USE CASE

IDENTITY AND ACCESS MANAGEMENT

Securing Networked Infrastructure for the Energy Sector

V. 2
November 5, 2013
energy_nccoe@nist.gov

This revision incorporates comments from the public.

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end reference designs that are broadly applicable and help businesses more easily align with relevant standards and best practices.

This document is a detailed description of a particular problem that is relevant across the energy sector. NCCoE cybersecurity experts will address this challenge through collaboration with members of the energy sector and vendors of cybersecurity solutions. The solutions proposed by this effort will not be the only ones available in the fast-moving cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at energy_nccoe@nist.gov*.*

1. Description

Goal

In order to protect power generation, transmission and distribution, energy companies need to be able to control physical and logical access to their resources, including buildings, equipment, information technology and industrial control systems (ICS). They must be able to authenticate the individuals and systems to which they are giving access rights with a high degree of certainty, whether they are employees, contractors, vendors, or partners. In addition, energy companies must be able to enforce access control policies (e.g. allow, deny, inquire further) consistently, uniformly and in a timely way across all of their resources.

Motivation

A foundation of cybersecurity is the principle of least privilege, or the notion that "Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job."[1] To enforce this principle, the access control system needs to know the appropriate privileges for a given user or system. Authentication is a necessary step in this process.

Identity also plays a role when a system is compromised, as determining accountability is generally a goal of the ensuing investigation. Security analysts will examine the information exchanges among systems associated with the incident, including which entities made those exchanges. Key to this process is the ability to trace the relevant behavior based on who (or which system) accessed what resources.

[1] J. Saltzer, Protection and the control of information sharing in multics, *Communications of the ACM*, **17** (7), 388-402 (1974)

Illustrative Scenario

An energy company technician attempts to enter a substation. She is challenged to prove her identity in a way that provides a high-degree of confidence and is not onerous (e.g., does not require a significant behavior change). Her attempt at entry initiates an authentication request that, if possible, connects to the company's authentication and authorization services to validate her identity, ensure that she is authorized to access the substation, and confirm that there is a work order on file for that substation and that worker at that time. Once she gains access to the substation, she focuses on the reason for her visit: She needs to diagnose a remote terminal unit (RTU) that has lost its network connectivity. She immediately identifies the cause of the failure as a frayed Ethernet cable and replaces the cable with a spare. She then uses her company-issued mobile device, along with the same electronic credential she used for physical access, to log into the RTU's web interface to test connectivity. The RTU queries the central authentication service to ensure the authenticity and authority of both the technician and her device, then logs the login attempt, the successful authentication and the commands the technician sends during her session.

2. Desired Solution Characteristics

- authentication, authorization and access control requirements for all operational technology (OT)
- ability to manage and log authentication, authorization and access control information for all OT using centralized or federated controls
- ability to centrally monitor authorized and unauthorized use of all OT and user accounts
- flexibility to meet operational requirements when devices are disconnected from the network or have limited network connectivity
- authentication, authorization and access control mechanisms that meet business security and regulatory requirements
- appropriate encryption to enable reasonably secure exchange of identity and access management information
- ability to provision, modify or revoke access throughout all federated entities in a timely manner
- a single set of credentials for each user, device or application to use throughout the federated enterprise
- authorization mechanisms that can tailor or escalate privilege based on contextual conditions
- compatibility with various electric utility ICS equipment and software
- compatibility with protocols and communication media commonly used by electric utilities
- ease of use (e.g., installation, configuration, maintenance, provisioning, de-provisioning, credentialing, revoking credentials)

3. Business Value

- reduces opportunities for attack or error, as well as the impact of such incidents on energy delivery, thereby lowering overall business risk
- increases the probability that investigations of attacks or anomalous system behavior will reach successful conclusions
- improves accountability and traceability, leading to valuable operational lessons learned
- simplifies regulatory compliance by automating generation and collection of access information

4. Relevant Standards and Regulations

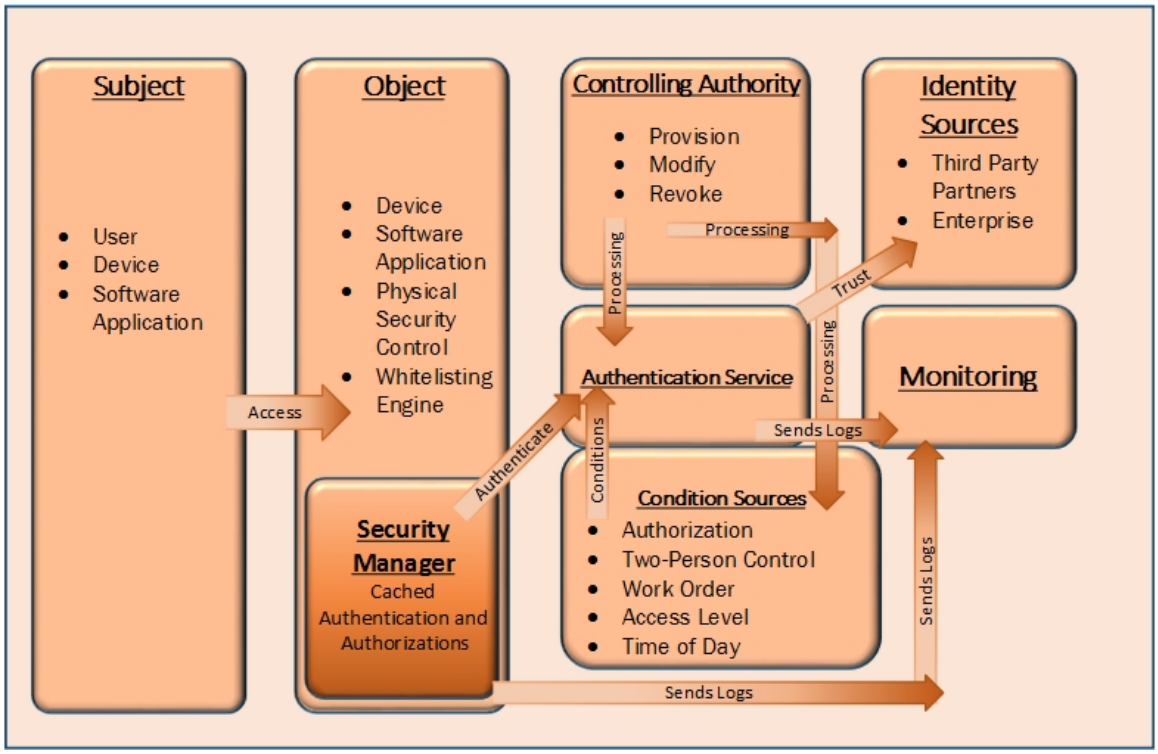
- ISA 99, Industrial Automation and Control Systems Security
  http://www.isa.org/isa99
- IEC 62351: Security
  http://www.iec.ch/smartgrid/standards/
- NERC Critical Infrastructure Protection Plans v.3 and v.5
  http://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
- NRC 10 CFR 73.54, Protection of Digital Computer and Communication Systems and Networks
  http://www.nrc.gov/reading-rm/doc-collections/cfr/part073/part073-0054.html
- NRC Regulatory Guide 1.152, Rev. 3, Criteria for Use of Computers in Safety Systems of Nuclear Power Plants
  http://pbadupws.nrc.gov/docs/ML1028/ML102870022.pdf
- NIST IR 7628, Guidelines for Smart Grid Cyber Security
  http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf
- NIST SP 800-82, Guide to Industrial Control Systems Security
  http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf
- Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
  http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybersecurity-capability-maturity-model-es-c2m2

5. Example Component List

- services for authenticating and authorizing users based on identity, role, third-party affiliation (e.g., federation) or other attributes (e.g., attribute-based access control)
- services for authenticating and authorizing devices
- services for whitelisting applications

- identity and access governance capability that translates human-readable access needs into machine-readable authorizations
- security incident and event management (SIEM) or log analysis software for monitoring access management events
- ICS equipment, such as RTUs, programmable logic controllers (PLC), and relays, along with associated software and communications equipment (e.g., radios, encryptors)
- physical access control devices that use standard communication interfaces
- "bump-in-the-wire" devices for augmenting OT with authentication, authorization, access control, encrypted communication and logging capabilities

6. High-Level Architecture



7. Approach to Comments

We received more than 130 comments from 40 reviewers regarding the two draft use cases. Comments were grouped according to their commonalities, then we distilled those grouped comments into these brief statements. We have provided a response to each statement and revised the use cases accordingly.

8. General Comments

1. There were many comments identifying products of potential interest, or indicating interest in getting involved.

   Response: We welcome inquiries from companies that are interested in participating in our use cases. In the next few weeks, we will publish a Federal Register notice for each use case with instructions for companies that hope to get involved. To receive announcements about the publication of the Federal Register notices, send an email to nccoe@nist.gov.

2. The (new) capabilities envisioned in each use case can themselves introduce new vulnerabilities or become targets of attack.

   Response: This is a legitimate concern for any new feature added to any system, but it should not prevent us from seeking out new capabilities that improve security, efficiency and function. The NCCoE's mission is to help American companies become more secure, so we take seriously the security of our example solutions. Unfortunately, because the field of cybersecurity currently cannot measure security, no solution can be proven to be free of vulnerability, and so there is no way to guarantee the security of a solution. The NCCoE will analyze the solutions to gain reasonable assurance that they are appropriate for the security of critical infrastructure like the energy industry.

3. Operational availability trumps security. In particular, offline operation of systems or endpoint devices needs to be addressed.

   Response: This comment is true of many critical infrastructure sectors, including electric power. The use case descriptions have been modified to reflect the need for disconnected operation.

4. Some comments conjectured that the capabilities are going to be expensive to procure and time-consuming to deploy. What near-term business value will justify that investment? Conversely, several additions to the Business Value sections were suggested.

   Response: These comments resulted in some modifications to the Business Value sections in the use cases. The NCCoE has found many private sector

companies developing unexpected solutions that are not well publicized. Therefore, we are hopeful that if we clearly state wished-for capabilities without assuming they are impractical to achieve, these use cases will result in a variety of solutions for utilities with a wide range of security needs and budgets.

5. The component lists are an inconsistent mix of technology, objectives and environmental factors.

   Response: The component lists have been modified for better consistency.

6. Several comments advocated making compliance to the NIST Federal Information Processing Standards and other federal security guidelines a requirement for the use cases.

   Response: Federal standards and guidelines are not mandatory for non-governmental use unless adopted by a relevant regulator. Furthermore, the solution sets that result from these use cases will not have any specific government or regulatory approval, certification, or accreditation. Nevertheless, the NCCoE will seek to be consistent with or improve upon the best available security practices in a manner that will be practical for all members of the affected sector.

9. Comments on this Use Case

1. "A single, centrally managed credential for each user," and a "company's central authentication service" seemed unrealistic or impractical with respect to:

   a. Lack of connectivity between physical access, operational control and enterprise management systems for policy as well as technology reasons

      Response: We hope to explore the technical options for balancing usability, security and connectivity; we are not presuming that everything has to be logically connected in order to satisfy the usability goal of a single physical identification artifact.

   b. Lack of central responsibility or awareness of users; responsibility is shared by a community of partnering organizations, suggesting that a federated approach would make more sense

      Response: We should have explicitly mentioned that a federated approach has a number of advantages and should be considered as an option. The use case description has been modified to address this issue.

   c. Lack of a well-defined utility network perimeter. If there were a central authentication service, it might be hard to define its scope of authority. In a federated environment, different authorities can take primary responsibility for different parts of the system.

Response: As above, we recognize that a federated approach has a number of advantages.

2. The authentication service needs to address revocation or "de-provisioning" of users.

   Response: Ease and consistency of enrolling and revoking users are important requirements for this use case. We have modified the use case description to address this issue.

3. An authentication decision has to have contextual scope (e.g. task, session, time period).

   Response: Authentication decisions necessarily have contextual scope, and the NCCoE would be interested in solutions that offer enterprises greater control over that scope (e.g., ensuring that a user has an appropriate work order for the given time and location as part of the authentication process). We encourage companies that market such solutions to respond to our upcoming Federal Register notices.

4. Access privileges should receive periodic certification.

   Response: The NCCoE considers this to be a policy issue rather than a technology issue, and therefore beyond the scope of this use case.

5. Authentication and authorization are separate functions and should be shown separately, even if they may be combined in some implementations. Moreover, responsibility over authorizations is usually quite distinct from responsibility for identity and authentication.

   Response: This is a valid concern, and we have modified our use case description to address it.

6. The principle of least privilege implies merit for gradations in authentication, whereby users can escalate privilege by authenticating with stronger methods.

   Response: The NCCoE would be interested in solutions that allow users to escalate privilege using multiple authentication methods provided that they were appropriately easy to use. This may also be an important element of dealing gracefully with general comment #3. We encourage companies that market such solutions to respond to our upcoming Federal Register notices.

7. Separation of duties is as important as least privilege.

   Response: Because separation of duties is important for security, the NCCoE is interested in products that will aid electric utilities in enforcing this principle. We encourage companies that market such products to respond to our upcoming Federal Register notices.

8. The use case should take advantage of Federal Information Processing Standard 201 and Personal Identity Verification Interoperability standards and guidance rather than “invent a new wheel.”

   Response: The use case will not invent any new wheels. We prefer standards-based solutions, but we will consider all proposed products on the merits of security capability, ease of use, compatibility with existing systems, and supported features.

9. Reference the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2).

   Response: We agree, and have added it to the list of relevant standards

Appendix: Security Control Map

This table maps the preliminary list of desired characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) and other NIST activities. This is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Example Characteristic			Cybersecurity Standards and Best Practices						Sector-Specifc Standards and Best Practices
Security Characteristics	**Example Capability**		**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27001**	**SANS CAG20**	**NERC CIP v3/5**
authentication for OT	authentication mechanisms		Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-007-5 R2, CIP-007-5 R5
access control for OT	access control mechanisms		Protect	Access Control and Protective Technology	PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	AC-3, AC-17, AC-19, AC-20, CM-7, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	ISO/IEC 27001:2013 A.6.2.2, A.9.1.2A, 11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3, A.13.1.1, A.13.2.1	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R2, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2, CIP-007-5 R1,
authorization (provisioning) OT	access policy management mechanisms		Protect	Access Control	PR.AC-4 Access Permissions are managed, incorporating principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R5
centrally monitor use of accounts	log account activity		Detect, Protect	Continuous Monitoring and Protective Technology	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events PR.PT-1: Audit/log records are determined, documented, implemented	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11, AU family	ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1	CSC 4-2,CSC 12-1, CSC 12-10, CSC 14-2, CSC 14-3,	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-006-5 R2 CIP-007-5 R4, CIP-007-5 R5, CIP-008-5 R2, CIP-010-5 R1, CIP-011-5 R2
protect exchange of identity and access information	encryption		Protect	Data Security	PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected	SC-8, SC-28	ISO/IEC 27001:2013 A.8.2, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3	CSC 16-16, CSC 17-7	CIP-011-5 R1
provision, modify or revoke access throughout all federated entities	mechanisms for centrally managed provisioning of access		Protect	Access Control	PR.AC-1: Identities and credentials are managed for authorized devices and users PR.AC-4 : Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16, IA Family	ISO/IEC 27001:2013 A.6.1.2, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3 , A.9.4.4	CSC 3-3, CSC 12-1, CSC 12-10, CSC 16-4, CSC 16-12	CIP-003-5 R1, CIP-004-5 R4, CIP-004-5 R5, CIP-005-5 R1, CIP-005-5 R2, CIP-006-5 R1, CIP-007-5 R4, CIP-007-5 R5