
OWASP 2024
GLOBAL
AppSec
CONGRESS CENTRE
LISBON
JUNE 24-28

OWASP 2024 GLOBAL AppSec | CONGRESS CENTRE LISBON JUNE 24-28

Paved Roads to Express RBAC in Threat Models

Eden Yardeni
Senior Security Engineer @ Samsara

A group brainstorming activity to proactively find risks in an application

Security team signs off on risks

Security team “approves” or “blesses” an application…whatever that means

Scenario: You’re The New PM At GlobalShop

“We're Worldwide So You Don't Have to Be”™

- A new fintech startup looking to integrate payment and banking services with local banks
- Your team is working on a feature that allows customers and bank employees to execute transactions
- You’d like assurances that your feature is safe before rolling it out

*** Bonus offer for new customers:** Deposit 500 ETH for exclusive access to our AI-driven Smart Investors Network™!

Scope

Scope

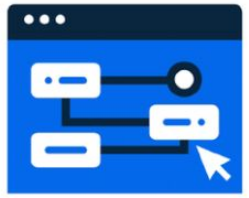
Identify the feature in scope for threat modeling.

Document

Write down any security or privacy-related concerns.

Decompose

Describe your feature in thorough technical detail.



Diagram

Create a dataflow diagram that describes how and what kinds of data are exchanged between components.

Enumerate

Use a framework to help think about potential threats to your feature.

Assign

Decide how to handle each threat and who should own it.

Application Decomposition, Massively Simplified

1.) Model the architecture
2.) Draw data flows
3.) Describe your users

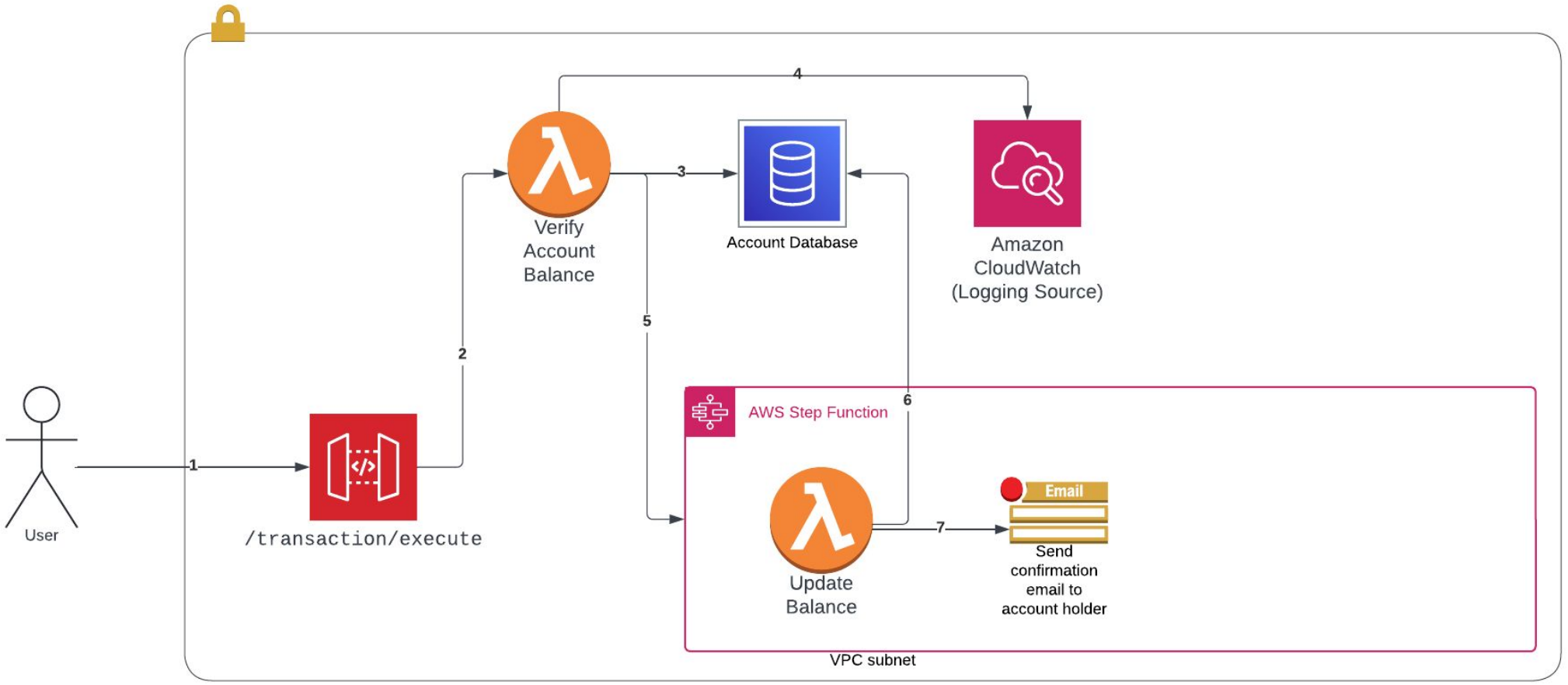
UcedaVélez, Tony, and Marco M. Morana. "Intro to PASTA." In *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, 2015. Hoboken, NJ: Wiley & Sons. ISBN 978-0470500965. Table 6.2.

Application Decomposition, Massively Simplified

1.) Model the architecture
2.) Draw data flows
3.) Describe your users

1.) Personas
2.) Service Accounts
3.) Identities + Authn methods
4.) Privileged functions

UcedaVélez, Tony, and Marco M. Morana. "Intro to PASTA." In *Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis*, 2015. Hoboken, NJ: Wiley & Sons. ISBN 978-0470500965. Table 6.2.


4
Verify Account Balance
3
Account Database
Amazon CloudWatch (Logging Source)
5
2
6
AWS Step Function
User
1
/transaction/execute
Update Balance
7
Email
Send confirmation email to account holder
VPC subnet

```
POST /v1/transactions/execute
Host: api.globalshop.com
Content-Type: application/json
Cookie: sessionId=67924acc-9f97-4599-a58d-6c500171b9d7
```

```
{
    "sourceAccount": "7b1b18c1-d7f0-41b4-bbec-e9d2b0f81417",
    "targetAccount": "8c56654c-6384-4f39-8078-50066de27cda",
    "branchId": 728,
    "amount": {
        "currency": "EUR",
        "value": 10000
    },
    "transactionType": "TRANSFER",
    "description": "Transfer to savings account",
    "emailToNotify": "some.jabroni@hotmail.com",
}
```

1.) Personas: User

2.) Service Accounts: IAM Roles

3.) Authn methods: SSO

4.) Privileged functionalities `/transaction/execute`

1.) Personas: User

2.) Service Accounts: IAM Roles

3.) Authn methods: SSO

4.) Privileged functionalities `/transaction/execute`

Core Properties

Endpoint
Principal
Action
Roles with access
Entity type
Domains providing access

Core Properties	Situational Properties	Dynamic Properties
Endpoint	Data Classification	Time of Access
Principal	Batch Domains Of	User Location
Action	Related Actions	Per-Object Sensitivity Level
Roles with access	Changes in Information Labels	Approval Status
Entity type	Changes in User Permissions	
Domains providing access	Additional Authz Checks	

Core Access Map: Constant properties about the action

Parameter	**Description**
Endpoint	`/transactions/execute`

Core Access Map: Constant properties of the action

Parameter	**Description**
Endpoint	`/transactions/execute`
Principal Type	User
Action Name	`transaction.execute`
Action Description	Allows executing financial transactions such as transfers, payments, and withdrawals.
Built-in Roles With Access	`Customer, BankTeller, BankManager, FinancialManagers`
Custom Roles With Access	`Auditor`
Entity Type	Transaction
Domains Providing Access	`account/728`, `branch/927`
Example Authorization Checks	- Customer: [`account/728, transaction.execute`] -Bank Manager: [`account/728, transaction.execute`]

Situational Access Map: Properties that might sometimes be relevant

Parameter	**Description**
Data Classification	Transactions involve personal financial data. Thus, all transactions are inherently sensitive.
Batch Domains Of	Group transactions by type (e.g., deposits, withdrawals, transfers) and treat differently based on risk profiles.
Related Actions	`transaction.validate, transaction.summarize`
Changes in Information Labels	Monitor changes in transaction status (e.g., pending, completed) and adjust access and notifications accordingly.
Changes in User Permissions	Dynamic adjustments based on transaction frequency, amounts, or suspicious activity patterns.
Additional Authz Checks	Multi-factor authentication for high-value transactions, additional approvals for unusual activities.

Dynamic Access Map: Properties that change at runtime

Parameter	**Description**
Time of access	Restrict transaction executions during off-hours for certain roles to minimize risk during low surveillance periods.
User location	Enable transactions only if the user's geographic location matches their registered bank or home address, unless explicitly approved.
Per-Object Sensitivity Level	Transactions that have been individually flagged must be withheld from certain roles.
Approval Status	Transactions should be immutable once their approval status is `In Review`.

Conclusions

- Threat models can be enriched with app decompositions that dive deep into user personas
- There are plenty of functional considerations about RBAC that might not make it into a traditional DFD
- Include product managers in threat modeling to make sure all those details get captured!
- And Access Maps are a handy way to structure all those details :)


OWASP 2024
GLOBAL
AppSec
CONGRESS CENTRE
LISBON
JUNE 24-28
THANK YOU