Threat model for Kubernetes high availability demo

Owner: Jakub Gorczynski
Reviewer: Marcin Ziolkowski, Mateusz Wasilewski
Contributors: Jakub Gorczynski
Date Generated: Sun May 19 2024

Executive Summary

High level system description

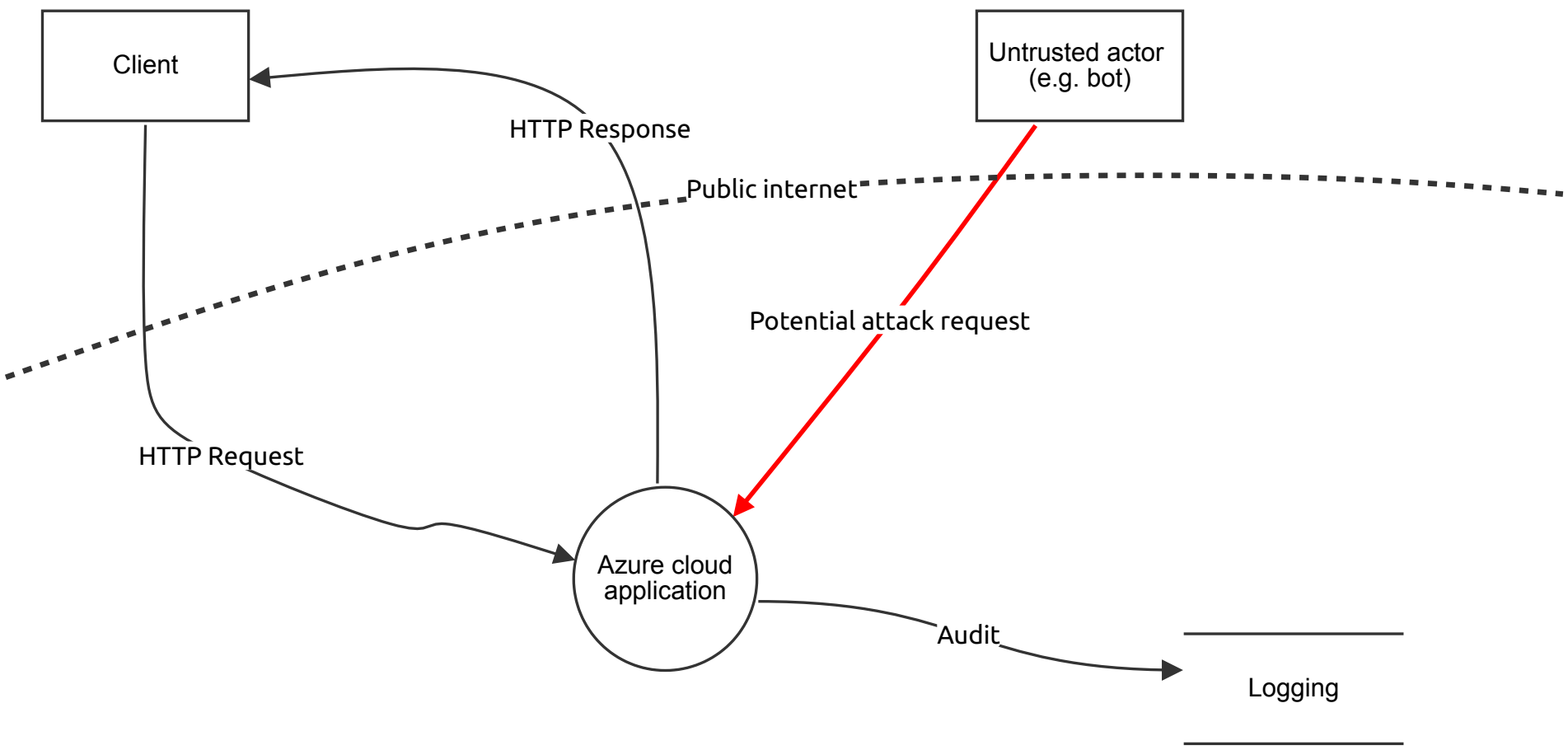
Application in a cloud on at least 3 simple types of microservices
Assumptions -
automation in infrastructure build and and setup – usage of a tools like Terraform, AWS CDK, Ansible, Chef, Puppet, etc -
control version system usage, like git, -
at least three types of microservices, -
database and state should be specific and owned by each microservice type separately, but it is required for exactly two types of microservices to have its own private mirror or cache of some subset of data/state owned as authoritative by other microservice type, to be used in scenarios when the strictly integral copy of these data subset is not necessary.
When the strict integrity for foreign data is still necessary, data should be reached by direct requests to the microservice owner of these data instead of usage of any local mirror or cache, -
authorization and session management, -
identities: administrator + identities federated via OAuth, for example with Google accounts, - user interface GUI (if you have any team member frontend oriented) -
monitoring of the service,
collecting all the logs -

Summary

Total Threats	2
Total Mitigated	1
Not Mitigated	1
Open / High Priority	0
Open / Medium Priority	1
Open / Low Priority	0
Open / Unknown Priority	0

resilient-six-stride

threat model of the service (using STRIDE framework)



resilient-six-stride

Client (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

HTTP Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	XSS	Tampering	Medium	Mitigated		Cross site scripting	Input sanitisation

HTTP Response (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Potential attack request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
0	New STRIDE threat	Tampering	Medium	Open		Provide a description for this threat	Provide remediation for this threat or a reason if status is N/A

Audit (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Azure cloud application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Untrusted actor (e.g. bot) (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Logging (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations