

# Written Assignment: Unit 6

## MICS-252, Fall 2024

### Threat Modelling

Prepared by: Karl-Johan Westhoff

email: kjwesthoff@berkeley.edu

UC Berkeley School of Information

MICS Course 252 Fall 2024 (Kristy Westphal)

## 1 Introduction

Threat modelling in cyber security is fairly unique compared to other industries, in other industries the risks to assets and processes are from accidents or involuntary 'incidents'. Cybersecurity threats are from malicious actors who actively tries to exploit the assets, in that regard cybersecurity is comparable to the military or law enforcement (which is probably the reason for all the acronyms in the industry!). OWASP proposes a 'four question' framework[1] to organize threat modelling in general, which I have freely interpreted as:

- What are we working on?
  - Scope definition (The thing could be anything from a feature in an app to a whole network)
- What can go wrong?
  - Risk assessment (Brainstorm and Prioritization)
- What are we going to do about it?
  - Mitigation (Develop proposals that are actually feasible)
- Did we do a good job?
  - Evaluate (Could be part of a higher level parent process e.g PDCA<sup>1</sup>)

I.e. the purpose of a threat model is to identify adversaries, attack techniques<sup>2</sup> and vulnerabilities, and provide clarity on how to mitigate these.

Threat modelling is a component in the overall security assessment of a system/process/company/asset and is applied both at a high level for a whole organization and at a detailed level for an application or feature, hence there is somewhat of a spread in threat assessment methodologies[3], depending on where

---

<sup>1</sup> Plan Do Check Act, a process for continual process improvement[2]

<sup>2</sup> e.g. using MITRE att&ck

they are applied. Much like a FMECA<sup>3</sup> is a "what could possibly break in this component/system and what are the probabilities and consequences", the Threat model is a "How could someone break/break-into/steal data from this system, and how do we protect it" Common in both cases are to identify risks and how to mitigate.

For this assignment I choose to apply the 'STRIDE' model to a fictitious home router setup which most households have (the question of security with these often comes up at dinner parties).

## 2 STRIDE

The stride model looks at six categories to capture, cover and quantify the threats to a system: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege, illustrated in Figure 1.

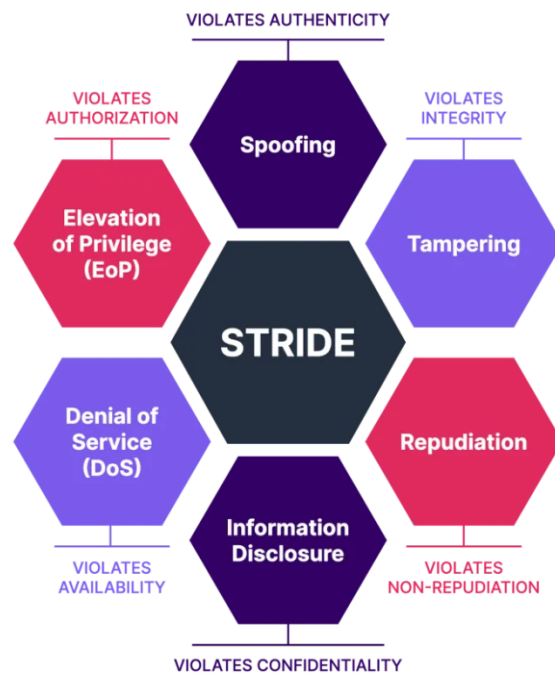


Figure 1: The STRIDE model summarized, illustration from [4]

### 2.1 Steps in a STRIDE analysis

1. Tally up assets (inventory)
2. Prepare a Data Flow Diagram (DFD)
3. Identify boundaries in the DFD, borders are where level of trust changes
4. Evaluate STRIDE for each component at each border
  - Identify Risk

<sup>3</sup> Failure Mode Effects and Criticality Analysis

- Propose Mitigation

## 2.2 Asset Enumeration

A simplified list of assets on the network is shown in Table 1, details such as protocols used and software versions should also be included in a detailed enumeration.

Item	Description
SmartTVs	Wifi connected, has embedded os, receives updates over port 80/443
Printer	Network discoverable on local network (IGMP/M-DNS)
KidsGamerPCs	Windows os, no restrictions on traffic
IOT gadgets	MQTT broker/server connected to internet service
Mobile devices	Ipdas, phones etc,
Guests joining Wifi	Kids share wifi passwords with their friends etc.
Work PC	Company issued pc, VPN client
Router	Provided by ISP, internal firewall blocks inbound traffic except port 80 and 443

**Table 1:** Simplified enumeration of assets on the network

## 2.3 DFD

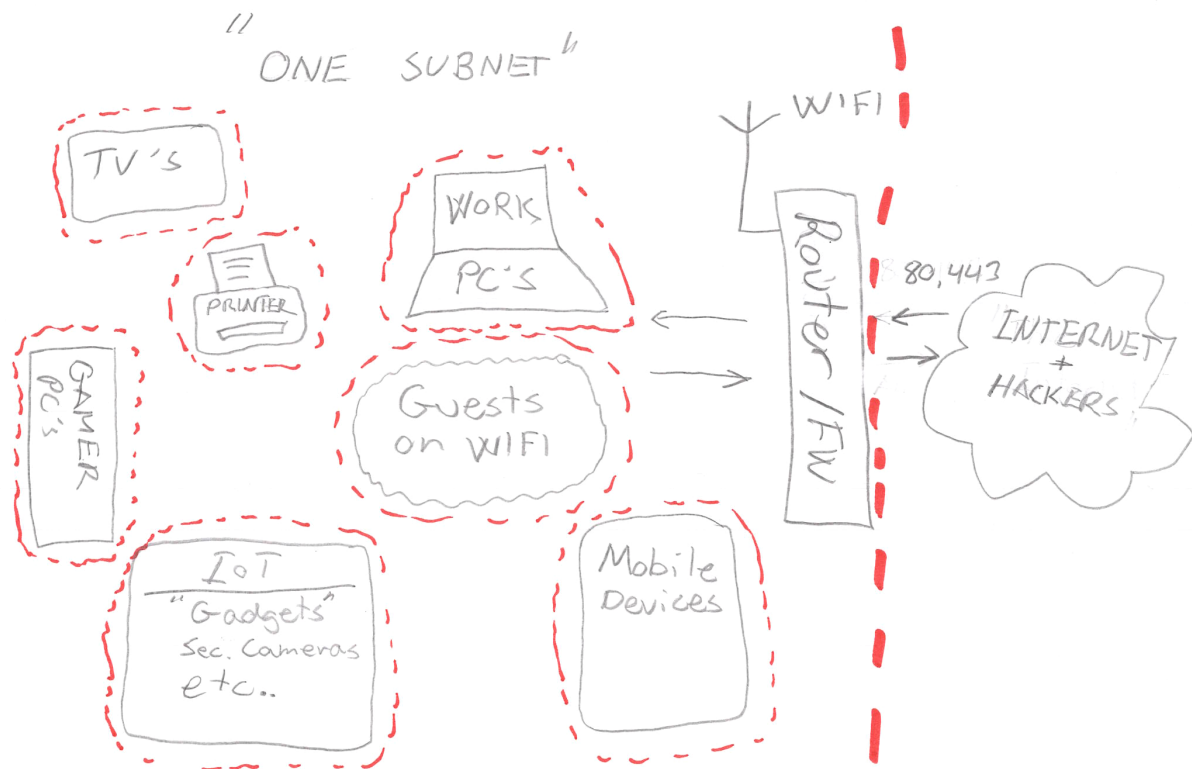
The Data flow diagram is shown in Figure 2, Traffic inbound is only allowed on TCP port 80 and 443, outbound traffic and traffic on the internal network in not limited.

## 2.4 Boundaries

The traffic on the internal network consists of a multitude of data and protocols, IOT devices communicate on their own sub protocols (MQTT, zigbee, bluetooth etc.) with servers connected to the home network. The main boundary to the internet in Figure 2 is marked with red, dashed line i.e. the main boundary asset is at the router. However, guests are sometimes allowed onto the network, all the IOT devices, TV's, mobile devices etc. communicates with servers outside the network (receives software updates etc.). Therefore each asset is within a trust boundary which should be considered (hence the dotted lines around everything.. in Figure 2).

## 3 STRIDE evaluation

Each asset in Table 1 is evaluated for each stride. Some of the assets can be lumped together as they share the same STRIDE weakness.



**Figure 2:** Simple home network Data Flow Diagram, Inbound data only allowed on port 80 and 443, traffic is unlimited on the internal subnet

### 3.1 Spoofing

- SmartTVs
- Printer
- IOT gadgets

**Weaknesses:** Un restricted communication on network, if assets are spoofed, it gives the attacker full access to the local network.

**Mitigaiton:** Put devices on a separate network, keep assets software versions updated

- KidsGamerPCs

**Weaknesses:** The pc's are open to the internet with a human in the loop, this gives a indirect access to the local network if e.g. phishing is successful

**Mitigaiton:** Restrict and monitor software on asset, keep endpoint protection (Windows defender) on asset. Possibly move asset to a separate subnet

- Guests joining Wifi

**Weaknesses:** Wifi passwords may be shared, so anyone can access the private network after the "guests" have left.

**Mitigaiton:** Put guest on a separate subnet (most home routers have this functionality out of the box)

- Work PC

**Weaknesses:** Asset is protected by a VPN, however if the VPN is spoofed (e.g. by a supply chain attack) the vpn provides a direct access into the local network

**Mitigaiton:** Keep software up to date

- Router

**Weaknesses:** The router may be spoofed (also partially by spoofing the wifi) someone else may portray to be the router.

**Mitigaiton:** Keep router firmware up to date, and follow the news if vulnerabilities are found for the asset

### 3.2 Tampering

- SmartTVs
- Printer
- IOT gadgets

**Weaknesses:** These often run on outdated firmware and may have security flaws that allow an attacker to tamper with their functionality, potentially turning IoT cameras into surveillance tools for attackers, or spoiling foods in a smart fridge.

**Mitigaiton:** Put devices on a separate network, keep assets software versions updated

- KidsGamerPCs
- Work pc
- Mobile devices

**Weaknesses:** If malware infects devices, attackers can tamper with system files, applications, etc. including exploiting local network access to spread freely

**Mitigation:** Restrict and monitor software on asset, keep endpoint protection (e.g. Windows defender) on asset. Possibly move asset to a separate subnet if possible to protect the local network

- Guests joining Wifi

**Weaknesses:** If guests assets are compromised, they may introduce malware to the the local network

**Mitigation:** Keep guest on a separate network

- Router

**Weaknesses:** Configuration settings could be tampered with (if management interfaces are insecure), allowing an attacker to disable protection mechanisms, open ports, or alter routing behavior. Tampering with the firewall could allow an attacker to bypass VPN protections, affecting not only home devices but also the work PCs connection to the corporate network.

**Mitigation:** Keep router firmware up to date, and follow the news to pick up if vulnerabilities are found for the asset

### 3.3 Repudiation

There are no formal requirements for repudiation on a home network, however if something happens then logging is extremely important for trouble shooting and investigation.

- SmartTVs
- Printer
- IOT gadgets

**Weaknesses:** Not formally required to log anything, but if these assets are compromised and the manufacturer is liable, proof is hard without a log trail.

**Mitigation:** Do your own logging (advanced), require manufacturer to provide logging.

- Router

**Weaknesses:** Most routers do basic logging, e.g. of which assets are connected to the network. If logging is compromised, a bad actor could hide on the network

**Mitigation:** Keep router firmware up to date, and follow the news if vulnerabilities are found for the asset

### 3.4 Information disclosure

- SmartTVs
- Printer
- IOT gadgets

**Weaknesses:** These 'things' record confidential data e.g. video and audio could disclose sensitive information

**Mitigation:** Put devices on a separate network, keep assets software versions updated

- KidsGamerPCs
- Work pc
- Mobile devices

**Weaknesses:** Personal information, viewing habits, or sensitive data from apps could be exposed, particularly if devices communicate with external servers insecurely. If the VPN connection or the endpoint is insecure, an attacker might capture sensitive traffic or exploit vulnerabilities to extract confidential information.

**Mitigation:** Restrict and monitor software on asset, keep endpoint protection (e.g. Windows defender) on asset. Possibly move asset to a separate subnet if possible to protect the local network

- Router

**Weaknesses:** If the router or firewall is misconfigured or compromised, network traffic (including passwords or personal data) could be disclosed to attackers. Disabling SSL/TLS inspection may also lead to information leakage.

**Mitigation:** Keep router firmware up to date, and follow the news if vulnerabilities are found for the asset, do not disable security measures

### 3.5 Denial of service

- SmartTVs
- IOT gadgets

**Weaknesses:** These could be made unavailable by resource exhaustion or being overwhelmed by malicious traffic, rendering them unusable.

**Mitigation:** Put devices on a separate network, keep assets software versions updated

- WorkPC

**Weaknesses:** Attackers could target the work PC to disconnect it from the corporate network, potentially causing a loss of productivity. This could be done by overloading the VPN connection with traffic incentivizing user to bypass the VPN making traffic insecure.

**Mitigation:** Have patience, report the incident using a separate channel and do not bypass the VPN

- Router

**Weaknesses:** Attackers could flood the network with traffic (DDoS) to overwhelm the router or firewall, causing loss of internet access.

**Mitigation:** Keep router firmware up to date, and follow the news if vulnerabilities are found for the asset, do not disable security measures.

### 3.6 Elevation of privilege

- SmartTVs
- IOT gadgets

**Weaknesses:** Vulnerabilities in the firmware might allow attackers to take over the devices entirely, giving them control over camera feeds or other sensitive functions.

**Mitigation:** Put devices on a separate network, keep assets software versions updated

- WorkPC

**Weaknesses:** If attackers gain access to the work PC, they could potentially escalate their privileges within the corporate network. This poses a significant risk, especially if the work PC is not properly secured or if the attacker can exploit the VPN connection to gain broader network access.

- Router

**Weaknesses:** Gaining privileged access to the router could allow attackers to control traffic, including the VPN connection. They could potentially reroute sensitive corporate data or exploit the work PCs connection to the corporate network.

**Mitigation:** Keep router firmware up to date, and follow the news if vulnerabilities are found for the asset, do not disable security measures.

## 4 Conclusion

Following is identified by the analysis:

**Vulnerabilities:** Assets (IOT devices, Smart TVs, guests) with security properties that we have no control over are a potential security risk to the network (if exploited, they have full access)

**Mitigations:** Put uncontrolled devices on separate subnet(s), most home routers have a 'Guest' network feature that can be used. For things that need access to the protected areas, keep software up to date. A home network should be treated as de-facto 'zero trust' zone, and deploy endpoint protections if possible (turn on local firewalls). For the more advanced user, deploy network monitoring .

I Highly recommend using a tool for this (doing it manually is a bit of a chore). There is a lot of copy-pasting, of weaknesses and mitigations, automating the filling out of STRIDE items would also make it easier to keep tally of which weaknesses and mitigations occur the most. A disadvantage of using tools to do the analysis is that reporting often ends up with 'consultant' flavor to it, where everything is covered but conclusions are difficult to identify. I think it is important that the analyses are carried out by someone both familiar with the systems being modelled, and the models themselves.



## References

- [1] *OWASP Threat Modeling Project*. <https://owasp.org/www-project-threat-model/>. Accessed: 2024-10-5.
- [2] Wikipedia contributors. *PDCA — Wikipedia, The Free Encyclopedia*. <https://en.wikipedia.org/w/index.php?title=PDCA&oldid=1238104300>. [Online; accessed 6-October-2024]. 2024.
- [3] *Threat Modeling: 12 Available Methods*. <https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/>. Accessed: 2024-10-4.
- [4] *Examples of STRIDE threats for payment applications*. <https://medium.com/@arielhacking/examples-of-stride-threats-for-payment-applications-87a0ad0c3a21>. Accessed: 2024-10-5.

## Appendices