Attack Vectors Models

Raymond A. Vejar

Grand Canyon University

CYB-630: Benchmark – Attack Vectors Models

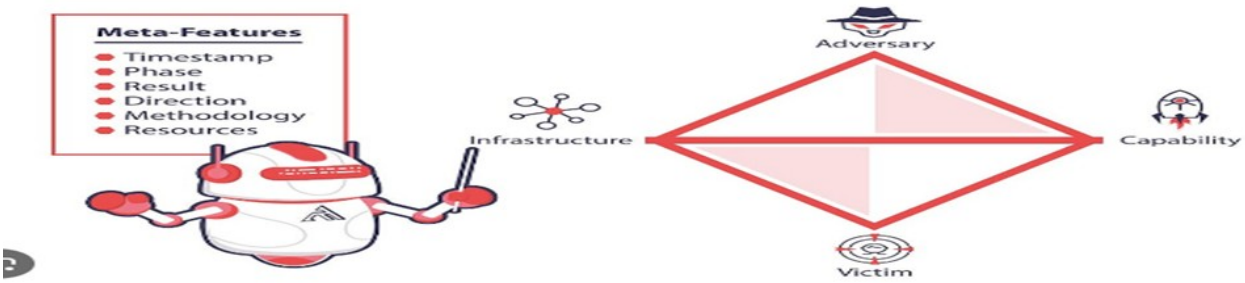
Professor Howard Goodman

July 24, 2024

Attack Vectors Model:

In cybersecurity, there are several approaches used to track and analyze the various characteristics of cyber intrusions by threat actors.

The main objectives of the Diamond Model of Intrusion Analysis is to identify specific attackers, understand the tactics, threats, and procedures they use, and more effectively respond to cyber incidents as they occur.



The model uses four vertices, or atomic elements, to represent the core components of an attack:

- **Adversary:** The attacker and their tools
- **Infrastructure:** The physical and logical communication channels used to deliver, deploy, and control the adversary's capability
- **Capability:** The adversary's capabilities
- **Victim:** The organizations, people, or other assets that the adversary is targeting to exploit their vulnerabilities

Cyber Kill Chain Model:

The Cyber Kill Chain Model (CKC), is a security model that helps organizations identify and stop cyber-attacks by mapping the stages of a cyber-attack. The model was derived from a military attack models and transposed over to the digital world to help teams understand, detect, and prevent persistent cyber threats.

The model, uses seven cyber kill chain phases that include:

- **Reconnaissance:** An attacker collects information about the target's organization, vulnerabilities, or weak points in a system.
- **Weaponization:** Exploit security vulnerabilities found, malicious code is engineered to suit the attackers needs and the attack's intent.

- **Delivery:** Malware delivered by hacking the organization's network and exploiting software, hardware, or through social engineering.
- **Exploitation:** The goal, of this process is to reach targets by moving laterally across a network by exploiting vulnerabilities they have identified in earlier stages.
- **Installation:** Cyberweapons, are installed to gain access to the targeted network by exploiting vulnerabilities, in order; to control and exfiltrate valuable information.
- **Command and Control:** An organization's systems are compromised during the attack by brute-force, searching for credentials, and changing permissions using privileged accounts.
- **Actions on Objectives:** Persistent access has been gained, the attacker has executed their objectives, which can be data theft, destruction, encryption, or exfiltration.

How These Two Models Deviate From Each Other:

Focus:
The cyber kill chain model focuses on the stages of a Cyber-attack, from surveillance to carrying out the attacker's objectives.

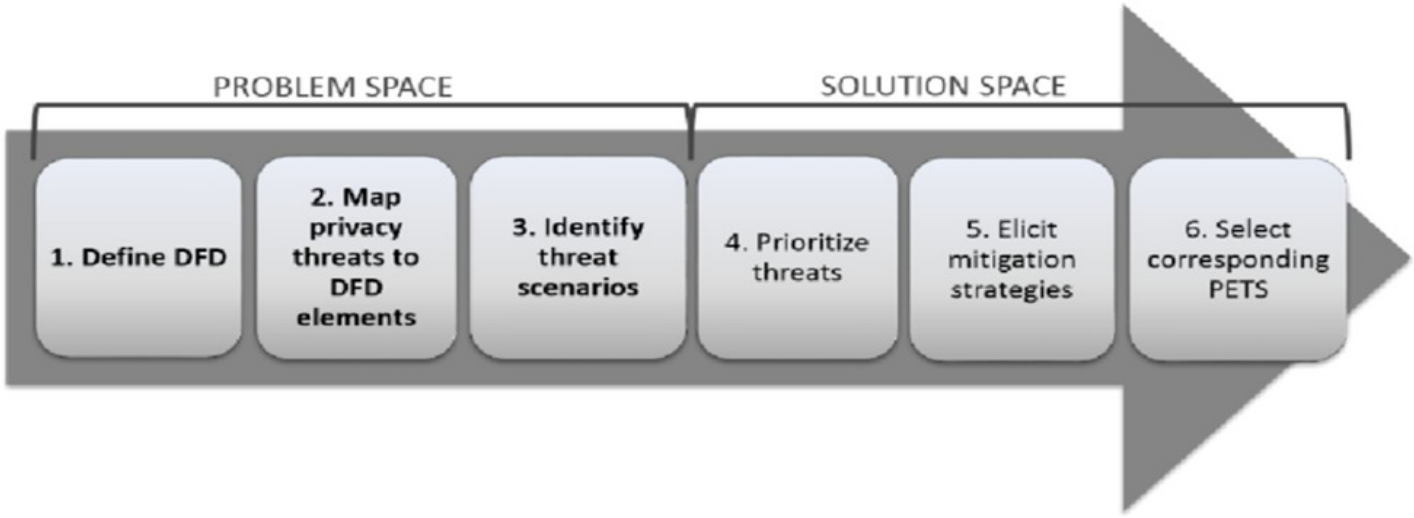
The Diamond Model focuses an attackers motivations and capabilities, including the relationships between adversaries and victims.

Granularity:
Cyber kill chain is more specific, while the Diamond Model offers a broader perspective.

Application:
Cyber Kill chain is more focused on incident response, while Diamond Model is useful for threat intelligence and threat hunting.

Privacy Protection Approaches:

Individuals, organizations, and the government has recognized the importance of using Privacy Threat Models to address privacy protection. For instance, the LINDDUN threat model, is a comprehensive approach that goes beyond traditional security threat modeling by explicitly focusing on privacy. The framework, uses four essential questions to address privacy at an individual, organizational, and government levels. This method comprises a catalog of privacy threat types, mapping tables, threats trees, taxonomy of mitigating strategies, and classification of privacy-enhancing solutions.



The Four Essential Questions that need to be Considers:

1**.What are we working on?** This step involves creating a detailed model of the system, understanding all its components and how they interact.

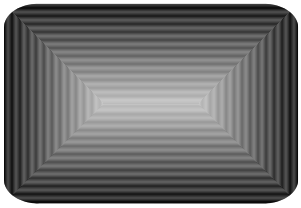
2.**What can go wrong?** This is about identifying potential privacy threats within the system, considering various scenarios and vulnerabilities.

3. **What are we going to do about it?** Here, strategies and measures are developed to mitigate the identified risks.

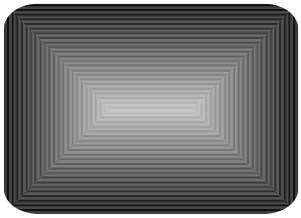
4**. Did we do a good enough job?** This final question involves evaluating the effectiveness of the implemented strategies, ensuring they adequately address the risks.

For example, with Individual privacy protection approach using the LINDDUN threat model:

1. **What are we working on?:** Individual Privacy Protection: Individual privacy is a fundamental human right that gives the people ability to control how their personal information is handled, and to be free from interference and intrusion.



2. **What can go wrong?:** Individual Privacy Risk: This is likelihood that individuals will experience problems resulting from data processing and sharing, and the impact of these problems should they occur.



- Data Breaches
- Identity theft
- Online Tracking
- Phishing scams
- Social engineering Attacks
- Public disclosure of Private facts
- Sharing too much personal information

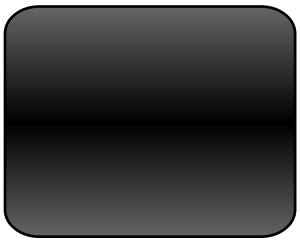
Public Wi-Fi
Information shared without consent
Banking PII made available to third-parties

3. **What are going to do about it?**: Mitigate the Identify Risk: Reduce the impact of potential risk by developing a plan to manage, eliminate, or limit setbacks.

- Create strong passwords
- Don’t overshare on social media
- Use caution watch out for links and attachments
- Use secure sites
- VPN encrypt personal traffic

- Additional protection -anti-virus, anti-spyware and firewall
- Read privacy policies and collection notices
- Secure Your Devices
- Use multi-factor authentication
- Password Mangers
- Lock personal devices

4. **Did we do a good enough job?:** Evaluating the effectiveness of the implemented strategies:



- Monitor Credit Reports
- Dark Web monitoring -Compromised Information
- Privacy pen test
- Practice best individual security measures and protection
- Risk assessment

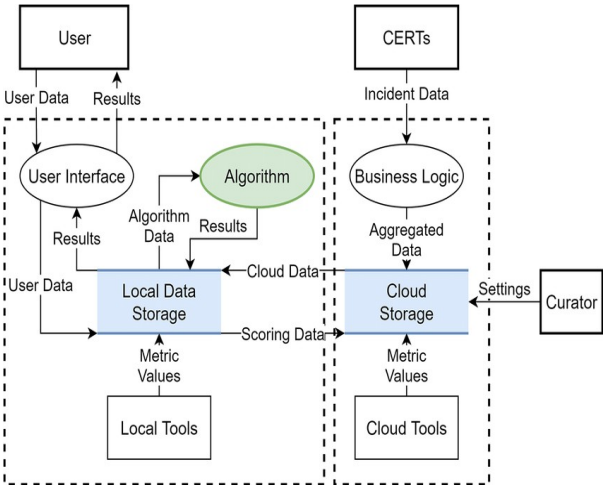
Privacy Theat Modeling, is a proactive process that helps identify and address potential privacy risk in individuals, systems, and applications. Which is a great approach for individuals, organizations, and government levels to address privacy threats. This process includes analyzing the collection, storage, processing, and sharing of personal data to foresee and mitigate potential privacy risks and breaches. Yet, it is imperative to note, that using several privacy threat models is recommended, as an approach to privacy protection that can include:

- STRIDE Central Differential Privacy
- DREAD LINDDUN

Cyber Theat Models:

Organization's should choose which cyber threat modeling method to use based on the specific needs of their project:

PASTA: The Process for Attack Simulation and Threat Analysis uses a seven-step, risk-based methodology for threat modeling in cybersecurity. PASTA's approach combines an attacker's perspective, risk, and impact analysis to create a complete picture of threats. This approach can help organizations meet compliance, regulatory and technical requirements.



Data Flow Diagrams: Simple technical diagrams that depict flows of data and interactions between key components of an application or information technology system. Security teams can use this information to identify and analyze data pathways to ensure secure data handling and optimized processes. DFDs depict the movement of information between components.

The Common Vulnerability Scoring System (CVSS) uses a formula to calculate a severity score for each vulnerability based on four metric groups: Base, Threat, Environmental, and Supplemental. This model, was developed by NIST, and classifies each vulnerability by a score out of 10, with 10 being the most critical.

Conclusion:

- **The cyber threat models can be used to detect and guard against a wide range of cybercrime threat vectors, motivations, and ideologies. Organizations can design more effective security controls to protect their data and systems by understanding these threat models.**
- **Cyber threat models, use hypothetical scenarios, system diagrams, and testing to help secure systems and their data. The processes, involves identifying potential attackers, their motivations, and the methods they might use to exploit vulnerabilities in a system.**

Cyber threat vectors include:

- **Malware, ransomware, spyware, worms, trojan, and viruses.**
- **Compromised, weak, or stolen credentials**
- **Phishing**
- **Zero-day vulnerabilities**
- **Missing or poor encryption**
- **Misconfigurations**

Motivations for Cyber threat Actors include:

- **Financial gain and Espionage**
- **Hacktivism and Sabotage**
- **Disruption and Ransom**
- **Personal vendettas and political discord**