Threat Modeling

Contents

General
- High level threat modeling process
- Example
- High level modeling tools

Business Asset Analysis
- Organizational Data
  - Policies, Plans, and Procedures
  - Product Information (e.g. trade secrets, R&D data)
  - Marketing Information (plans, roadmaps, etc.)
  - Financial Information (e.g. bank, credit, equity accounts)
  - Technical Information
  - Employee Data
  - Customer Data
- Human Assets

Business Process Analysis
- Technical infrastructure supporting process
- Information assets supporting process
- Human assets supporting process
- 3rd party integration and/or usage of/by process

Threat Agents/Community Analysis
- Employees
- Management (Executive, middle)

Threat Capability Analysis
- Analysis of tools in use
- Availability to relevant exploits/payloads
- Communication mechanisms
- Accessibility

Motivation Modeling

Finding relevant news of comparable Organizations being compromised

General

This section defines a threat modeling approach as required for a correct execution of a penetration testing. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results.

The standard focuses on two key elements of traditional threat modeling - assets and attacker (threat community/agent). Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities.

As a minimum, all four elements should be clearly identified and documented in every penetration test.

When modeling the attacker side, on top of the threat community (which is mostly semantic and can be tied back to the organization's business SWOT analysis), and the capabilities (which is mostly technical), additional aspects of motivation modeling should also be provided. These additional points essentially take into account the value of the different assets available at the target and are combined with the cost of acquiring it. As a complementary model, impact modeling should also be performed for the organization in order to provide a more accurate view of the "what-if?" scenario surrounding the loss event of each of the identified assets. This should take into account the assets "net" value, its intrinsic value, and other indirectly incurred costs associated with a loss event.

The threat modeling phase of any penetration testing engagement is critical for both the testers, as well as the organization. It provides clarity as far as the organization's risk appetite and prioritization (which assets are more important than others? what threat communities are more relevant than others?). Additionally, it enables the tester to focus on delivering an engagement that closely emulates the tools, techniques, capabilities, accessibility and general profile of the attacker, while keeping in mind what are the actual targets inside the organization such that the more relevant controls, processes, and infrastructure are put to the test rather than an inventory list of IT elements. The threat model should be constructed in coordination with the organization being tested whenever possible, and even in a complete black-box situation where the tester does not have any prior information on the organization, the tester should create a threat model based on the attacker's view in combination with OSINT related to the target organization.

The model should be clearly documented, and be delivered as part of the final report as the findings in the report will reference the threat model in order to create a more accurate relevance and risk score that is specific to the organization (rather than a generic technical one).

High level threat modeling process

1. Gather relevant documentation
2. Identify and categorize primary and secondary assets
3. Identify and categorize threats and threat communities
4. Map threat communities against primary and secondary assets

Example

In the light of a PTES assessment the internally hosted CRM application may be in scope. The customer information stored in the back-end database is an easily identifiable primary asset as it is directly linked to the application in scope. However, by reviewing the technical design of the database server, it can also be identified that the HR database stored on the same back-end database server is a secondary asset. An attacker can use the CRM application as a stepping stone to obtain employee information. In a basic threat modeling exercise, certain threat communities may be identified as not relevant when mapped to the CRM application, but by identifying the secondary assets the threat landscape suddenly changes.

High level modeling tools

There are a variety of tools available to identify targets and map attack vectors. These normally focus on the business assets (what systems to target) and business processes (how to attack them.) Depending on the engagement, the penetration testing team may perform these exercises with no input from the customer; or they may spend a lot of time with customer stakeholders identifying targets of interest. Tools with a business asset focus usually require a quantitative input to describe how important each potential target is to test. The inputs may also be qualitative, such as a description by the customer's CIO that a system is mission-critical. Tools focused on business processes, information flows and technical architecture are used to identify potential attack vectors and choose which are mostly likely to succed or most likely to be used by a certain class of adversary.

Business Asset Analysis

During the business asset analysis part of the threat modeling exercise an asset-centric view is taken on all assets, and business processes they support them, included in the scope. By analyzing the gathered documentation and interviewing relevant personnel within the organization, the pentester is able to identify the assets that are most likely to be targeted by an attacker, what their value is and what the impact of their (partial) loss would be.

Organizational Data

Policies, Plans, and Procedures

Internal policies, plans, and procedures define how the organization does business. These documents are of particular interest as they can help identify key roles within an organization and critical business processes that keep a company running.

Product Information (e.g. trade secrets, R&D data)

Product related information includes any patents, trade secrets, future plans, source code, supporting systems that directly affect the product market value, algorithms, and any other information that the organization regards as a key factor to the business success of such product.

Marketing Information (plans, roadmaps, etc.)

Marketing plans for promotions, launches, product changes, positioning, partnerships, 3rd party providers, business plans related to activities inside or outside the organization. Additionally, PR related data such as details of partners, reporters, consulting firm, and any correspondence with such entities is also considered a highly sought after target.

Financial Information (e.g. bank, credit, equity accounts)

Financial information is often some of the most guarded information an organization possesses. This information can include bank account information, credit card account information and/or credit card numbers, and investment accounts, among others.

Technical Information

Technical information about the organization, and the organization's operations, is of unique interest to the penetration tester. Such information is often not the expected deliverable of a penetration test, however, it facilitates the testing process by feeding valuable information to other areas;

infrastructure design information may provide valuable data to the Intelligence Gathering process.

- Infrastructure Design Information

Infrastructure design related information pertains to all the core technologies and facilities used to run the organization. Building blueprints, technical wiring and connectivity diagrams, computing equipment/networking designs, and application level data processing are all considered infrastructure design information.

- System Configuration Information

System configuration information includes configuration baseline documentation, configuration checklists and hardening procedures, group policy information, operating system images, software inventories, etc. This information could aid the discovery of vulnerabilities (such as through the knowledge of configuration errors or outdated software installations).

- User Account Credentials

User account credentials help facilitate access to the information system, at a non-privileged level, as long as a means to authenticate exists (e.g. VPN, web portal, etc.).

- Privileged User Account Credentials

Privileged user account credentials help facilitate access to the information system, at an elevated level of access, as long as a means to authenticate exists (e.g. VPN, web portal, etc.). Obtaining privileged user account credentials often leads to compromise of the information system being tested.

Employee Data

Here employee data is being analyzed as any data that can have a DIRECT affect on the organization is obtained or compromised by an attacker. Organizations that have to adhere to some compliance which places fines on the loss or exposure of such data are obvious candidates for such a direct loss effect. Also, organizations who’s employees may be considered critical assets may also be subjected to such scrutiny (specific government bodies, specialized trade secret related employees/departments, etc...). The following list provides examples to information realms of personal data that may be considered business assets for the threat modeling.

- National Identification Numbers (SSNs, etc.)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Information (e.g. bank, credit accounts)

Customer Data

Much like employee data, customer data is considered a business asset in the threat modeling process when such information will incur a direct/indirect loss to the organization. On top of regulatory/compliance need (based on fines), an additional factor comes into play here when such data can be used to conduct fraud, where the organization may be held liable or sued for the losses related to the fraud (based on losing the customer information that enabled the fraud to take place). The following list provides examples of such information realms that may hold relevant customer data and should be considered business assets for the sake of the threat modeling

- National Identification Numbers (SSN’s, etc.)

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Accounts (e.g. bank, credit, equity accounts)
- Supplier Data

Information related to suppliers that is considered critical to the organization (such as critical component manufacturers, agreements with suppliers that may be part of a trade secret, cost analysis of supplied components), as well as any data that may be used to affect the business operations of the organization through its suppliers is considered a business asset.

- Partner Data
- “Cloud” Service Account Information

Human Assets

When identifying human assets in an organization, we have to remember that the context is having such assets part of a greater effort to compromise the organization. As such, human assets that are identified as business assets are those that could be leveraged to divulge information, manipulated to make decisions or actions that would adversely affect the organization or enable an attacker to further compromise it. Human assets are not necessarily the highest up within the corporate hierarchy, but are more often key personnel that are related to previously identified business assets, or are in positions to enable access to such assets. This list can also include employees that normally would not be associated with access to restricted company assets, but may be in a position to grant physical access to a company that facilitates a breach of security or procedure. The following list provides some examples of such assets, and should be adapted to the organization being tested.

- Executive Management
- Executive Assistants
- Middle Management
- Administrative Assistants
- Technical/Team Leads
- Engineers
- Technicians
- Human Resources

Business Process Analysis

A business isn't a business if it doesn't make money. The way this happens is by having either raw goods or knowledge run through various processes to enhance them and create added value. This generates revenue. Business processes and the assets (people, technology, money) supporting them form value chains. By mapping these processes, identifying the critical vs. non-critical processes and eventually finding flaws in them we are able to understand how the business works, what makes them money and eventually how specific threat communities can make them lose money.

In the business process analysis we differentiate between critical business processes, and non-critical processes. For each category the analysis is the same, and takes into account the same elements. The main difference is in the weighting that the threat from a critical business process is assigned with as opposed to a non-critical one. Nevertheless, it's imperative to remember that an aggregation of a few non-critical business processes can be combined into a scenario that essentially forms a critical flaw within an element/process. Such threat scenarios should also be identified within this phase and mapped out for later use in the penetration test.

Technical infrastructure supporting process

As business processes are usually supported by IT infrastructure (such as computer networks, processing power, PCs for entering information and managing the business process, etc...), all those elements must be identified and mapped. Such mapping should be clear enough to be used later on in the process when translating the threat model to the vulnerability mapping and exploitation.

Information assets supporting process

Contrary to technical infrastructure, information assets are existing knowledge bases in the organization that are used as either a reference, or as support material (decision making, legal, marketing, etc...). Such assets are usually identified in the business process already, and should be mapped alongside the technical infrastructure, as well as any additional technical infrastructure that supports the information assets themselves.

Human assets supporting process

Identification of the HR that are involved in the business process should be made in conjunction with the process analysis itself (whether documented or not), and every person that has any kind of involvement (even if it does not relate to a specific information asset or a technical infrastructure element) should be documented and mapped in the process. Such HR assets are usually part of an approval sub-process, a verification sub-process, or even a reference (such as legal advice). These kinds of assets (especially ones that have no relation to information assets or technical infrastructure) would be later mapped to attack vectors that are more social than technical in nature.

3rd party integration and/or usage of/by process

Similar to human assets supporting the process, any 3rd party that has any involvement with the business process should be mapped as well. This category can be tricky to map out, as it could contain both human assets, as well as information/technical ones (such as a SaaS provider).

Threat Agents/Community Analysis

When defining the relevant threat communities and agents, a clear identification of the threat should be provided in terms of location (internal / external to the organization), the specific community within the location, and any additional relevant information that would assist in establishing a capabilities/motivation profile for the specific agent/community. Where possible, specific agents should be identified. Otherwise, a more general community should be outlined, along-with any supporting material and intelligence. Some examples of threat agent/community classifications are:

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

Employees

Persons working directly for the company under a part-time or full-time contract. In general they are not regarded as posing a severe threat as most of them are relying on the company to make a living and, assuming they are treated well, are inclined to protect the company rather than to hurt it. Oftentimes involved in data loss incidents or accidental compromise. In rare cases they may be motivated by outsiders to assist in intrusions or they may engage in malicious acts on their own (e.g. rogue traders). While the skill level may vary, it is usually low to medium.

Management (Executive, middle)

Employees working directly for the company as described above. Given their position and function within the company they oftentimes have access to privileged information and may

Threat Capability Analysis

Once a threat community has been identified, the capabilities of said community must also be analyzed in order to build an accurate threat model that reflects the actual probability of such a community/agent to successfully act upon the organization and compromise it. This analysis requires both a technical analysis as well as an opportunity analysis (where applicable).

Analysis of tools in use

Any tools that are known to be available to the threat community/agent are to be included here. Additionally, tools that may be freely available should be analyzed for the required skill level needed to be able to utilize them to their potential, and mapped in the threat capability.

Availability to relevant exploits/payloads

The threat community/agent should be analyzed in terms of its capability to either obtain or develop exploits for the environment relevant to the organization. Additionally, accessibility to such exploits/payloads through 3rd parties, business partners, or underground communities should also be to taken into account in this analysis.

Communication mechanisms

An analysis of communication mechanisms available to the threat agent/community should be made to evaluate the complexity of attacks against an organization. These communication mechanisms range from simple and openly available technologies such as encryption, through to specialist tools and services such as bulletproof hosting, use of drop-sites, and the use of known or unknown botnets to perform attacks or mask source information. For example, as part of testing we test to see what the overall attack surface for an organization is from the outside. However, there is another whole component that is often times missed. What types of threats can exist post exploitation? This falls under the context of detecting exfiltration channels. Coincidentally, penetration testers are uniquely situated to test an organizations capability to detect command and control channels of today's modern malware. When this is in scope, we recommend the tester create a series of malware specimens that increase the level of obfuscation used to hide C2. The goal is to create malware that is easily detected, then increase the obfuscation to the point where detection no longer occurs.

Accessibility

The final element in the threat actor capability analysis is their accessibility to the organization and/or the specific assets in question. Completing the profile depicted above while factoring in accessibility analysis would enable the penetration test to create clear scenarios that are relevant to the organization’s risk.

Motivation Modeling

The possible motivation of threat agents/communities should be noted for further analysis. Motivations of attackers are constantly changing, as can be seen by the increase in hacktivism branded attacks by groups such as Anonymous and Antisec. There will be subtle differences in unique motivations based on each organization and/or vertical market, some common motivations include :

- Profit (direct or indirect)
- Hacktivism
- Direct grudge
- Fun / Reputation
- Further access to partner/connected systems

Finding relevant news of comparable Organizations being compromised

In order to provide a complete threat model, a comparison to other organizations within the same industry vertical should be provided. This comparison should include any relevant incidents or news related to such organizations and the challenges they face. Such a comparison is used to validate the threat model and offer a baseline for the organization to compare itself to (taking into account that this publicly available information only represents a portion of the actual threats and incidents the compared organization actually face).

Retrieved from "http://www.pentest-standard.org/index.php?title=Threat_Modeling&oldid=956"

This page was last edited on 7 December 2015, at 22:24.