security

basics

- dependability, to justify trust in delivering services

  confidentiality: information is disclosed only to authorized parties

  integrity: alterations to asset can only be made authorized

- security

  three broad classes of threats: CIA

  - Confidentiality,
  - Integrity,
  - Availability (no unauthorized denial of use)

- security policy vs. security mechanism
  - policy: which actions are allowed / prohibited
  - mechanism: utilized to enforce the security policy

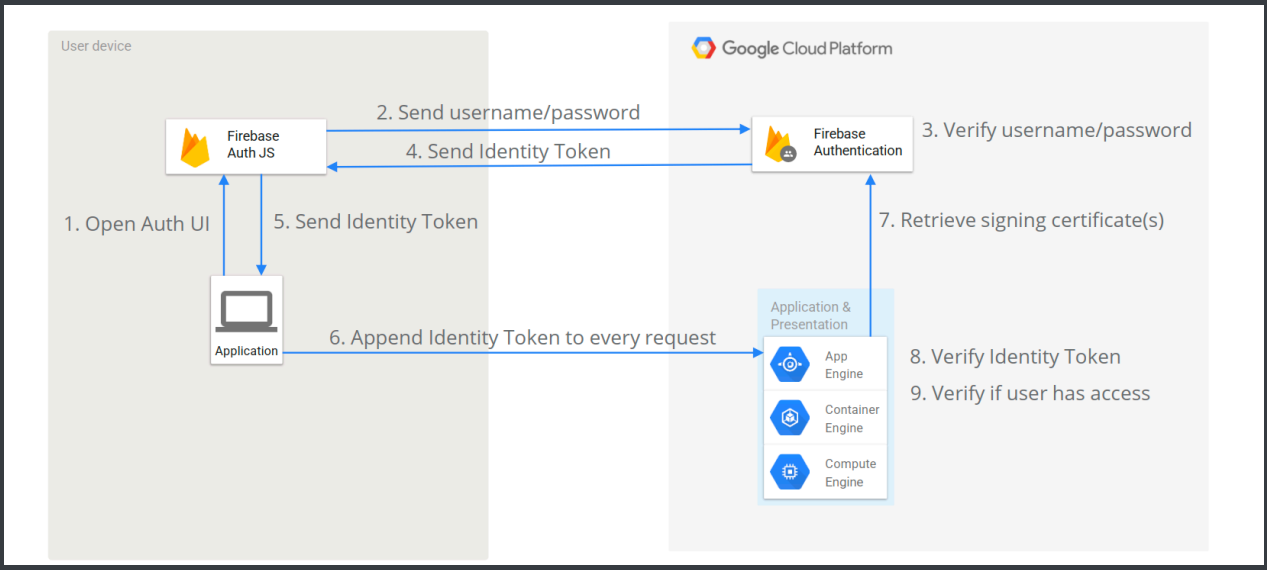
  比如policy是只有授权用户才能访问保险箱，mechanism是用指纹识别来确保...

  major concern 1: policies typically evolve

- mechanisms
  - encryption,
  - **authentication**, to verify the claimed identity

    认证（比如通过指纹认证我确实是这个人）

    firebase: login a user to an application, identity token



- **authorization**, proper access after authentication

  授权（身份认证完成后，我只能看我的工资）

  via a resource monitor, 4 types of access control policies

  - mandatory access control

    强制访问控制，基于安全标签和强制规则决定谁能访问

  - discretionary access control

    自主访问控制，资源的所有者决定谁能访问

  - **role-based** access control

    权限与用户的角色关联

  - **attribute-based** access control

    权限与用户或资源的属性（时间/位置等）关联

    application-level security / authorization is conceptually *embedded* in the application logic!

    但理想情况下，security logic和application logic应该是分离的，低耦合性的；

    -> challenge: fully separate security from application

    ->-> **security binding**: where to deploy & how to use security

    why to we need this?

    提高安全规则的灵活性和可维护性

    提供统一的安全管理方式

    简化应用逻辑，专注于business logic而不是security细节

- monitoring & audit

major concern 2: mechanisms typically fade out

(e.g. post quantum cryptography)

major concern 3: the attack surface of access control can be huge

basics vs. full complexity

software is an enabler of functionality, but new functionality comes with a certain risk

major concern 04: threats often not caused by security mechanisms / security implementation

意思是软件安全性是系统整体设计的问题，而不仅仅是某些局部实现的结果；security需要从system design的整体性考虑，而不是补丁单一问题

no policy? no mechanism?

policy & mechanism together form the basis of security

3 dimensions of achieving security

(all assuming we have defined the right policy)

1. Selecting (or implementing) the appropriate mechanisms
2. Developing quality code
3. Calling / utilizing the mechanisms in sync with the prescribed policy!

plus:

policy evolving & implementation. deployment environment selecting / configuration

in practice

Practitioners need to bring all elements together