A Capability-based Distributed Authorization System to Enforce Context-aware Permission Sequences

ACM SACMAT 2022

Adrian Shuai Li
li3944@purdue.edu

Reihaneh Safavi-Naini
rei@ucalgary.ca

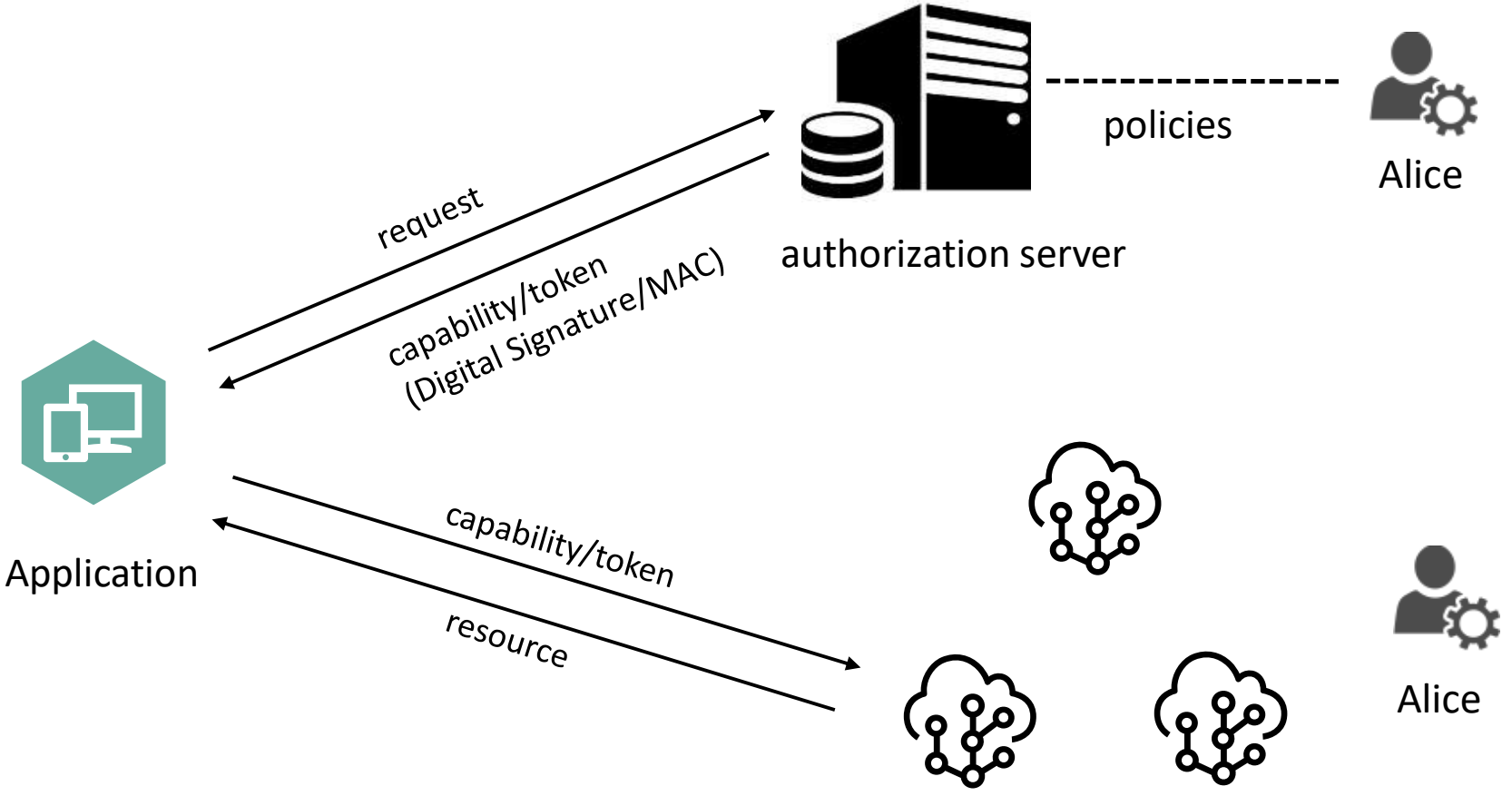
Philip W. L. Fong
pwlfong@ucalgary.ca

PURDUE UNIVERSITY | Department of Computer Science

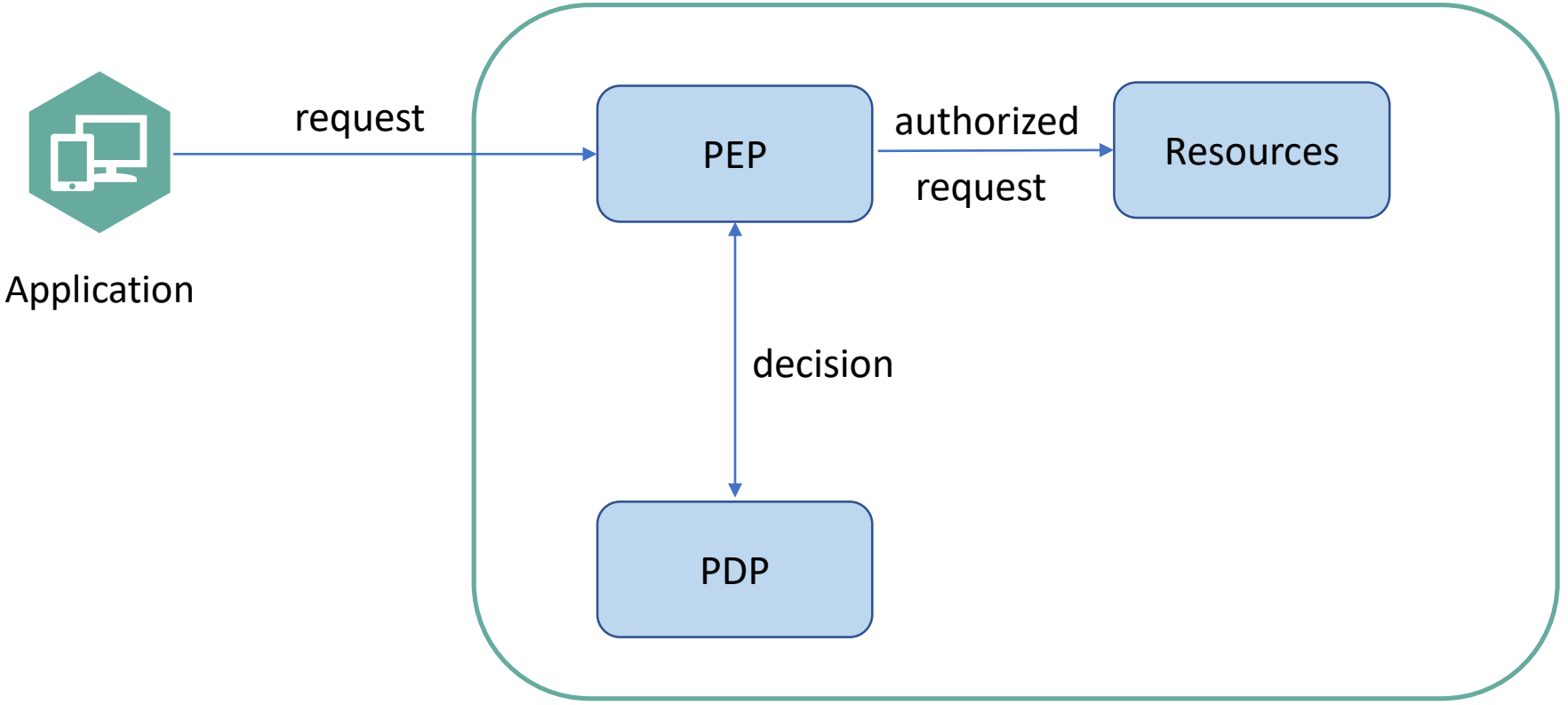
UNIVERSITY OF CALGARY

Capability-based distributed authorization

Protocols include OAuth 2.0 [H,2012], UMA [MCMH, 2016], ICAP [G,1989]



Centralized authorization systems



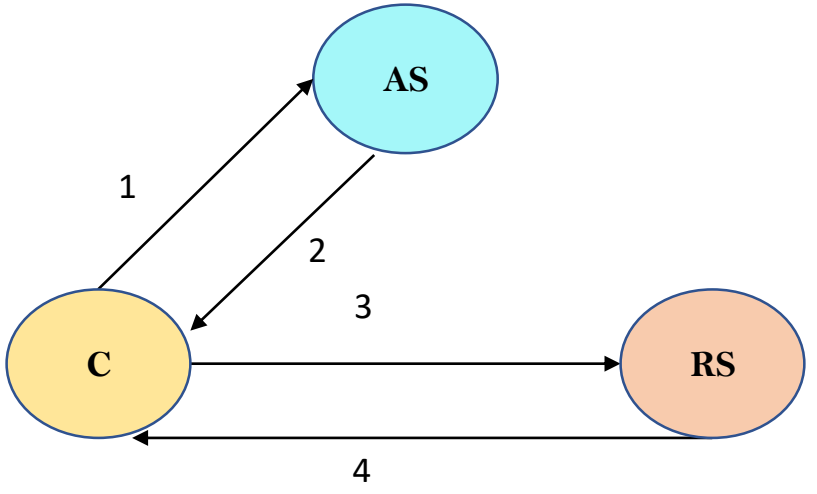
OAuth 2.0 and Proof-of-Possession Tokens

Two Legged OAuth*

1. $C \rightarrow AS$: ID_C, credentials, ID_{RS}
2. $AS \rightarrow C$: $Token$
3. $C \rightarrow RS$: $ID_C, Token$

$$Token = \left(t, auth_k(t)\right)$$

$$t = (ID_C, ID_{RS}, P, exp)$$



OAuth has been successfully used for authentication and authorization in mobile applications [CPCT, 2014] [SM,2014], and web services [FKS, 2016] [SB, 2012].

However, it is missing some important features.

The missing usage constraints

- Existing systems do not offer control over orderings of permissions
  - **Problem:** Delegated permissions can be exercised with arbitrary order
  - **Example 1:** decentralized business and financial systems:
    - Payment workflows require approvals of different authorities in a particular order.
  - **Example 2:** Industrial Control Systems (ICS)
    - The ordering of permissions to operate electronic equipment must conform to the workflow sequence

- Existing systems do not limit the number of permission use.
  - **Problem:** Delegated permissions can be exercised for unlimited number of times
  - **Security concern: unlimited access to critical assets**

- Existing systems do not support full “context” of access
  - Observation: access often depends on external conditions in the policies
  - Example: turn on the home camera when the user is not home

Enforcing permission sequences

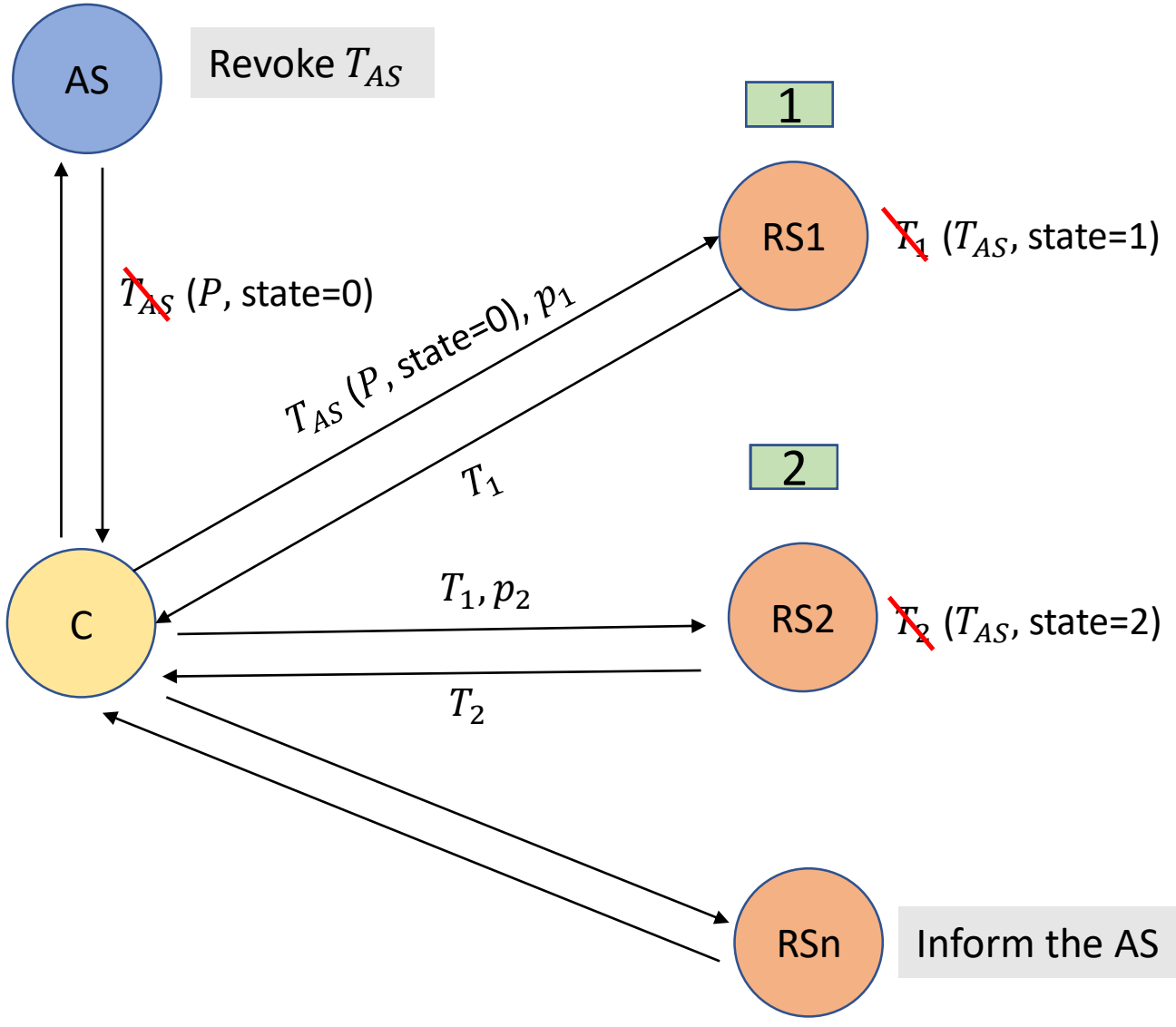
Our contributions

- Theoretical
  - Proposed an efficient method of enforcing permission sequences with proof
    - HCAP supports history-based access control [TFS, 2018]
    - Less overhead, context-aware
  - Our capability-based system includes the “context” of access
    - Integrate a context server called Environmental Situational Oracle (ESO) [SST, 2018],
    - An ESO encapsulates the implementation of how a situation is sensed, inferred, or actuated
    - Our security proof is still valid with the addition of context confinement
- Practical
  - Implemented our capability system as an extension of the OAuth framework
  - Showed how our proposed system can strengthen OAuth to enforce context-aware permission sequences in distributed financial systems

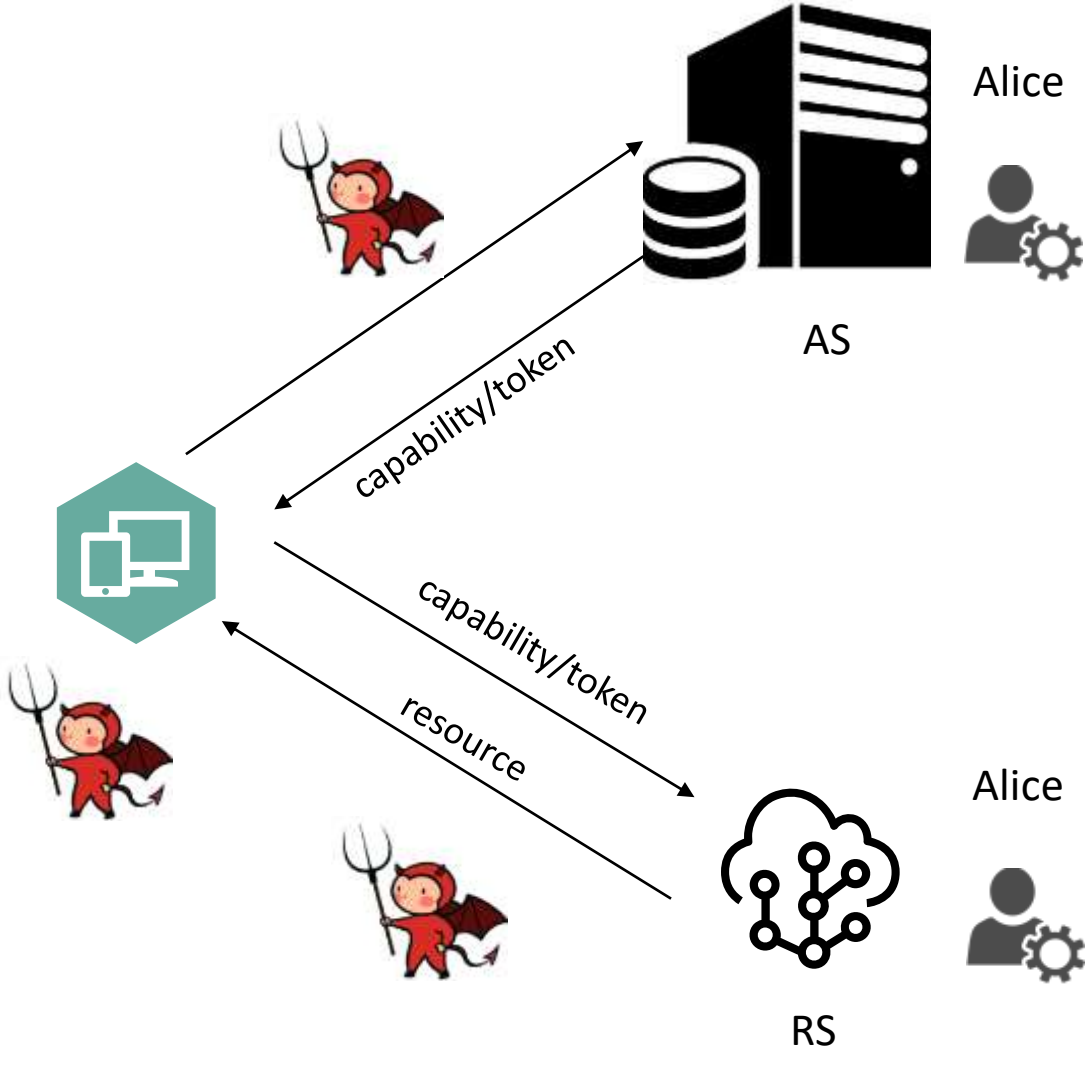
- Performance Evaluation
  - Competitive performance compared with OAuth 2.0

Permission Sequence

$P: p_1 p_2 p_3 p_4 \cdots p_n$

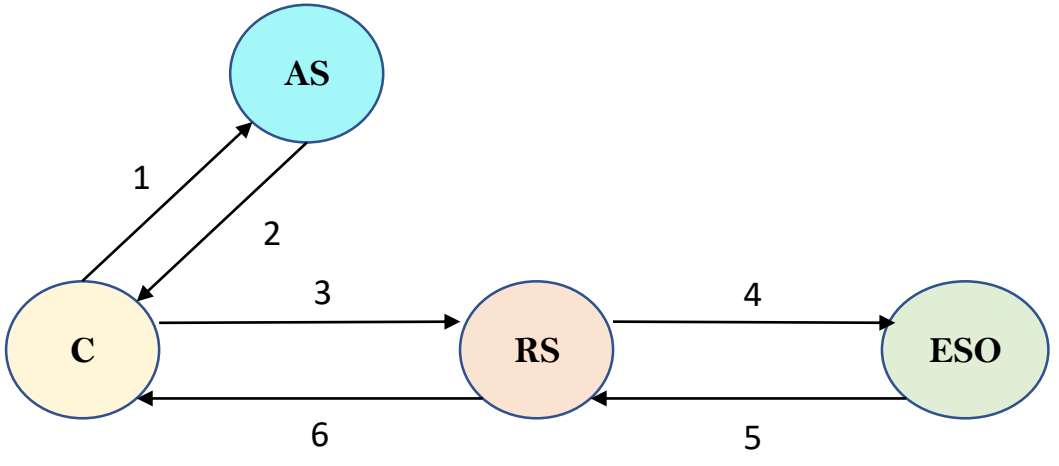


Adversary model and Attacks



- Token forgery and tampering
  - Digital Signature
- Token theft
  - Proof-of-possession tokens
- Client Impersonation
  - Public-key based client authentication
- Replay attack
  - Proof of safety property

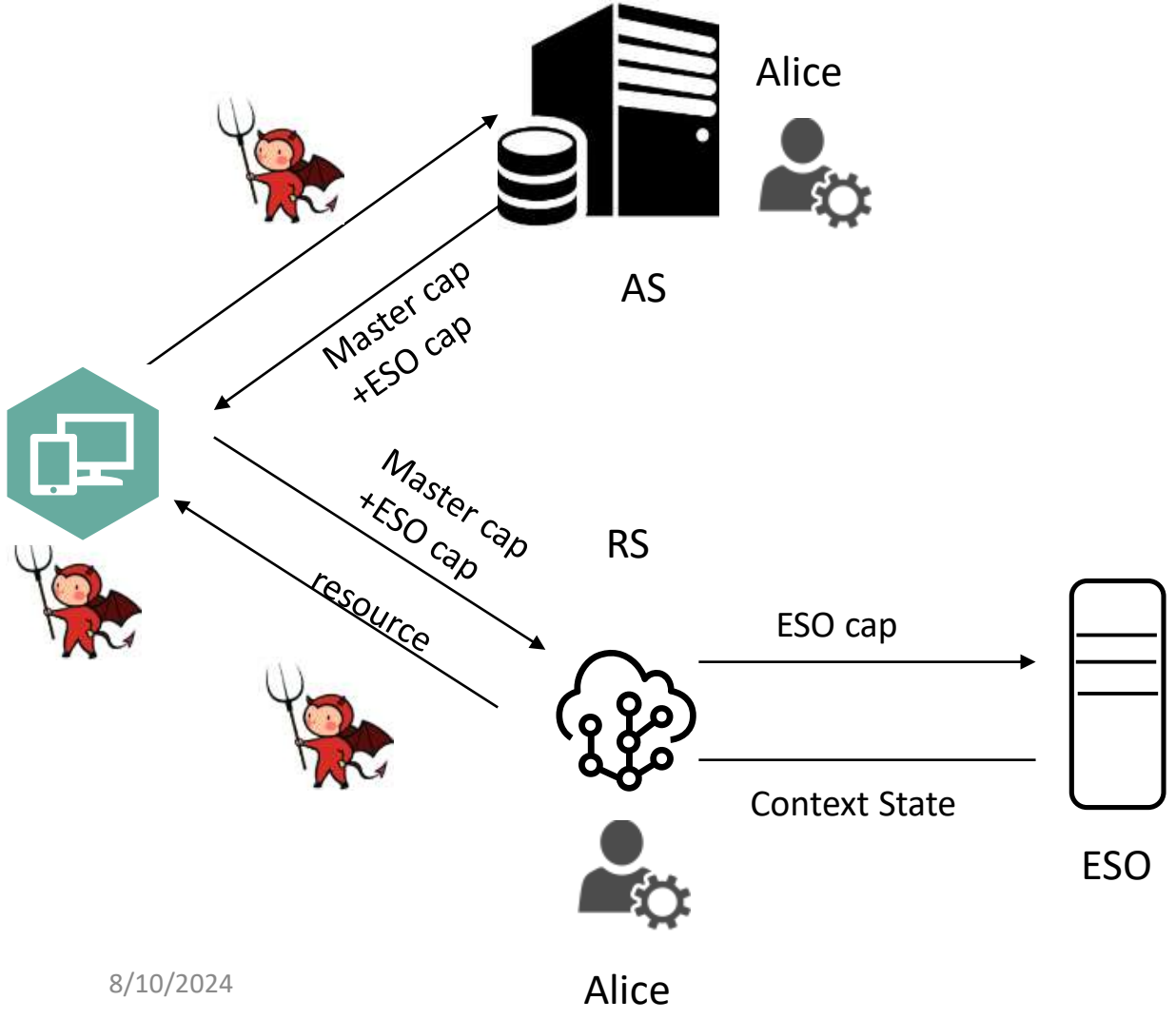
Context Awareness



ESO: environmental situation oracle [SST, 2018]

1. Request master token and ESO token
2. Get tokens $T_{AS}, T_{ESO}(H(T_{AS}))$
3. Request for service by presenting tokens together
4. Request for situation state using ESO token
5. Return ESO state Y/N
6. Provide service/return failure

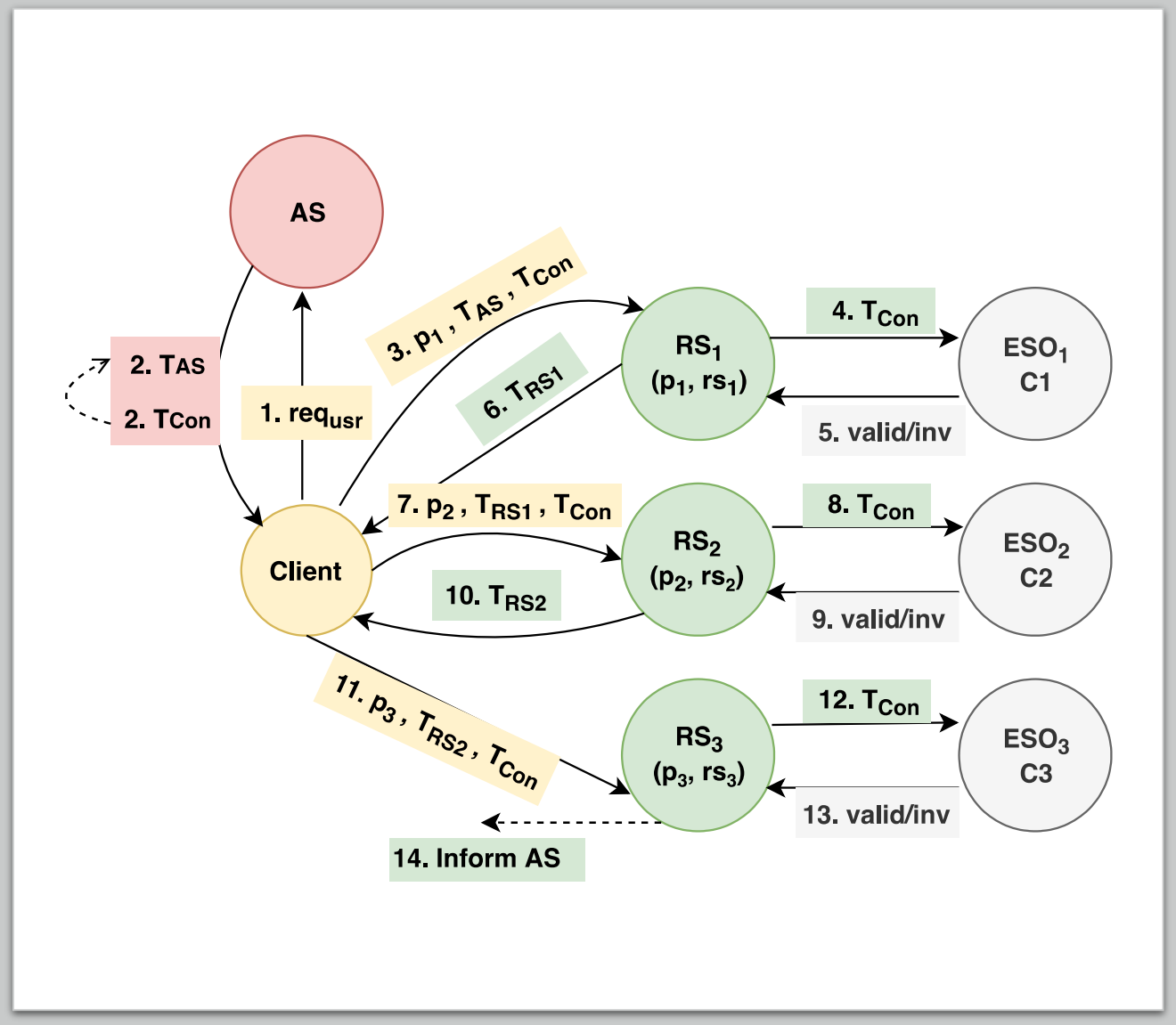
Adversary model and Attacks



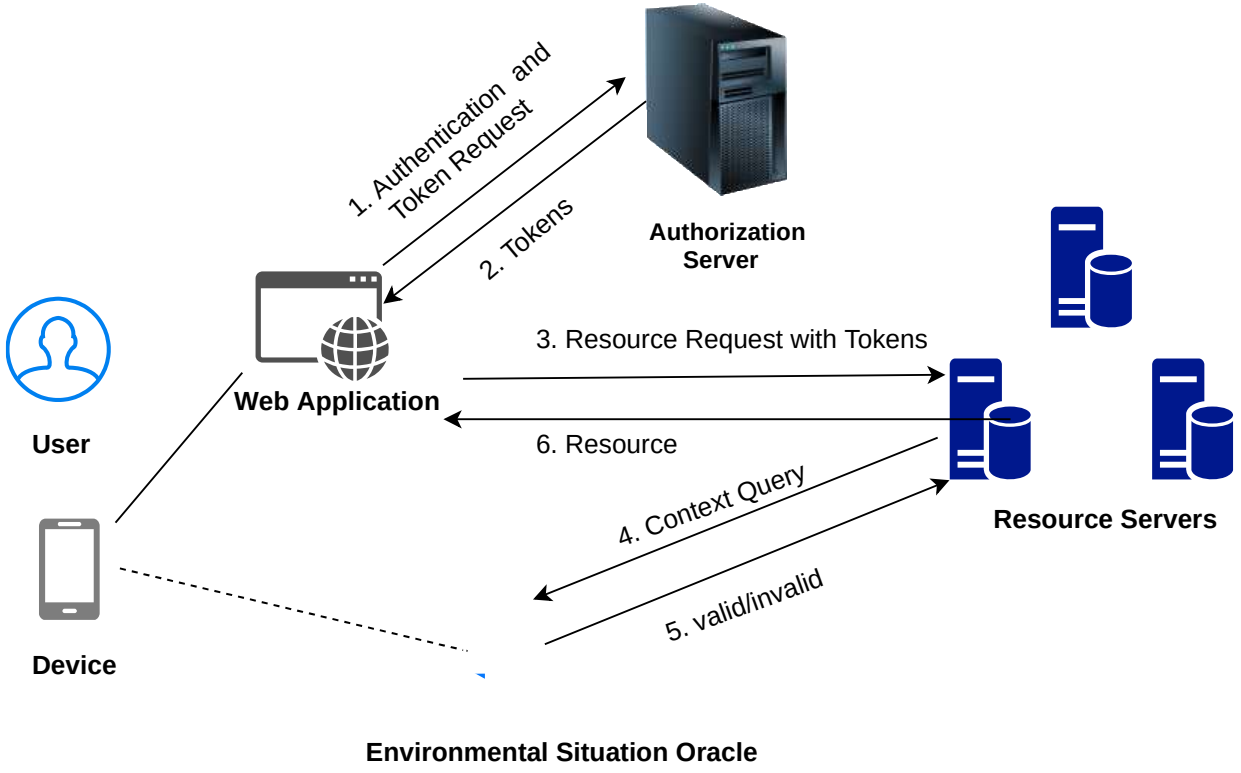
- Token forgery and tampering ✓
- Token theft ✓
- Client Impersonation ✓
- Replay attack ✓
- **Client impersonates as RS**
  - RS Authentication

Generic flow diagram of our system

- ➞ fast revocation
- ➞ One time interaction with the AS per session
- ➞ Lightweight computation on the RS
- ➞ Verifiable integrity
- ➞ Inability to violate the permission sequence by replaying tokens.



Implementation – OAuth extension



- OAuth client credential grant with proof-of-possession tokens.
- We implement ABAC as the authorization mechanism in the AS.

Use case

Alice uses Application B that requires a paid membership. Application B offers Alice the option to pay her membership monthly using her credit card. Alice authorizes her credit card company to pay the application fee under the following conditions.

Application B can make once a month $10 charge to Alice's account, under the condition that Alice has been using Application B for the past two months.

Thus a payment request will be rejected in the following cases,

- Application B is requesting an amount different from $10.
- Application B is charging $10 to Alice's account for the second time in the same month.
- Alice has stopped using Application B, but she has not canceled her subscription.

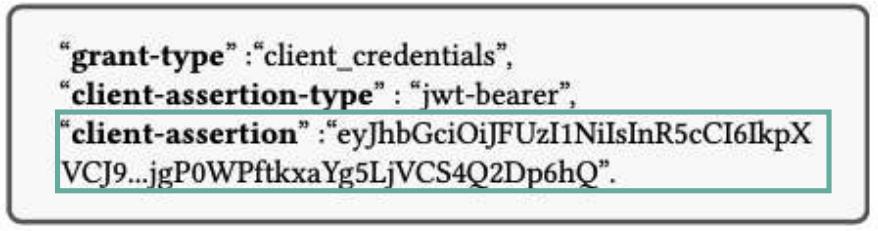
This last case will be detected by monitoring access to the application.

Solutions – policy example in JSON

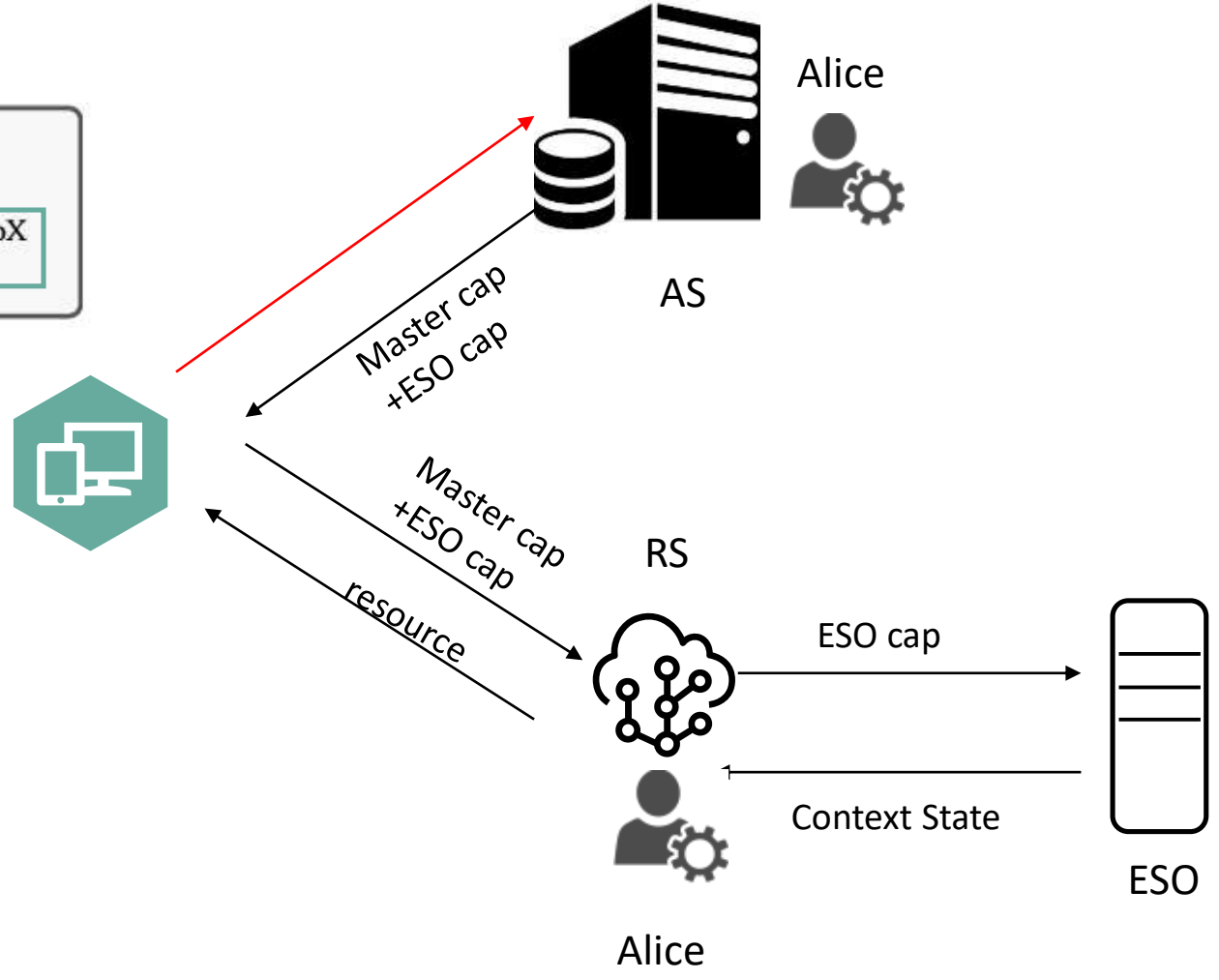
```
{
    "type":"ABAC policy",
    "name":"ApplicationServiceCharge",
    "application":"Payment",
    "rules":{
        "subjectAttribute":{
            "ApplicationID":["B"]
        },
        "objectAttribute":{
            "resourceType":["balance"],
            "resourceID": "Alice"
        },
        "authorization":"permit",
        "actionAttribute":{
            "actions":["charge"],
            "amount": "$10",
            "frequency": "monthly"
        },
        "environmentcontext":["used_within_two_months"],
        "Default":{
            "authorization":"deny"
        }
    }
}
```

Application B can make once a month $10 charge to Alice's account, under the condition that Alice has been using Application B for the past two months.

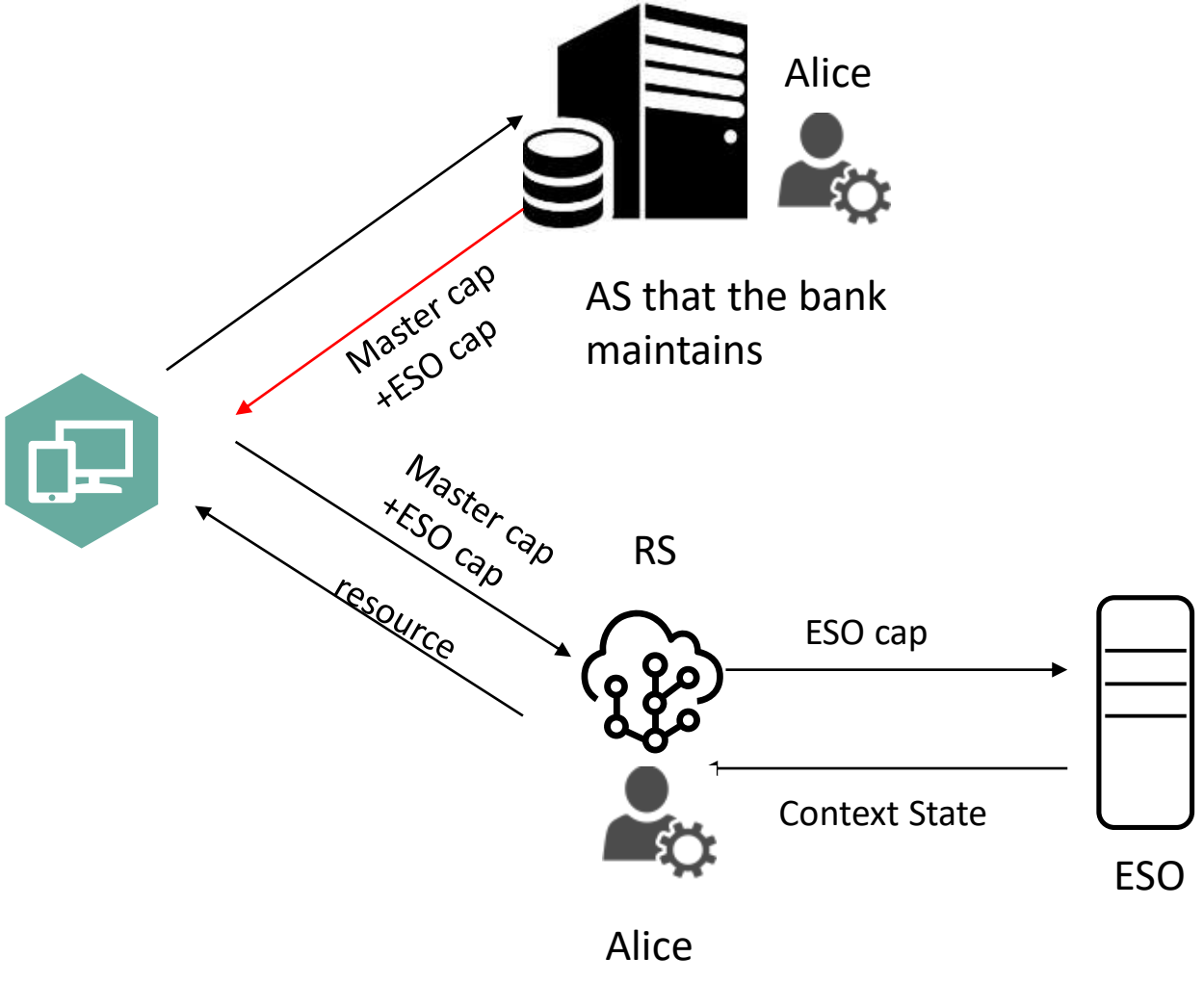
Solutions – policy example in JSON



```
{
    "client_id":"B",
    "issuer":"ApplicationB",
    "application":"Payment",
    "objectAttribute":{
        "resourceType":["balance"],
        "resourceID": "Alice"
    },
    "structured_scope":{
        "actions":["charge"],
        "amount": "$10"
    }
}
```



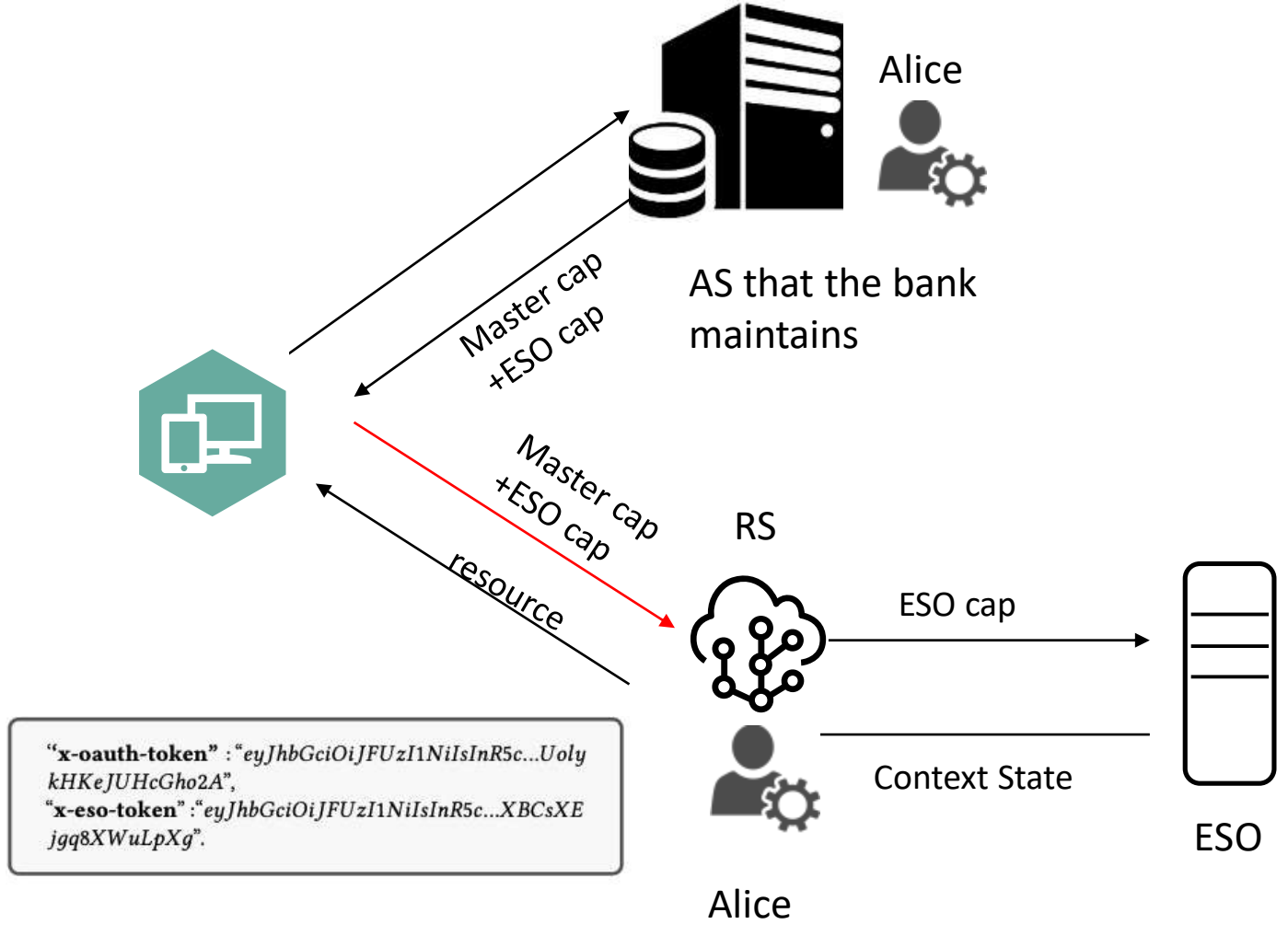
Solutions – policy example in JSON



"x-oauth-token" :"*eyJhbGciOiJFUzI1NiIsInR5c...Uoly kHKeJUHcGho2A*",
"x-eso-token" :"*eyJhbGciOiJFUzI1NiIsInR5c...XBCsXE jgq8XWuLpXg*".

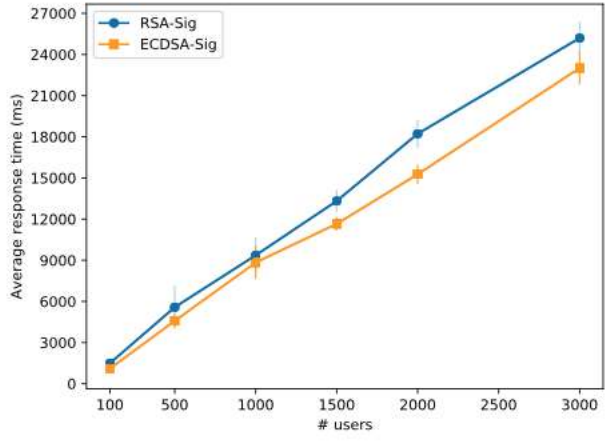
```
{
    "expireIn":"1 day",
    "hashAT":{
        "words":[
            1904756807,
            -1499235065,
            -860331953,
            -1557528208,
            -355723369,
            -1355021346,
            -70944964,
            -653925533
        ],
        sigBytes":32
    },
    "subject":"https://localhost:4990/Alice/balance",
    "audience":"https://localhost:4995/used_within_two_months",
    "issuer":"https://localhost:5000/authorization",
    "action":["read"],
    "userID": "Alice",
    "environmentContext":["used_within_two_months"],
    "iat":1567468693
}
```

Solutions – policy example in JSON

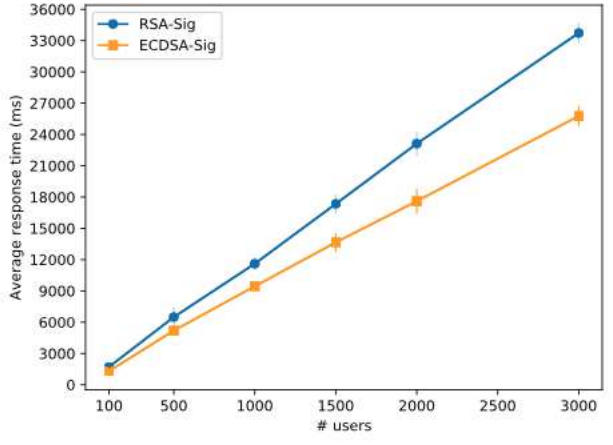


track Alice's login history of App B in the past two months.

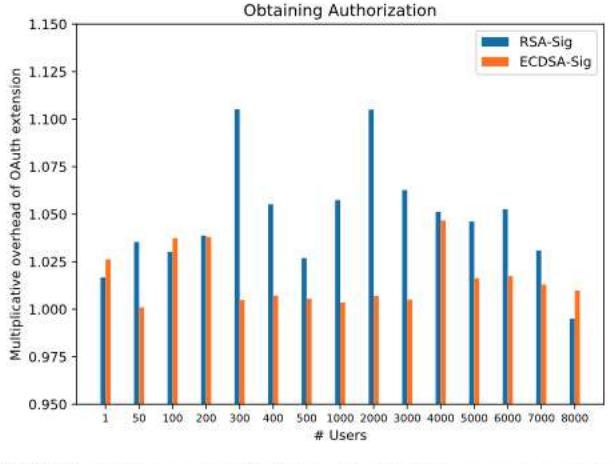
Performance Evaluation



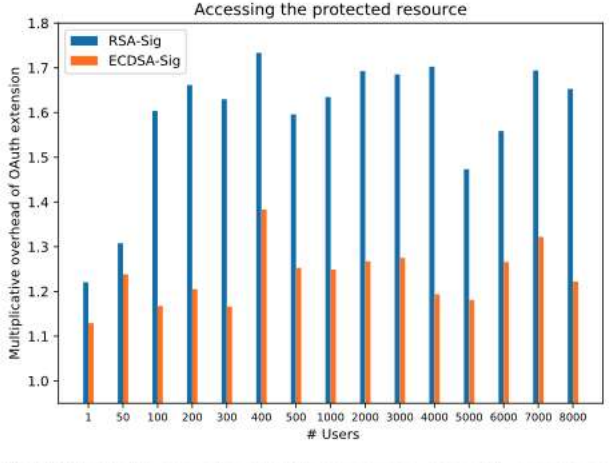
(a) Average response time (in milliseconds) for authorization request through our system with 95% confidence interval.



(b) Average response time (in milliseconds) for the resource request through our system with 95% confidence interval.



(c) Multiplicative overhead of the authorization request: average response time in our system compared to OAuth.



(d) Multiplicative overhead of the resource request: average response time in our system compared to OAuth.

Future work

- Enforcing the other history-based policies using minimum state.

- we will consider an honest but curious RS and ensure that the RS can not passively/actively learn more information about the user and their surrounding environment.

References

[TFS, 2018] L. Tandon, P. W. Fong, and R. Safavi-Naini. Hcap: A history-based capability system for iot devices. In Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies, pages 247–258. ACM, 2018.

[GPR,2013] S. Gusmeroli, S. Piccione, and D. Rotondi. A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling, 58(5-6):1189–1205, 2013.

[HJMS, 2016] J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta Gómez. Dcapbac: embedding authorization logic into smart things through ecc optimizations. International Journal of Computer Mathematics, 93(2):345–366, 2016.

[SST, 2018] R. Schuster, V. Shmatikov, and E. Tromer. Situational access control in the internet of things. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 1056–1073. ACM, 2018.

[CPCT, 2014] E.Y.Chen, Y.Pei, S.Chen, Y.Tian, R.Kotcher, and P.Tague.OAuthdemystifiedfor mobile application developers. In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security, pages 892–903. ACM, 2014.

[SM, 2014] M. Shehab and F. Mohsen. Towards enhancing the security of OAuth implemen- tations in smart phones. In 2014 IEEE International Conference on Mobile Services, pages 39–46. IEEE, 2014.

References

[FKS, 2016] D. Fett, R. Küsters, and G. Schmitz. A comprehensive formal security analysis of OAuth 2.0. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 1204–1215, 2016.

[SB, 2012] S.-T. Sun and K. Beznosov. The devil is in the (implementation) details: an empirical analysis of OAuth SSO systems. In Proceedings of the 2012 ACM conference on Computer and communications security, pages 378–390, 2012.

Thank you!

Questions?

Email: li3944@purdue.edu