor agreeing to pay a large amount of money for a product.
- ✓ The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unsolicited shipment without payment.
- ✓ The customer has repudiated the origin of the letter. If the vendor cannot prove that the letter came from the customer, the attack succeeds.
- ✓ A variant of this is denial by a user that he created specific information or entities such as files. Integrity mechanisms cope with this threat. (Email Spoofing)

- ✓ **Nonrepudiation** refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package.
- ✓ **Information disclosure.** Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers.

- ✓ **Denial of service. Denial** of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability.

- ✓ **Elevation of privilege.** In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed.

Threats and Mitigation Techniques

STRIDE Threat & Mitigation Techniques List	
Threat Type	**Mitigation Techniques**
Spoofing Identity	1. Appropriate authentication 2. Protect secret data 3. Don't store secrets
Tampering with data	1. Appropriate authorization 2. Hashes 3. MACs 4. Digital signatures 5. Tamper resistant protocols
Repudiation	1. Digital signatures 2. Timestamps 3. Audit trails
Information Disclosure	1. Authorization 2. Privacy-enhanced protocols 3. Encryption 4. Protect secrets 5. Don't store secrets
Denial of Service	1. Appropriate authentication 2. Appropriate authorization 3. Filtering 4. Throttling 5. Quality of service
Elevation of privilege	1. Run with least privilege

The STRIDE Threat Model

- ✓ For Detail Study - https://owasp.org/www-community/Threat_Modeling_Process

Threat Modelling

DREAD

DREAD

- ✓ DREAD threat modeling is a
  - ✓ quantitive assessment regarding the severity of a threat, with a scaled rating assigned to risk. DREAD has five categories, consisting of
  - ✓ developed by Microsoft
  - ✓ Damage,
  - ✓ Reproducibility,
  - ✓ Exploitability,
  - ✓ Affected Users, and
  - ✓ Discoverability

DREAD

- ✓ **Damage:** The total damage (or impact) that a threat can cause.
- ✓ **Reproducibility:** The ease at which an attack can occur (or be replicated).
- ✓ **Exploitability:** How likely or easy the weakness or threat can be exploited.
- ✓ **Affected Users:** The number of (end) users that could be affected by a threat being exploited.
- ✓ **Discoverability:** How likely a threat will be discovered by an attacker.

DREAD

- ✓ **Damage:** The total damage (or impact) that a threat can cause.
- ✓ **Reproducibility:** The ease at which an attack can occur (or be replicated).
- ✓ **Exploitability:** How likely or easy the weakness or threat can be exploited.
- ✓ **Affected Users:** The number of (end) users that could be affected by a threat being exploited.
- ✓ **Discoverability:** How likely a threat will be discovered by an attacker.

DREAD is one of the available threat modeling methods. There are many others, such as STRIDE, PASTA, and LINDDUN.

DREAD

- ✓ Note: DREAD threat modeling is not widely used anymore, it was initially developed by Microsoft, but its usage was discontinued due to the belief that its ratings are subjective (from those that perform DREAD threat modeling, and assign ratings).

Mobile Phone Security

Dr. Digvijaysinh Rathod
Associate Professor
School of Cyber Security and Digital Forensics
National Forensic Sciences University

digvijay.rathod@nfsu.ac.in