Recitation 10

Threat Modeling

Shreyans Sheth
July 29th, 2020

What and Why ?

- Threat modeling is the practice of identifying and prioritizing potential threats and security mitigations to protect something of value, such as confidential data or intellectual property.

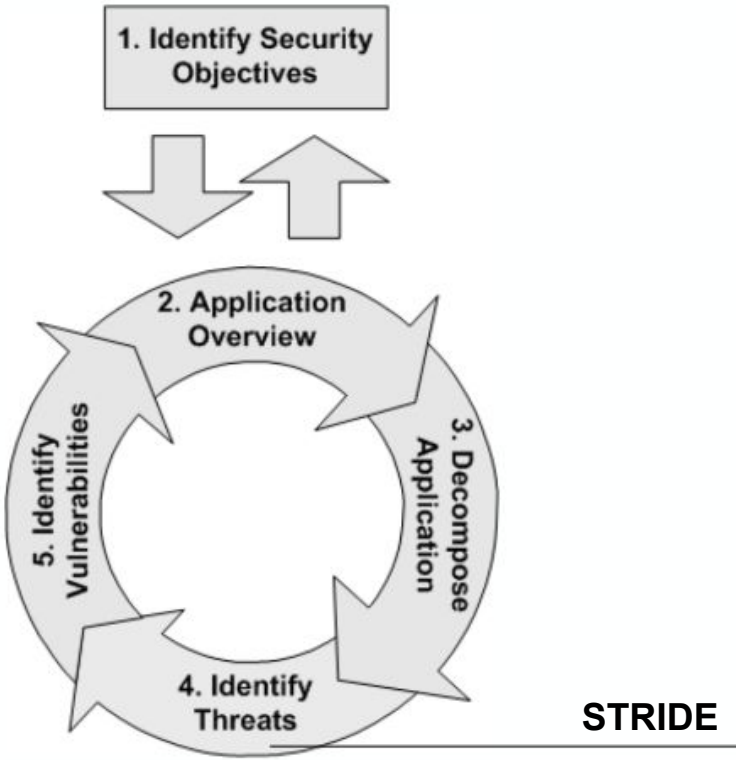
- By continuously threat modeling applications, security teams can better protect apps while educating the development team and building a culture of security throughout the enterprise.

STRIDE Modeling

- Used by microsoft for modeling threats before/while developing applications
- STRIDE++ - Poisoning (a model) and Evasion (AI confused by input)

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

How is STRIDE performed ?



- Decompose your system into relevant components
- Analyze each component susceptibility to the threats
- Mitigate threats and repeat.

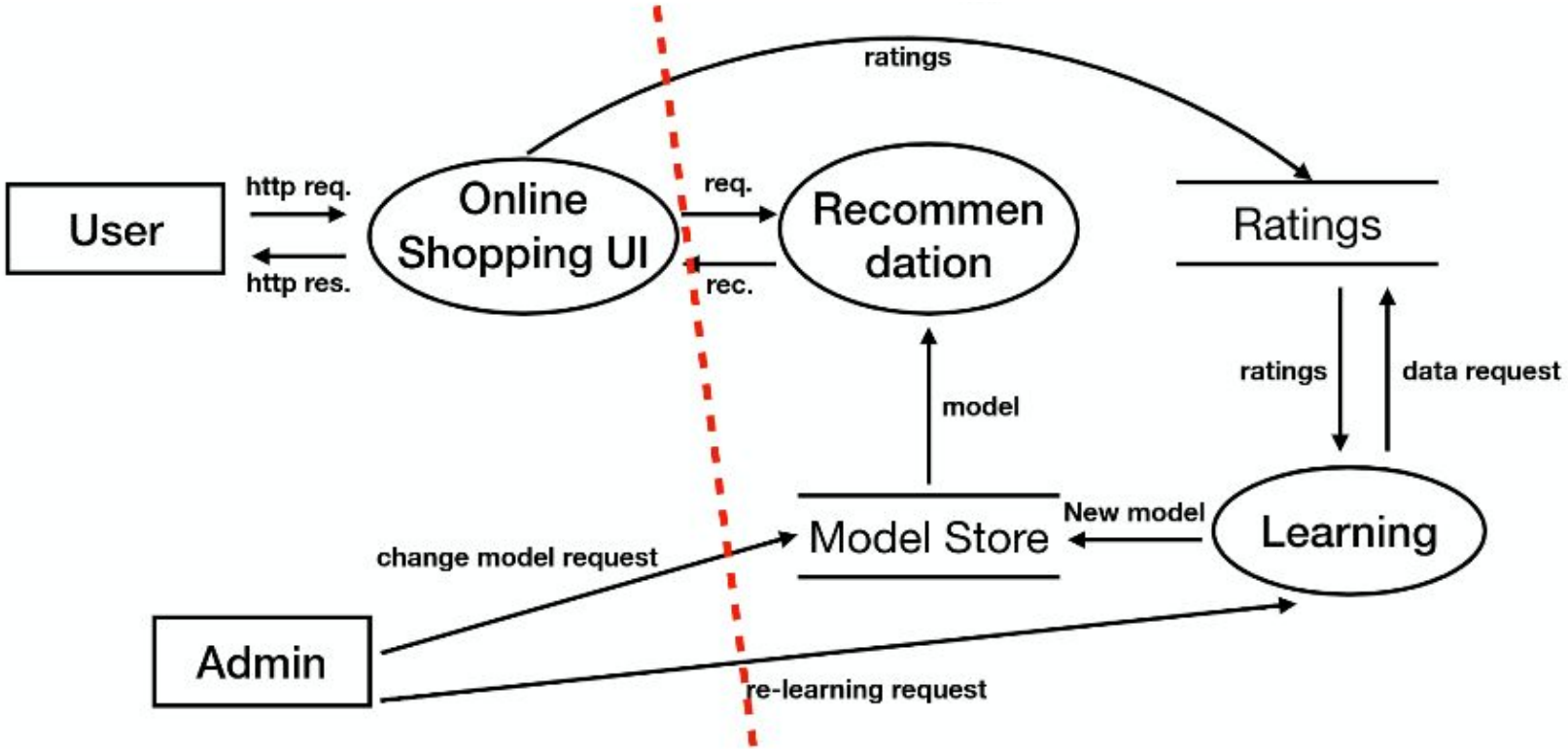
Scenario

- We have an Amazon like shopping platform
- The ML components in this system recommends products based on user’s ratings
- Several competitors for the same product

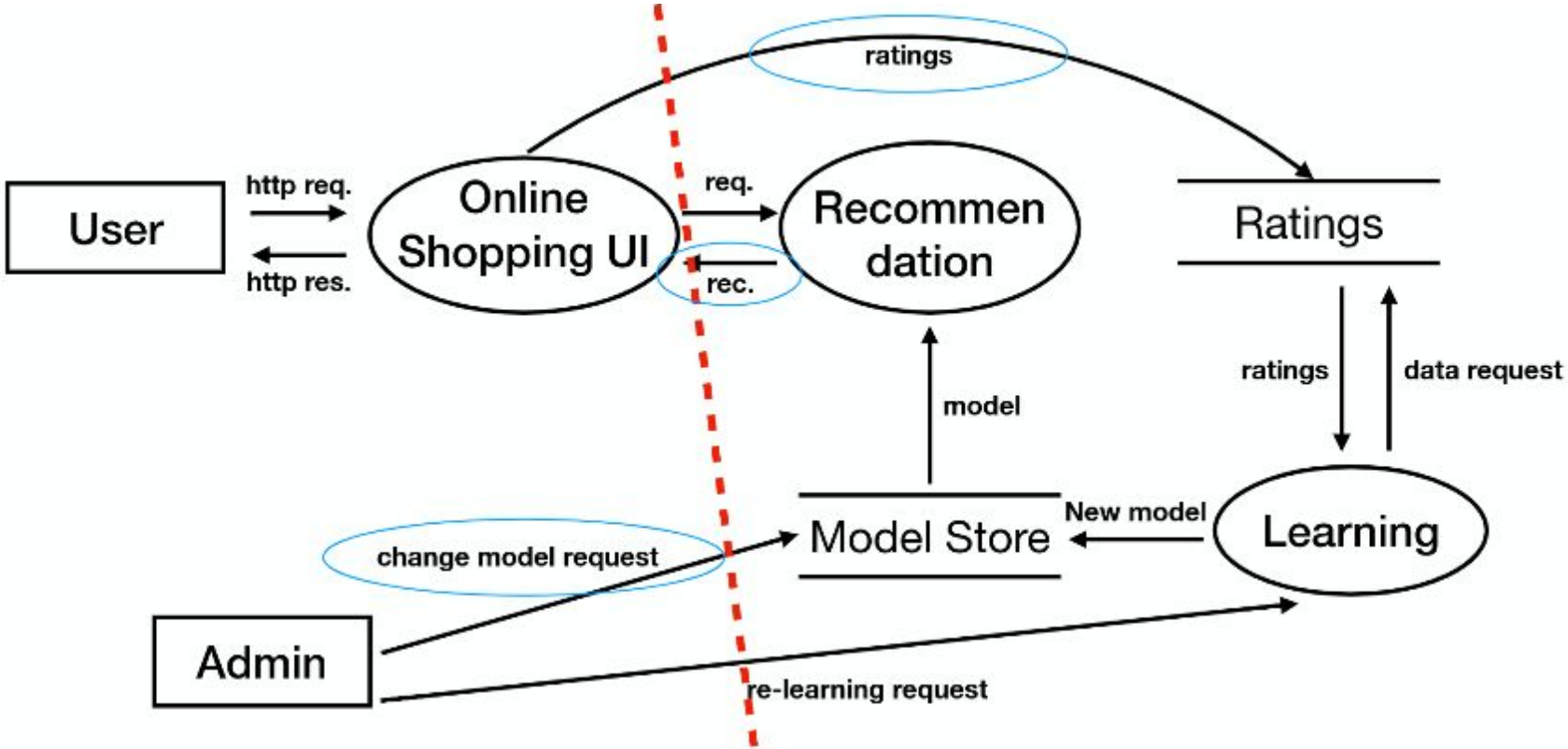
Security Threat

- The attacker’s goal is to favour certain products over others, in the system recommendations

STRIDE: Data Flow Diagram



STRIDE: Data Flow Diagram (Annotated)



Thanks!

References

1. Se4AI - 2019 (ChuPan Wong)
2. SEI - STRIDE Modeling