Research Week 04

Chaz Davis

February 8, 2020

1 What is a Trust Framework? Give at least one real-world example of its use in Microsoft or Linux offerings

In digital identity systems, a trust framework functions as a certification program. It enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security, and privacy policies of the party who issues the credential (called the identity service provider) and vice versa.

A trust framework is primarily a legal framework that captures a set of activities and responsibilities of participatin entities in a way that it promotes trust among those entities. Trust framework may or may not be accompanied by technical spec.

2 Who is OIX? ICF? ICAM? OITF? OIDF? What is the mission of each of these?

- OIDF The OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies. OIDF assists the community by providing needed infra- structure and help in promoting and supporting expanded adoption of OpenID.

- ICF The Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem. Information Cards are personal digital identities people can use online, and the key component of identity metasystems. Visually, each Information Card has a card-shaped picture and a card name associated with it that enable people to organize their digital identities and to easily select one they want to use for any given interaction.

- OITF The Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF.

- OIX The Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the Open Identity Trust Frameworks model.
- AXN An Attribute Exchange Network (AXN) is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user-asserted, permissioned, and verified online identity attributes in high volumes at affordable costs

3 Explain what an AXN does.

- Subjects These are users of an RP's services, including customers, employees, trading partners, and subscribers.
- Attribute providers (APs) APs are entities acknowledged by the community of interest as being able to verify given attributes as presented by subjects and which are equipped through the AXN to create conformant attribute credentials according to the rules and agreements of the AXN. Some APs will be sources of authority for certain information; more commonly APs will be brokers of derived attributes.
- Identity providers (IDPs) These are entities able to authenticate user credentials and to vouch for the names (or pseudonyms or handles) of subjects, and which are equipped through the AXN or some other compatible Identity and Access Management (IDAM) system to create digital identities that may be used to index user attributes.

There are also the following important support elements as part on an AXN:

- Assessors Assessors evaluate identity service providers and RPs and certify that they are capable of following the OITF provider's blueprint.
- Auditors These entities may be called on to check that parties' practices have been in line with what was agreed for the OITF.
- Dispute resolvers These entities provide arbitration and dispute resolution under OIX guidelines.
- Trust framework providers A trust framework provider is an organization that translates the requirements of policymakers into an own blueprint for a trust framework that it then proceeds to build, doing so in a way that is consistent with the minimum requirements set out in the OITF specification. In almost all cases, there will be a reasonably obvious candidate organization to take on this role, for each industry sector or large organization that decides it is appropriate to interoperate with an AXN.

4 How are capability tickets utilized?

capability ticket A discretionary access control technique organized by subject. For each subject, the capability ticket lists objects and their permitted access rights by this subject.

When it is desired to determine which subjects have which access rights to a particular resource, ACLs are convenient, because each ACL provides the information for a given resource. However, this data structure is not convenient for determining the access rights available to a specific user.

Decomposition by rows yields capability tickets. A capability ticket specifies authorized objects and operations for a particular user. Each user has a number of tickets and may be authorized to loan or give them to others. Because tickets may be dispersed around the system, they present a greater security problem than access control lists. The integrity of the ticket must be protected, and guaranteed (usually by the operating system). In particular, the ticket must be unforgeable. One way to accomplish this is to have the operating system hold all tickets on behalf of users. These tickets would have to be held in a region of memory inaccessible to users. Another alternative is to include an unforgeable token in the capability. This could be a large random password, or a cryptographic message authentication code. This value is verified by the relevant resource whenever access is requested. This form of capability ticket is appropriate for use in a distributed environment, when the security of its contents cannot be guaranteed.

The convenient and inconvenient aspects of capability tickets are the opposite of those for ACLs. It is easy to determine the set of access rights that a given user has, but more difficult to determine the list of users with specific access rights for a specific resource.

5 Briefly define the difference between DAC and MAC.

Discretionary Access Control

- the control access is defined based on the requestor identity and the access rule authorizations.
- It permits the requestors only to perform the allowed activity
- The above policy is termed as a discretionary
- Because the entity must have access rights to permit another entity by its own decision
- It enables another entity to access some resource

Mandatory Access Control

- The control access is defined based on comparing the security labels with the security clearances.
- The security label indicates whether the system resource is sensitive or critical.
- The security clearance refers the system entities which are eligible to access the certain resources.
- The above policy is termed as mandatory
- Because the entity may or may not have eligibility to access the resource by its own decision and enable another entity to access some resource.

6 How does RBAC relate to DAC and MAC?

RBAC is a Role Based Access Control. The user roles are defined within the system and the access allowed based on the given roles.

All three are not mutually exclusive and the access control mechanism can employ two or all the three of the policies to cover different types of system resource.

The RBAC may use the discretionary or the mandatory mechanism for user roles.

7 List and define the three classes of subject in an access control system.

Access Control System The access control system is embodied in the authorization database. It states the types of permitted access, circumstances for the permission and who are all permitted.

- The access control system defines the three classes of the subject with different access rights:

- Owner
- Group
- World

8 What is the difference between an access control list and a capability ticket?

Access Control Lists can be simply explained as the mechanism that allows the permission on who can access the object. Capability Ticket refers to the process that shows what objects are allowed to access and what operations are allowed on it.

9 In the NIST RBAC model, what is the difference between SSD and DSD?

SSD is a constraint of the National Institute of Standards and Technology role based access(NIST RBAC) model. It enables a set of mutually exclusive roles. If one role is assigned to a user from a set, then the user may not be assigned to any other roles from that set. DSD is a constraint of NIST RBAC model. DSD relation is used to limit the permissions available to the user. DSD places constraints on the role which is activated within or across a user's session to limit available permissions.

10 What is a protection domain?

A protection domain is a grouping of code source and permissions. A protection domain represents all the permissions that are granted to a particular code source. In the default implementation of the Policy class, a protection domain is one grant entry in the file.

11 UNIX treats file directories in the same fashion as files; that is, both are defined by the same type of data structure, called an inode. As with files, directories include a nine-bit protection string. If care is not taken, this can create access control problems. For example, consider a file with protection mode 644 (octal) contained in a directory with protection mode 730. How might the file be compromised in this case?

If the file's octal code is 644 then that represents

- read and write access for the owner
- read access to the group
- read access to the everyone else

If the directory's octal code is 730 then that represents

- read and write and execute access for the owner
- write and execute access to the group
- and null value access for all other users

Since the file has only read permission for the group and others, the file has no write and execute permissions for the group and others. Whereas the directory has the write and execute permissions for the users group. So, the member of the group may change the content of the file or the file may be deleted. Thus, the permissions given to the file are of no use. The file has read permission for everyone else whereas the directory has no permission for others. Thus, the content of the file cannot be read by the others. The permissions given to the file are of no use.

12 what is a session?

A session is a temporary and interactive information exchange between two or more communicating devices. A browser may be making a series of http requests and transactions all initiated by the same user. Typically a session is started when a user authenticates their identity using a password or another authentication protocol.

13 give a brief overview of credential management.

Credential Management is the set of practices that an organization uses to issue, track, update, and revoke credentials for identities within their context.