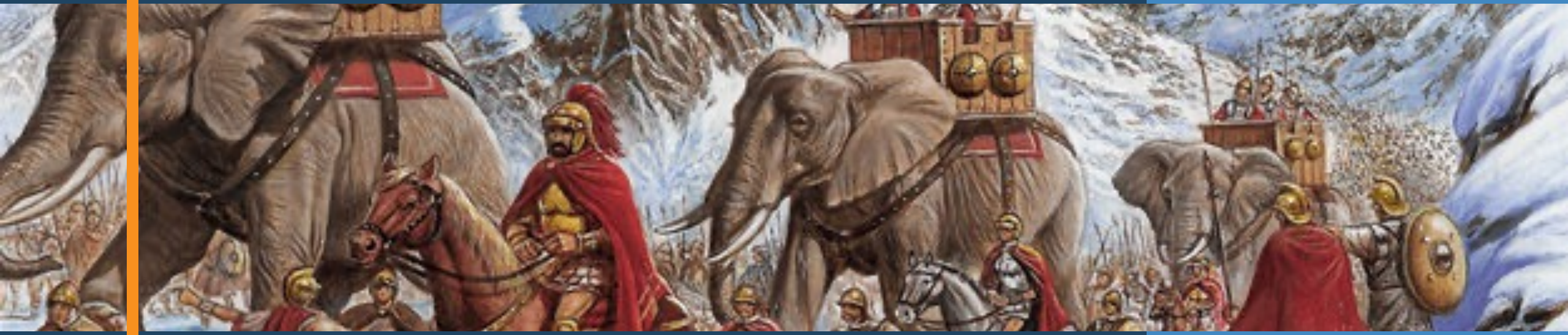
ZAKTI
SECURITY LABS

Threat Modeling Walkthrough

Kumar Setty, Principal
Zakti Security Labs



The Problem

- The attacks never end.
- There are new attacks and new attack surfaces which are uncovered every day.
- Most organizations just recycle risks. We fail to think outside the box.

Sun Tzu

If you know the enemy and know yourself, you need not fear the result of a hundred battles.

If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle.

The Battle of Cannae

In 216 BCE, a pivotal battle, The Battle of Cannae, was fought between Carthage and the Roman Republic. This battle was the closest the Roman state had come to destruction in its history up to this point. The Roman Republic survived this disaster and actually ended up annexing the Carthaginian Empire (present day Tunisia).

This Battle was fought in southeast Italy between Carthaginian forces led by the general Hannibal Barca and Roman legions led by generals Lucius Paullus and Gaius Varro. After Rome won the First Punic War, they became the dominant naval power in the Mediterranean Sea, and Rome colonized Iberia to mine its silver, further enriching the Republic.

Hannibal understood Roman strategy and decided to take the initiative by taking the fight to the heart of the Roman Republic.

Hannibal started his campaign by invading Iberia. There he procured silver, supplies, and food, and then used these provisions to cross the Alps into Italy with his army and war elephants. After winning some decisive battles, Hannibal marched through to southern Italy, where he used his silver to buy off Greek and Italian vassals of Rome to join his army. He then encamped at Cannae.

He chose Cannae because it was the center of farming and grain production for the Roman heartland. Hannibal specifically chose a region in Cannae which was near the only source of water in the area. This applied tremendous pressure on the Roman legions and in this manner, he provoked a fight on his terms. Hannibal then outflanked the legions and crushed the Roman army. However, unfortunately for Hannibal, Rome's legions were too big to lose. This battle initiated a long drawn out campaign in which Hannibal was eventually defeated by the Roman general Scipio Africanus and Carthage was annexed by Rome.

The Battle of Cannae - Lessons

What can we learn from this? Rome lost the Battle of Cannae because they underestimated and failed to understand their adversary. The Romans never imagined an army would cross the Alps from North Africa (audacious move) with elephants (unique attacker tools) and they did not anticipate what to defend (Iberia, the Alps, and southern Italy) and they failed to anticipate where they would be attacked (from the sole source of water in Cannae).

Hannibal Barca was a bold genius and unlike any adversary the Roman Republic had ever encountered. Hannibal understood his own capabilities and Rome's, he wisely utilized his assets, he knew Roman strategy and battle formations, he understood Rome's weaknesses and who might be willing to betray Rome. He employed assets to gather intelligence prior to engaging Rome in battle. Hannibal found the right attack surfaces.

Threat modeling is something the Roman Republic should have employed. Rome failed to understand Hannibal, his motivations, his strengths, and where, when, and how he would attack them. If the Romans had established a threat model, they might have won the Battle of Cannae.

The Mongol Invasions of India

Well within the 13th century, the Mongolian Empire was the largest empire in the world. They ruled from Siberia and China and reached Budapest.

The Mongols tried dozens of times to invade India. Every time they failed. In one instance, just when it seemed like the Mongols would win, they were crushed as a result of a unique counterattack.

In 1299, the Mongol army led by Duwa Khan marched 200,000 cavalry, thousands of foot soldiers, and siege weapons and projectile weapons using gunpowder - all designed by Chinese engineers. This army camped outside of Delhi prepared to crush the city walls and to annihilate all the inhabitants. Delhi was under the rule of the Delhi Sultanate, controlled by Sultan Alauddin Khalji. Not a benevolent ruler but a great tactician.

The Mongol Siege of Delhi

The siege went on for days and at one point it seemed that the Mongol army would breach the fortifications and annihilate the residents of Delhi.

At the brink of defeat, some of the generals of the Sultan came up with a plan.

Within the walls of the Delhi, there was a huge store of fermented ale, which was being saved for a festival. Also, there were several thousand war elephants.

During this time, it was elephant breeding season. The male elephants were irritable because their libido was high.

Drunk Elephants

The army of the sultan made the male elephants thirsty and hungry.

They then placed the female elephants at the other end of the battlefield and fed the females beer so they would be docile.

They fed the male elephants ale to make them more aggressive.

In between the drunk female elephants and the drunk and libidinous male elephants were most of the Mongol army and their siege weapons.

The Sultan’s army released the male elephants.

The drunk male elephants flanked, crushed, and destroyed the Mongol siege weapons and crushed the invading army so that they could reach the female elephants.

The Sultan then led his archers, cavalry, and army and defeated the remaining Mongol army.

The Sultan then had the elephants crush all the surviving Mongols and thousands of heads were sent back to Mongolia as a warning not to invade India ever again.

The Mongol army tried for many years even after this disaster, but they never were able to conquer India.

Mongolian Invasion of India - Lessons

The Mongol adversary model vs the Indian defender model. Model vs. model and machine vs machine.

The Mongol threat model did not take into account that within the Delhi walls there was a huge store of ale and elephants. Also, it was breeding season for the elephants. Their model did not take this into account. Also, the Mongols did not study Indian warfare methods.

In ancient India, elephants were commonly used in war. When Alexander of Macedon tried to invade India, Indian forces used elephants fed with opium to counter-attack the Macedonian army. Other Indian rulers used this same method of intoxicating elephants. Using elephants was not a new strategy, but the application was novel - inebriation and enticement.

The Mongol army was “dug in” and concentrated on breaching the walls of Delhi. They were inflexible at this critical point.

The generals in India used out of the box thinking in developing a counterattack. The defender model enabled flexibility so the Sultan’s men could formulate this attack.

What is Threat Modeling?

Threat modeling is an adversary centric process through which security professionals identify threats and vulnerabilities, quantify the likelihood and impact, and then formulate techniques to mitigate attacks to protect an organization.

Combination of art and science.

A crystal ball is not possible.

The process should be ***systematic*** *and* ***structured****.*

Goal is “forewarned is forearmed”.

Threat Modeling

An important feature of a security professional is the ability to "predict" the future – future threats, future attacks, and future frauds and enablers. I put "predict" in quotes because it's impossible to predict the future with certainty but using the right tools and methodologies we can at least ask the right questions in order to clarify our thoughts and impressions and obtain some measurements which we can use as inputs into our planning and strategic decisions.

A completely siloed approach will not work.

Threat Modeling Approach

One suggested approach

#	Question	Tasks	Output(s)
1	**KNOW YOURSELF** What are you trying to protect?	1. Identify the overall system boundary and identify the flow of information into and out of these boundaries. 2. Enumerate the physical, logical assets – servers, databases, and other components. 3. Identify any intangible assets which are critical to the business.	1. Data Flow Diagram 2. Asset List 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
2	**KNOW YOUR ENEMY** **KNOW YOUR FRIENDS** Who are the attackers (internal and external)?	1. Identify potential threat actors, threats, and attack scenarios. 2. Brainstorm motivations of an attacker through cooperation with different teams and groups. 3. Identify business risks and results of other assessments such as a fraud risk assessment. 4. Who wants to steal or damage the assets? 5. Who are you most concerned about?	1. Adversary Model – resources, access, risk tolerance, and objectives. 2. Attack scenarios or "abuse cases". 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
3	**KNOW YOUR ENEMY** **KNOW YOUR FRIENDS** **KNOW YOURSELF** What type of attack surfaces are present? Where will the organization be attacked?	1. Identify the methods, tools, where an attacker or other systems interact with the system. 2. Identify all the third-party integrations and dependencies.	1. Vulnerability Model – Using the Adversary Model above as an input, map vulnerabilities. 2. Interface or integration diagram – high-level and low-level. 3. Surveys sent to individual stakeholders 4. Notes from group sessions.
4	**KNOW IT ALL** What are the risks, controls, likelihood, and impact? Countermeasures?	1. Using an established framework such as NIST, identify risks, controls, and calculate likelihood and impact. 2. Calculate total risk exposure by multiplying likelihood and impact. 3. Above a certain threshold for risk exposure, maybe High and Critical, document exploits. 4. Generate corresponding countermeasures for each High and Critical risk exposure.	1. NIST matrix with risks, controls, likelihoods, impact, calculated risk exposure, and detailed countermeasures.

Caveat

It is not as important to generate copious paperwork as it is to *understand* the organization's posture, threats, and countermeasures.

You may not have accounted for all the threats and countermeasures, but at least you have documented your understanding and you might identify any gaps in your understanding. In essence you will know what you don't know.

Threat Modeling Frameworks

The structured approaches for threat modeling are frameworks or methodologies (both interchangeable terms) and are a veritable alphabet soup of acronyms and special lingo. The main frameworks are as follows:

NIST

OCTAVE

PASTA

STRIDE

DREAD

MITRE ATT&CK

NIST Threat Modeling Methodology

The U.S. National Institute of Standards and Technology has its own data-centric threat modeling methodology, which consists of four steps:

Identify and characterize the system and data of interest

Identify and select the attack vectors to be included in the model

Validate the security controls for mitigating the attack vectors

Evaluate the threat model

If you are looking for a great example of how to apply a threat modeling methodology in practice, this is a good resource.

https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

OCTAVE

OCTAVE, which stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a threat modeling methodology developed at Carnegie Mellon University that focuses on organizational rather than technological risks. It consists of three phases:

Build asset-based threat profiles

Identify infrastructure vulnerability

Develop a security strategy and plans

https://resources.sei.cmu.edu/library/Asset-view.cfm?assetid=51546

PASTA

PASTA or Process for Attack Simulation and Threat Analysis is a seven-step process focused on aligning technical security requirements with business objectives. Each step is fairly involved. The overall sequence is as follows:

Define objectives

Define technical scope

Application decomposition

Threat analysis

Vulnerability and weaknesses analysis

Attack modeling

Risk and impact analysis

https://owasp.org/www-pdf-archive/AppSecEU2012_PASTA.pdf

STRIDE

STRIDE was developed at Microsoft in the 1990s and popularized by developers and project managers. STRIDE emphasizes the six categories of threats which violate one of the properties of the CIA triad (confidentiality, integrity, availability):

Spoofing identity: An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password.

Tampering with data: Data tampering involves the malicious modification of data.

Repudiation: Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise. Nonrepudiation refers to the ability of a system to counter repudiation threats.

Information disclosure: Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it.

Denial of service: Denial of service (DoS) attacks deny service to valid users.

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.

DREAD

DREAD was created as a supplement to the STRIDE methodology which enables analysts to rank threats once they have been identified. DREAD is an acronym for the six questions asked regarding each potential threat:

Damage potential: How great is the damage if the vulnerability is exploited?

Reproducibility: How easy is it to reproduce the attack?

Exploitability: How easy is it to launch an attack?

Affected users: As a rough percentage, how many users are affected?

Discoverability: How easy is it to find the vulnerability?

MITRE ATT&CK

The MITRE ATT&CK framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations from security professionals. This framework is constantly being updated and there are variations which can be “spun off” which concentrate on a specific area, such as cloud computing or mobile security.

Version 9 was just recently released. The ATT&CK framework is an excellent resource for understanding attacker techniques and it is a great starting point for integrating common attacks into a threat model. There are also many resources available to get started on using this methodology.

If you are a visual person, the Enterprise Matrix is an excellent tool for understanding the different stages of attacks from Reconnaissance to Exfiltration to Impact and all the techniques and sub-techniques within each attack category.

https://attack.mitre.org/resources/getting-started/

https://attack.mitre.org/matrices/enterprise/

Recommendations

Many frameworks exist and there are many similarities.

First understand the organization, study previous assessments, and understand exactly what you are attempting to secure.

Use the OCTAVE methodology since it has a more organizational emphasis. OCTAVE has comprehensive information for developing surveys which can be sent to individuals for completion.

Also use OCTAVE guidelines for the group sessions.

Obtain an understanding of the business risks and fraud risks. These insights should flow into the Adversary Model.

The NIST threat modeling framework as a starting point. I would then integrate the attacker techniques from the MITRE ATT&CK framework to complete the Adversary Model.

In the final stage, the overall model should include overall risk ratings and specific countermeasures. Finally, always remember that your threat model should be a living document and should be revisited and edited on a frequent basis to accommodate changes to the organization’s risk profile.

Always Remember

KNOW THYSELF

KNOW THINE ENEMIES AND THINE FRIENDS

KNOW IT ALL

ZAKTI
SECURITY LABS

Kumar Setty

Kumar Setty, CISSP, CISA

@zaktilabs

@zaktilabs