I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Safety and Consistency of Subject Attributes for Attribute-Based Pre-Authorization Models

Fall C-SPECC Scholar Seminar
Presented by: Mehrnoosh Shakarami
PhD Supervisor: Professor Ravi Sandhu

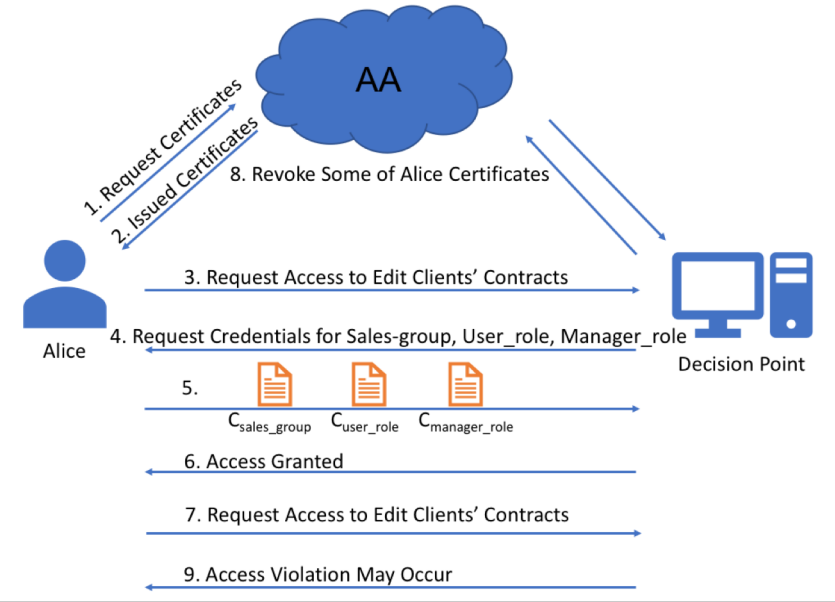
Institute for Cyber Security (ICS)
Center for Security and Privacy Enhanced Cloud Computing (C-SPECC)
Department of Computer Science
University of Texas at San Antonio

Introduction

- Access control imposes restrictions on subjects' access to protected objects according to specified policies.
- In Attribute-Based Access Control (ABAC), policy decision point makes authorization decisions based on evaluating attribute values of subjects, objects and environment with respect to a policy, which are exposed to change over time.
- Due to following challenges, the resulting decision may be incorrect in allowing access which should be denied or denying access which should be allowed. We call this the safety and consistency problem.
  - Asynchronous nature of distributed systems.
  - Cached values of attributes.
  - Network and system failures which makes attribute authorities unreachable.

Motivating Example

- Incremental assembly of subject attributes along with differing validity periods for subject attribute values, raises the potential for inconsistency of subject attribute values at the decision point.
- So, we may need multiple revocation checks for credentials, especially for long-lived ones.

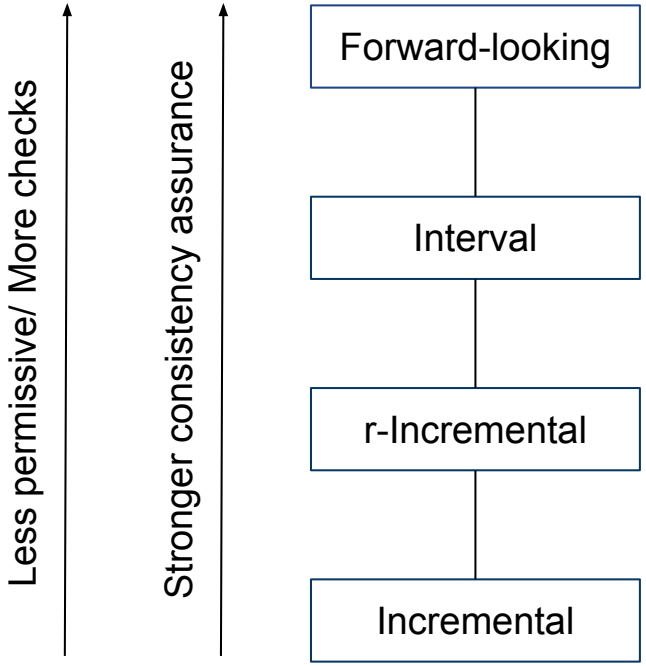


Problem Statement

Symbol	Meaning
c_i	i^{th} credential
t_{req}	request time
t_d	decision time
t_e	enforcement time
t^i_{start}	start time of c_i
t^i_{end}	end time of c_i
$t^i_{r,k}$	time of k^{th} revocation check for c_i
$t^i_{r,max}$	last time of revocation status check for c_i
t^i_{revoc}	actual revocation time for c_i (if any)

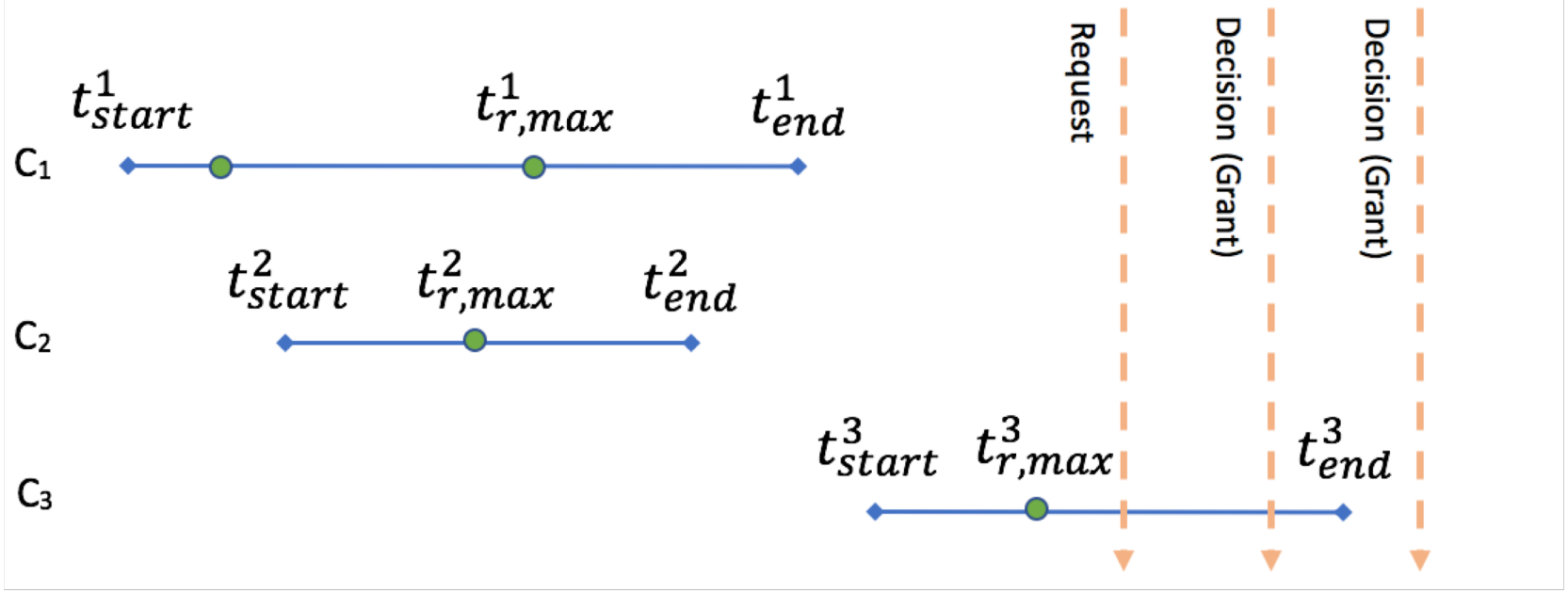
Consistency Levels

- We proposed four increasingly powerful consistency levels which provide the decision point more safety and consistency by applying more restrictive constraints on timing and sequencing of attribute revocation checks:



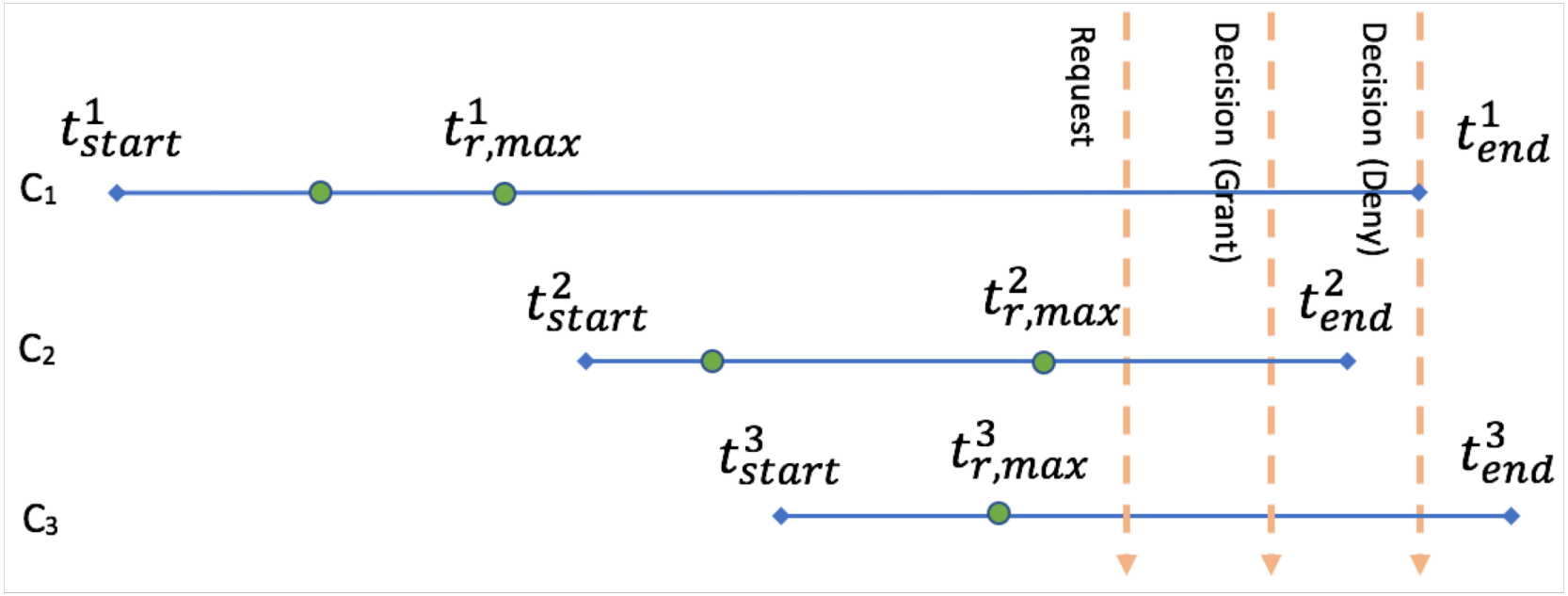
Incremental Consistency

- This level is the most permissive. It only requires each relevant credential be validated by a revocation check before being relied upon in an access decision.



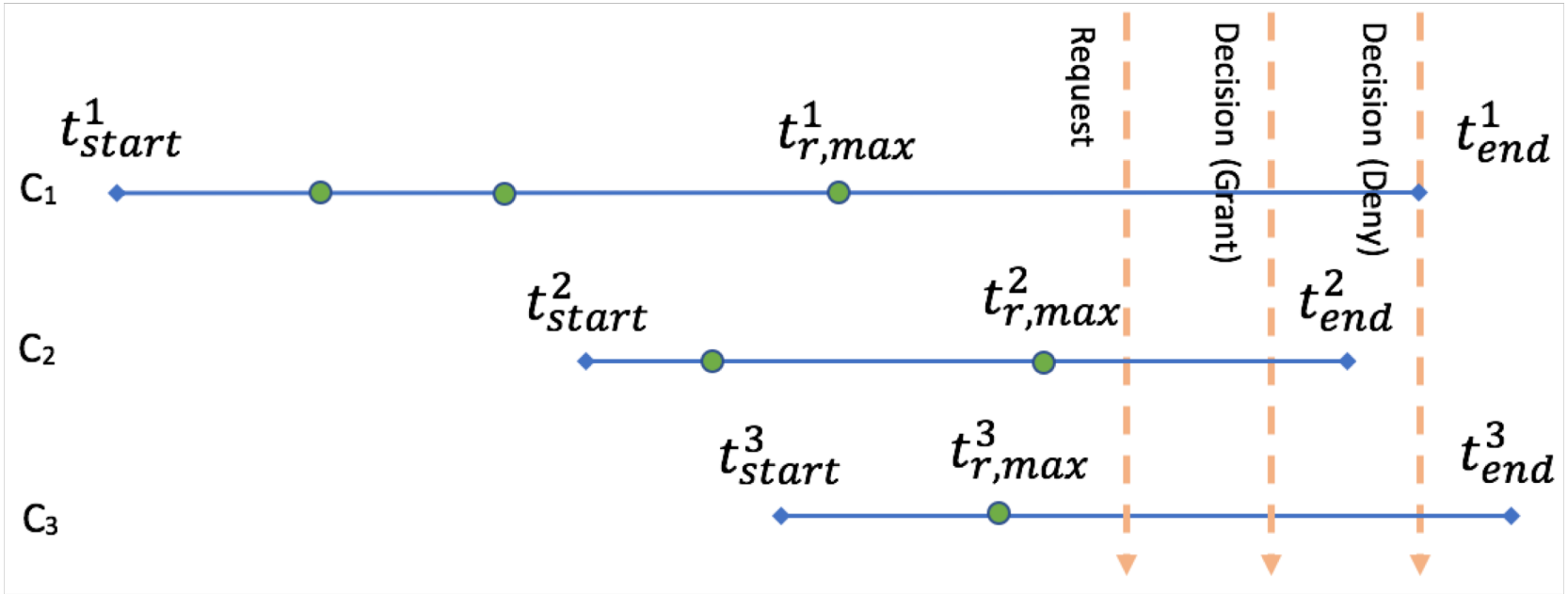
Restricted Incremental Consistency (r-Incremental)

- In the second level, we restrict the decision time to happen necessarily in lifetime interval of all relevant credentials. As opposed to the previous level, in this level if any of the relevant credentials has been expired the access request would be denied.



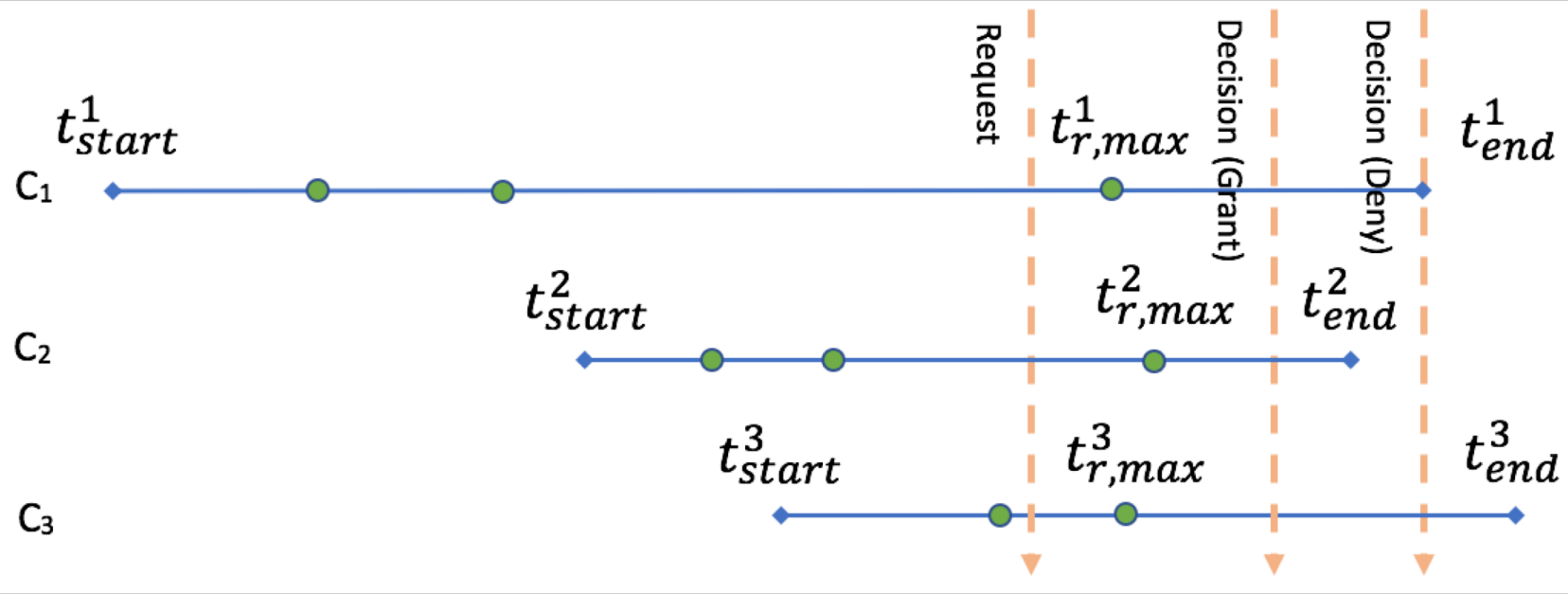
Interval Consistency

- We impose restrictions on the latest revocation check of all relevant credentials to happen after all relevant credentials have been started and before any of them ends, prior to decision time. So, all relevant credentials are unrevoked simultaneously (at least) at one point in time.



Forward-looking Consistency

- In this level, we need stronger constraints on the latest revocation check time for relevant credentials to make sure that all of them have been valid simultaneously at some point after the *request time.*



Discussions

- Our proposed levels of consistency could be applied in any of following real-world scenarios:
  - **Short-lived vs. long-lived credentials:** In case of long-lived certificates, it is needed to rely on Certificate Revocation Lists (CRL) or Online Certificate Status Protocol (OCSP) to obtain information about certificates' revocation status. In case of short-lived credentials there would be only one revocation check which happens when the certificate has turned in.
  - **Different revocation scenarios:** different scenarios ranging from no actual revocation to revocations which have not been revealed is possible, none of which would hinder applying our consistency levels. Our approach guarantees that a credential which has known to be revoked would not be used in decision making process.
  - **Considering enforcement time:** enforcement time could be used to propose stronger levels of consistency.

Conclusion

- We provide added foundational rigor and precision which is essential in a critical aspect of attribute-based access control to restrict the exposure of an ABAC decision point to outdated information, which may result in access violation.
- The notion of request time is new in our work to guarantee higher safety assurance.
- We make assumptions which provide more precise definition of safety and consistency and provide a totally ordered relationship among levels.
- From a practical point of view, implications in the con- texts of short-lived and long-lived credentials and different real-word revocation scenarios are discussed.