Expanding CIP Security with the CIP Authorization Profile

Introduction

- No standard way to define what privilege levels are required to access what resources
- A standard profile gives the user a powerful mechanism to define authorization in a highly flexible and configurable way
- An investigation of technology options, as well as tradeoffs for the user

Existing CIP Security Profiles

Security Profile	General Description
EtherNet/IP Integrity Profile (Obsoleted)	Provides secure communications between EtherNet/IP endpoints to assure data integrity and device authenticity.
EtherNet/IP Confidentially Profile	Provides secure communications between EtherNet/IP endpoints and ensures data confidentiality for transport class 0/1 traffic. Includes the EtherNet/IP Integrity profile as a subset.
CIP Authorization Profile (future)	Provides secure communications between CIP endpoints to ensure device and user authenticity.
CIP User Authentication Profile	Provides User-level authentication for CIP communication
Resource-Constrained CIP Security Profile	Provides a lightweight version of the protections afforded by other CIP Security Profiles specifically for highly Resource-Constrained devices

Security Properties in existing CIP Security Profiles

Security Property	EtherNet/IP Confidentially Profile	CIP Authorization Profile (future)	CIP User Authentication Profile	Resource-Constrained CIP Security Profile
Device Authentication	√	√		√
Trust Domain	Broad – group of devices		Narrow - individual device/user	Broad – option to be Narrow via Gateway or Proxy
Device Identity	√		√ (Identity of User)	√
Data Integrity	√			√
Data Confidentiality	√			Via Gateway or Proxy
User Authentication			√	
Change Detection (Audit)		√		
Policy Enforcement (Authorization)		Flexible	Fixed	Via Gateway or Proxy

Authentication vs. Authorization

- Authentication is the security practice to confirm that the users is who they claim to be
- Authentication is the first step in security on logging in and gaining access to digital information
- The process of authenticating a user could be accomplished by different means such as passwords, authentication apps, or biometrics
- This is used to prove that that the user is who they claim to be, thereby authenticating the user

Authentication vs. Authorization

- Once authenticated, a user can see the information that they are authorized to see and access information that they are authorized to access
- Authorization in system security is the process of giving the user permission to access a specific resource or function
- This could be granting access to folders on a server or starting certain applications

Authorization strategies

- Authorization can be determined in different ways, often referred to as authorization strategies
- Different authorization strategies have been developed for different purposes and use cases
- The two most prominent authorization strategies are:
  - Role-Based Access Control (RBAC)
  - Attribute-Based Access Control (ABAC)

Role-Based Access Control

- Well-known roles are defined and users are mapped to one (or more) roles
  - Whichever role a user is mapped to is the basis of the privileges that user has
  - Example: ”Operator” role may be able to create I/O connections and diagnose problems but not program a controller, that may be reserved for the ”Engineer” role
- Note CIP Security User Authentication Profile already has some roles defined and associated permissions
  - However, there is no way to change what a given role can do

Attribute-Based Access Control

- Permissions depend on one or more attributes
  - This is more general than RBAC, which can be seen as a subset of ABAC (role is just one attribute)
  - Example: your permissions might depend on your role, time of day, training record status, and your location
- This is a more powerful and configurable mechanism for authorization, although the complexity needs to be managed

Requirements for CIP Authorization Profile

- CIP Endpoints must be policy enforcement point
  - Profile must be suitable for implementation in an embedded device
- Reuse existing technologies if possible
  - Sometimes this is not possible but the preference is always to use what is there (e.g.: TLS, OpendID Connect, EST)
- Support both RBAC and ABAC
  - ABAC might be optional
- Provide options for simple access policy and complex policy
  - Simple declarative statements to complex logical operations
- Integrate with IT systems
  - Similar to reusing existing technology

Existing Authorization systems

- There are some existing authorization schemes that may be usable within a CIP environment
- Most existing schemes rely on a “policy document” format
  - A policy authority generates a document with access policy rules encoded
    - Rules may be complex logical statements or simple descriptions, depending on what the technology supports
  - Document is signed for authenticity assurances, can even be encrypted if needed
  - Document is then distributed to policy enforcement points (in this case CIP endpoints, although a proxy model could be used)

Document-Based Access Policy Management

- Managing access policy using a document-based structure
- A signed document enumerates access policy and then distributed to CIP endpoints that will then enforce that access policy
- The document might implement complex access policy rules that include logical operations (AND/OR/IF THEN) on various attributes and device state
- Based on Rego, XACML, and a YANG Model-based mechanism.
  - Provides the advantage of better integrating with many existing authorization definition technologies
  - The downside that CIP endpoints would have to support the technology

Open Policy Agent and Rego

- OPA is the agent and Rego the Access Policy language
- Supports RBAC and ABAC
- Commonly used in software and cloud-based architectures
- Powerful, but may not be well suited to embedded devices
  - OPA in particular would be challenging to run in an embedded device, but Rego could be used without OPA

eXtensible Access Control Markup Language (XACML)

- Access Policy language based on XML
- Supports RBAC and ABAC
- Has been used in some web/Internet applications before
  - Somewhat older than OPA and Rego
  - Not as richly features as Rego
- Generally not designed for embedded systems, but not as complex as Rego

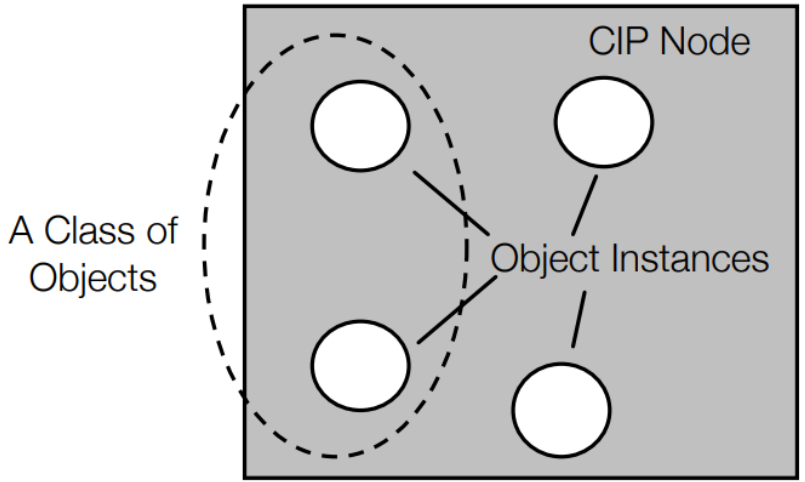
General Data Modeling Language

- An existing data modeling/encoding language could be used to create an access policy language specific to CIP endpoints
  - Example: YANG (Yet Another Next Generation)
- Significantly more design work
- Could be tailored to be specific to CIP
- Much less opportunity for technology reuse

Mapping to CIP

- Every CIP node is modeled as a collection of objects
- CIP objects are structured into classes, instances and attributes

- Hard to manage all combinations of CIP defined classes and attributes as well as Vendor Specific classes and attributes in a generic way



Mapping to CIP

- CIP Security Roles:
  - Administrator
  - Engineer
  - Operator
  - Auditor
  - Viewer
  - Anonymous

CIP Service-Based Access Policy Management

- Each attribute to also carry permission information
- Would be additional information that would go together with the rest of the attribute data within the device

Attr ID	Need in Implem	Access Rule	NV	Name	Data Type	Description of Attribute
1	Optional	Get		AtReference	BOOL	0 = Drive hasn't reached SpeedRef 1 = Drive has reached SpeedRef
2	Required	Get		SpeedActual	INT	Actual speed
3	Required	Set		SpeedRef	INT	Commanded reference speed

CIP Service-Based Access Policy Management

- New services to manage the permissions:
  - View_Permission_Information
  - Apply_Permission_Information

Name	Data Type	Description of Parameter
Engineer access	ENUM	Access rights to Engineer
Operator access	ENUM	Access rights to Operator
Auditor access	ENUM	Access rights to Auditor
Viewer access	ENUM	Access rights to Viewer
Anonymous access	ENUM	Access rights to Anonymous

Access	Value
No access	0
Read access	1
Write access	2

CIP Service-Based Access Policy Management

- Example with permission information

Attr ID	Need in Imp	Access Rule	NV	Name	Data Type	Permission information		Description of Attribute
1	Optional	Get		AtReference	BOOL	Engineer access	Read	0 = Drive hasn't reached SpeedRef 1 = Drive has reached SpeedRef
						Operator access	Read	
						Auditor access	Read	
						Viewer access	No	
						Anonymous access	No	
2	Required	Get		SpeedActual	INT	Engineer access	Read	Actual speed
						Operator access	Read	
						Auditor access	Read	
						Viewer access	Read	
						Anonymous access	No	
3	Required	Set		SpeedRef	INT	Engineer access	Write	Commanded reference speed
						Operator access	Read	
						Auditor access	Read	
						Viewer access	No	
						Anonymous access	No	

Conclusions

- This serves as an introduction into possibilities for the CIP Authorization Profile
- Many options exist for access policy/authorization within CIP endpoints
- Each option has particular advantages and disadvantages that must be weighed
- Further investigation is needed to determine the optimal direction

2022 ODVA

INDUSTRY CONFERENCE AND 21ST ANNUAL MEETING