Threat Modeling Using STRIDE

STRIDE

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

STRIDE++

Spoofing

Tampering

Repudiation

Information disclosure

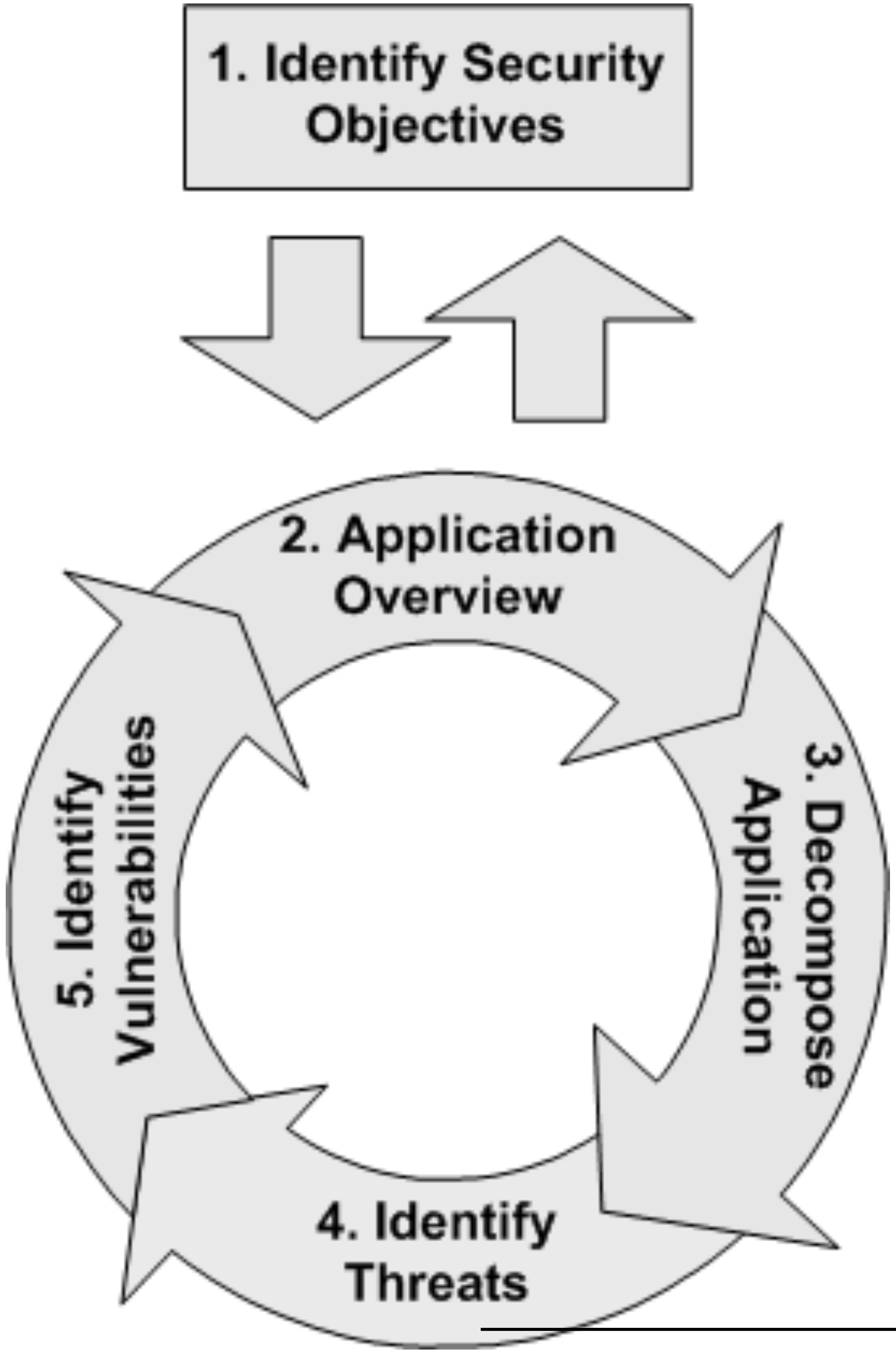
Denial of service

Elevation of privilege

Poisoning Attach

Evasion Attack

Why STRIDE?



STRIDE

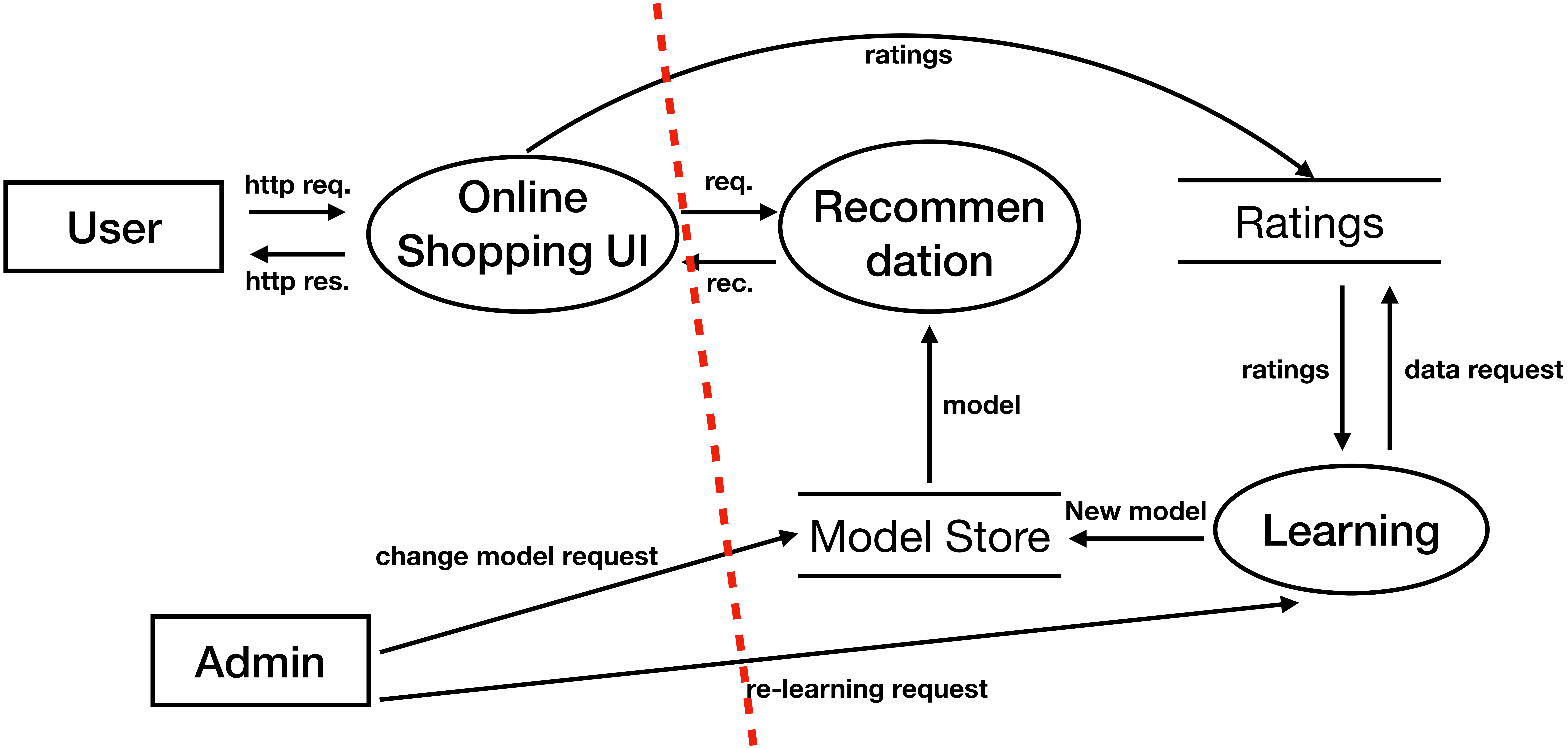
Scenario: Online Shopping Recommendations

- Amazon-like online shopping platform
- ML component recommends products based on users’ ratings
- Several competitors for the same products

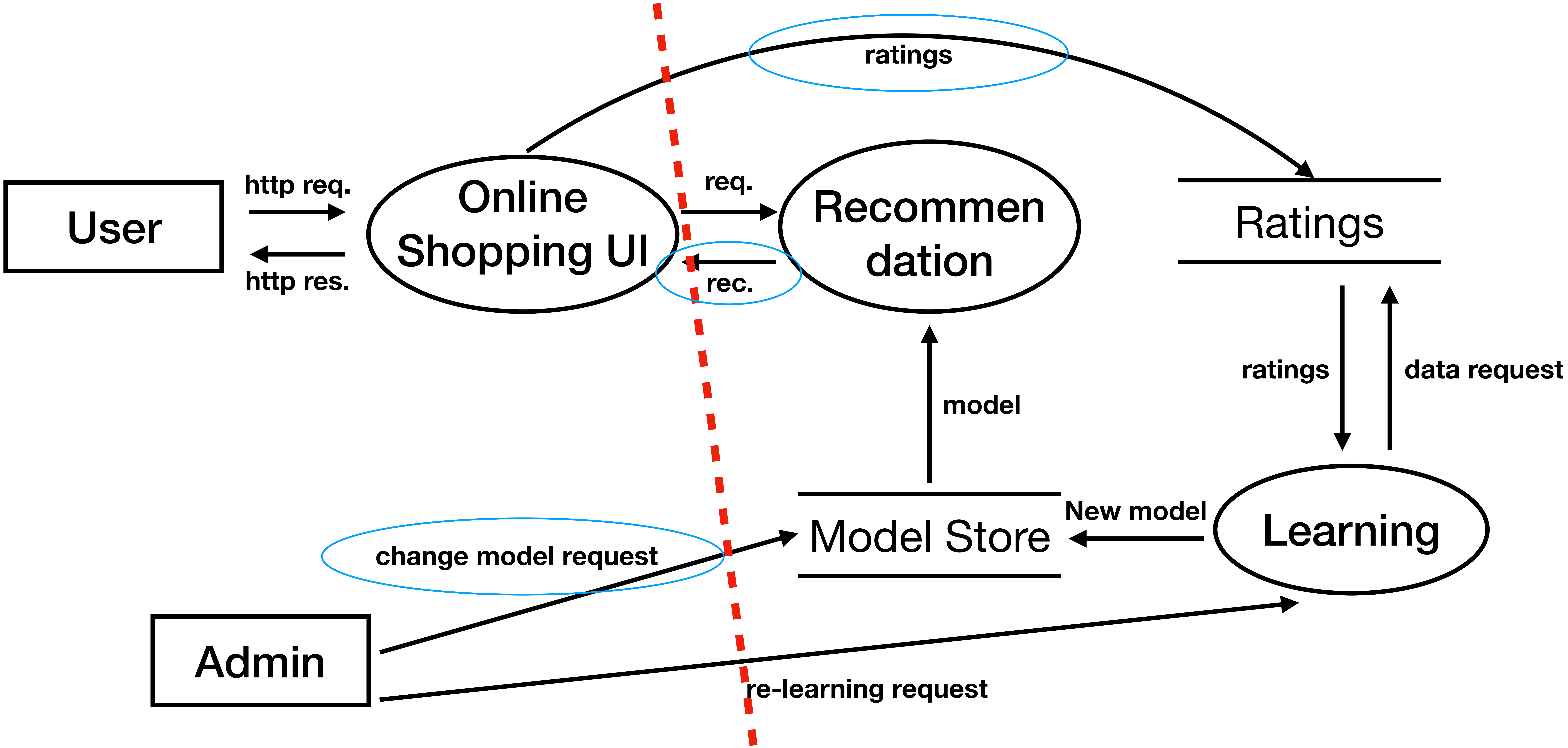
Attacker Goal

Attack the system to favor certain products in recommendations.

Data Flow Diagram



Data Flow Diagram



Have we covered all?

Spoofing

Tampering

Repudiation

Information disclosure

Denial of service

Elevation of privilege

Poisoning Attach

Evasion Attack