CYBERSECURITY INTEGRATED PROJECT TEAM

Secure Interoperability Governance Process

Version 1.0
8/5/2016

This document contains a governance process to ensure secure interoperability of diverse systems. The purpose of this governance process is to provide guidance of how to govern the incorporation and demonstration of security architectures and technologies into federated cross-domain interoperability environments. The goal is a process that is universally trusted for establishing agreed-to rules, policies and methodologies to standing up and interconnecting networks where the participants have sufficient trust such that they are willing to share data in support of a common mission.

Approved for Public Release
NCOIC_Secure_Interoperability_Governance_v1.0
5 August 2016

VERSION HISTORY			
Version #	**Description**	**Date**	**Author**
1.0	Initial Release	8/5/2016	Cybersecurity IPT

Acknowledgements

The following individuals participated in the creation of this document and are gratefully acknowledged:

Chair

- Andrew Born

Primary Authors and Editors

- Andrew Born (Boeing)
- Mark Bowler (Boeing)
- Dr. Craig Lee (The Aerospace Corp)
- Dr. Alenka Brown (McClure, Brown, and Associates)
- Al Sipe (Boeing)
- Pat Ryan (NCOIC)

Table of Contents

List of Figures

1 Introduction

1.1 Purpose

The purpose of a secure interoperability governance process (SIGP) is to define how to govern the incorporation and demonstration of security architectures and technologies into federated cross-domain interoperability environments. This document describes the steps needed to define and implement a secure interoperability governance process.

1.2 Goal

The goal is a process that is universally trusted by the participants for establishing agreed-to rules, policies and methodologies to standing up and interconnecting networks, where the participants have sufficient trust such that they are willing to share data in support of a common mission, including disaster response, civil-military cooperation, military coalitions, etc.

2 Secure Interoperability Governance Process

2.1 Steps to Establish a Secure Interoperability Governance Process

The following steps are recommended for standing up a collaborative secure information exchange system. The rules, policies and methodologies (collectively known as the secure interoperability governance process) must be agreed to beforehand by all owners of the federated systems and all owners of the data. The process details how to define and establish a trust framework that will be followed by the participants.

1. Identify your stakeholders/users and community of interest. Understand all users/stakeholder’s cybersecurity needs and postures, since this is critical for appropriate implementation of the process.
2. Define what you are governing.
    a. Determine what system components and end points need to be interoperable (service oriented architecture, clouds, etc.).
    b. Determine the sensitivity level of the data that you are ultimately protecting, since highly sensitive data requires appropriate governance procedures and processes; personally identifiable information (PII) and protected health information (PHI) have very strict governance requirements, such as protections by the Health Insurance Portability and Accountability Act (HIPAA).
    c. Determine auditing requirements.
3. Define which data and apps need to be interoperable (chat, all data, etc.).

4. Define and document a set of agree-to governance elements that will be applied or utilized during the start-up and operation of the collaborative network. All of the elements identified in the list below should be addressed. It is essential the key stakeholders agree to the elements up front. Additional information and examples of these elements are found in the Appendix of this document.
5. Assess your current posture. Use a risk-based approach to assess your cybersecurity practices against the framework core industry standards and guidelines. This will help you determine the elements to include as desired control objectives.
6. Define a target profile and execute. Based on your assessment, establish a current profile of cybersecurity activities and risk-management practices. Using a combination of the framework core and business-specific requirements that have been endorsed by your executive sponsor, create a baseline to guide cybersecurity risk-management activities. Next, determine a target profile to identify gaps and draft a prioritized action roadmap and execution program to achieve the target profile.
7. Continuously monitor, communicate and collaborate. In a reiterative process, continuously monitor and routinely assess your critical infrastructure assets' current profile against the business-defined target profile. Share information about the target profile with your executive sponsor, who can help transform progress toward the target profile into a business context. Use this business context to inform internal stakeholders, including legal counsel, audit functions, lines of business and board of directors, if necessary.

Here are the governance elements that should be considered in the overall governance process. See the examples in the Appendix for details on each.

- Cybersecurity Framework
- Standards and Guidelines
- Roles, Responsibilities and Authorizations
- Authentication Technology
- Authorization Technology
- Human Interoperability Framework
- Use Cases
- Threat Modeling
- Layered Security and Defense in Depth
- Rules for Graceful Lowering of Security Controls

2.2 Integration Functionalities of a Governance Process

The following functionalities should be part of a successful secure interoperability governance framework.

- Control integration - Alerting and notification integration, launching events and actions, and integration of service governance and lifecycle.
- Data integration - Leveraging the service registry as the primary service description, characteristic and policy catalog.
- Provisioning integration - Leveraging the governance system as part of the provisioning and deployment process of business services; once integrated, bi-directional exchange of service information between participants is enabled.
- Deployment integration - Upon deployment of services, all parties should have the ability to alert others to the existence of the service and the need to put the service and its definitions under management.

2.3 Attributes of a Secure Interoperability Governance Process

The four attributes of a secure interoperability governance process are described below.

1. Federated identity management
    - A federated identity in information technology (IT) is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.
    - Federated identity management (FIM) is an arrangement that can be made among multiple enterprises that lets subscribers use the same identification data to obtain access to the networks of all enterprises in the group.
    - Federated identity management uses a common set of policies, practices and protocols to manage the identity and trust into IT users and devices across organizations.
2. Transitivity
    - A trusted boundary can be expanded if the already-trusted elements are used to attest to the trustworthiness of a secondary set of elements, assuming that the initial state of these secondary elements can be determined to be trustworthy.
        - These secondary elements can then be used to attest to the trustworthiness of a tertiary set, and soon on; and the trusted boundary can be expanded theoretically infinitely in a chain of trust as long as the roots of trust retain their integrity.
3. Delegation of trust

- If one system accepts the identification and authentication (I&A) of users provided by a second, and the second system accepts user I&A from a third, then the first system in effect trusts the I&A of the third.

4. Manage the trust ecosystem

- Trust management systems support risk evaluation and decision making on whether collaboration is worth joining and continuing.
- Collaboration experiences are shared through reputation systems in order to help establish inter-enterprise collaborations in a service ecosystem where first-hand experiences are not always available.
- There are two high-level trust management architectures for cloud-based service ecosystems.
    - Closed collaboration environments (e.g., traditional virtual organization breeding environments) are often built around a hub actor, are centrally managed and apply pre-formed trust relationships in determining who is allowed into the breeding environment.
    - Open service ecosystems, in contrast, allow service providers to enter the ecosystem by publishing a valid service offer, and trust relationships are formed and evolve within the ecosystem.

3 Acronym List

FIPS	Federal Information Processing Standards
GFIPM	Global Federated Identity and Privilege Management
HIPAA	Health Insurance Portability and Accountability Act
IDEF	Identity Ecosystem Framework
NCIF	Net-Centric Information Framework
NCSF	Net-Centric Service Framework
NIEF	National Identity Exchange Federation
NIF	NCOIC Interoperability Framework
NIST	National Institute of Standards and Technology
NSTIC	National Strategy for Trusted Identities in Cyberspace
PHI	Protected Health Information
PII	Personally Identifiable Information
PRMF	Privacy Risk Management Framework
RRA	Roles, Responsibilities and Authorities
SIGP	Secure Interoperability Governance Process
SOA	Service Oriented Architecture

4 Appendix

4.1 Frameworks

A governance process will, by necessity, either specify or make reference to commonly used frameworks that address issues in cybersecurity and trust in federated cloud environments.

The following is a partial list of frameworks that may be useful in developing a governance process. It is strongly recommended that the governance process leverage and utilize existing, publicly available frameworks.

This document recommends frameworks created by three organizations.

- National Institute of Standards and Technology (NIST), which is the federal technology agency that works with industry to develop and apply technology, measurements and standards. NIST is an agency within the U.S. Department of Commerce. http://www.nist.gov
- National Strategy for Trusted Identities in Cyberspace (NSTIC) is a U.S. government initiative to improve the privacy, security and convenience of sensitive online transactions through collaborative efforts with the private sector, advocacy groups, government agencies and other organizations. Its strategy is to develop an online environment where individuals and organizations can trust each other because they identify and authenticate their digital identities and the digital identities of organizations and devices. It was promoted to offer, but not mandate, stronger identification and authentication while protecting privacy by limiting the amount of information that individuals must disclose. http://www.nist.gov/nstic/
- Network Centric Operations Industry Consortium (NCOIC), the owner of this document, is an international, not-for-profit consortium of industry, customers, and governmental organizations focused on accelerating the global use of network-centric principles and systems. Our goal is to improve information sharing among different communities of interest to enhance their productivity, interactivity, safety and security. www.ncoic.org

Suggested Frameworks

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- National Identity Exchange Federation (NIEF) Framework
- Global Federated Identity and Privilege Management (GFIPM) Program
- Risk Management Framework
- NSTIC Identity Ecosystem Framework (IDEF)

- NSTIC Privacy Risk Management Framework (PRMF)
- NCOIC Interoperability Framework (NIF)
- NCOIC Net-centric Service Framework (NCSF)
- NCOIC Net-Centric Information Framework (NCIF)

4.1.1 Framework 1: NIST Cybersecurity

The NIST Framework contains guidance (based on existing standards, guidelines and practices) for critical infrastructure organizations to better manage and reduce cybersecurity risk, and foster risk and cybersecurity management communications among organization stakeholders.

The NIST Framework is composed of three components: the framework core, framework implementation tiers, and framework profiles.

Framework Core

- The framework core is a set of cybersecurity activities, desired outcomes and applicable references that are common across critical infrastructure sectors.
- The core presents industry standards, guidelines and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization, from the executive level to the implementation/operations level.
- The framework c ore consists of five concurrent and continuous functions: identify, protect, detect, respond and recover.

Framework Implementation Tiers

- Framework implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.
- Tiers describe the degree to which an organization’s cybersecurity risk-management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable and adaptive).
- The tiers characterize an organization’s practices over a range, from partial (Tier 1) to adaptive (Tier 4).

Framework Profile

- The framework profile represents the outcomes based on business needs that an organization has selected from the framework categories and subcategories.

- The profile can be characterized as the alignment of standards, guidelines and practices to the framework core in a particular implementation scenario.
- Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a current profile (the as-is state) with a target profile (the to-be state).

More information at: http://www.nist.gov/cyberframework

4.1.2 Framework 2: NIST Risk Management Framework

Risk Management Framework (RMF) is the unified information security framework for the entire U.S. federal government that is replacing the legacy Certification and Accreditation (C&A) processes within federal government departments and agencies, the Department of Defense and the intelligence community.

Department of Commerce NIST Special Publication 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF). The six steps of the framework are illustrated in Figure 4-1. http://csrc.nist.gov/groups/SMA/fisma/framework.html

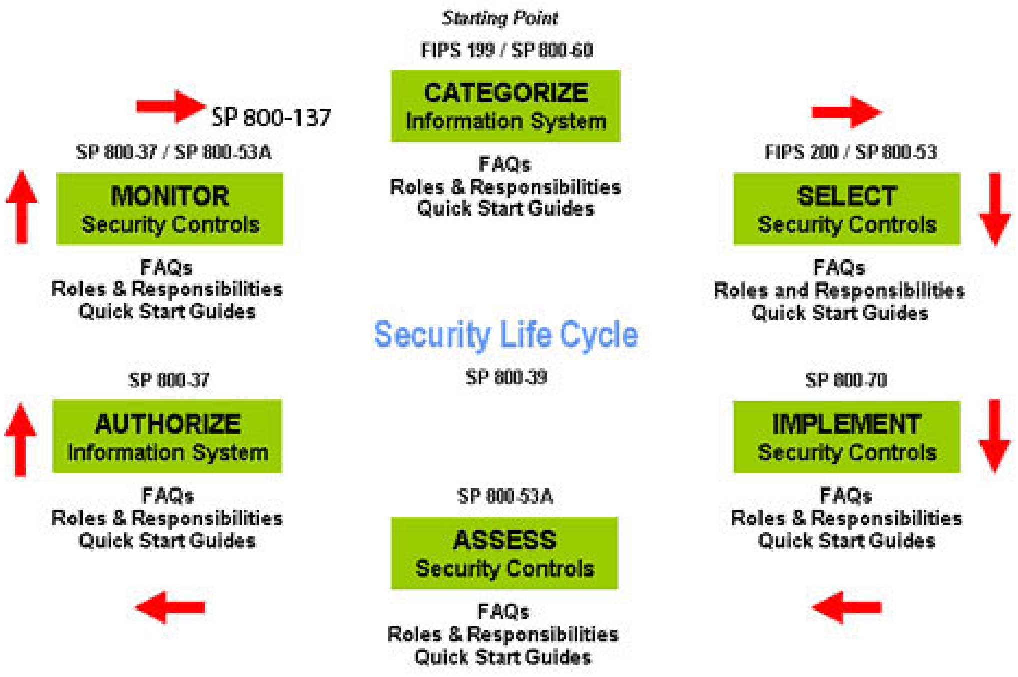


Figure 4-1 Risk Management Framework. (Source: NIST)

4.1.3 Framework 3: National Identity Exchange Federation (NIEF)

National Identity Exchange Federation is a trust framework that enables a wider range of secure information exchanges among its member agencies by providing a basic infrastructure consisting of governance, policies and procedures, cryptographic trust, and open standards for securely sharing identity information about users and non-user (system) entities.

There are four NIEF objectives.

- Share user identity and attribute information for authentication, identification, authorization and auditing.
- Share agency and resource metadata information.
- Provide onramp and roadmap other relevant identity, credential and access management (ICAM) initiatives.
- Provide an operational trust framework for accomplishing the other objectives.

https://nief.gfipm.net/policies/nief-identity-assurance-framework-1.1.pdf

4.1.4 Framework 4: Global Federated Identity and Privilege Management (GFIPM)

Global Federated Identity and Privilege Management, a collaboration of the U.S. Departments of Justice and Homeland Security, develops secure, scalable and cost-effective technologies for information sharing within the law enforcement and criminal justice communities, which control identity and privilege management. This consists of organizational guidelines, technical standards, implementation resources and outreach resources. http://www.gfipm.net/about/

4.1.5 Framework 5: NSTIC Identity Ecosystem Framework (IDEF)

The NSTIC Identity Ecosystem Framework is a user-centric online environment, a set of technologies, policies and agreed-upon standards that securely supports transactions, ranging from anonymous to fully authenticated and from low to high value. Key attributes of the identity ecosystem include privacy, convenience, efficiency, ease of use, security, confidence, innovation and choice.

Here are examples of how the identity ecosystem could work.

- Faster online errands
  - A smart card issued by Internet service providers “memorizes” the passwords that a consumer would normally need to memorize, thus

allowing consumers the ability to conduct business. The consumer inserts the card into her computer and in a matter of minutes, with just clicks of her mouse, she is able to securely conduct business with her bank, mortgage company and doctor, while also sending an email to her friend and checking her office calendar.

- Age-appropriate access
  - A teenager loves to visit online chat rooms to talk to other students his age. His parents give him permission to get an identity credential, stored on a keychain fob, from his school. The credential verifies his age so he can visit chat rooms for adolescents, but it does not reveal his birth date, name or other information. Nor does it inform the school about his online activities.
- Smart phone transactions
  - A consumer does most of her online transactions using her smart phone. She downloads a "digital certificate" from an ID provider that resides as an application on her phone. With a single, short PIN or password, the phone's application is used to prove her identity. She can do all of her sensitive transactions, even pay taxes, through her smart phone without remembering complex passwords and whenever and wherever it is convenient for her.
- Efficient and secure business operations
  - A small business owner is setting up a new online storefront. Without making large investments, he wants customers to know that his small firm can provide the same safety and privacy for their transactions as larger companies. He agrees to follow the identity ecosystem privacy and security requirements, earning a "trustmark" logo for his website. To reduce his risk of fraud, he needs to know that his customers' credit cards or other payment mechanisms are valid and where to ship merchandise. There are a number of different ID providers that can issue credentials to validate this information. Millions of individuals can now use his website without having to share extra personal information or even set up accounts with his company. This saves his customers time, increases their confidence and saves him money.
- Enhanced public safety
  - A devastating hurricane occurs close to a doctor’s home. Using an interoperable ID credential embedded in his cell phone and issued by his employer, he logs in to a Web portal maintained by a federal agency. The site tells him that his medical specialty is urgently needed at a triage center nearby. When he arrives, officials at the center use his credential to

verify he is a licensed doctor, and he is able to provide medical attention for victims.

http://www.nist.gov/nstic/identity-ecosystem.html

4.1.6 Framework 6: NSTIC Privacy Risk Management Framework (PRMF)

The NSTIC Privacy Risk Management Framework describes a framework for federal information systems. It provides the basis for establishing a common vocabulary to facilitate better understanding of and communication about privacy risks and the effective implementation of privacy principles in federal information systems. This publication focuses on the development of two key pillars to support the application of the framework: privacy engineering objectives and a privacy risk model.

http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf

4.1.7 Framework 7: NCOIC Interoperability Framework (NIF)

The NCOIC Interoperability Framework provides top-level net-centric and interoperability guidance for system architects designing and building systems and systems-of-systems. It gives architectural guidance for overarching architectures, elements of enterprise architecture that describe interaction and information exchange between systems at the enterprise level. It is supported by underlying NCOIC specialized frameworks and net-centric patterns.

https://www.ncoic.org/technology/technical-products/frameworks/10-technology/33-tech-prod-framework-nif

4.1.8 Framework 8: NCOIC Net-Centric Service Framework (NCSF)

The NCOIC Net-Centric Service Framework, which complements the NIF overarching framework, provides high-level guidance in the form of concepts, principles, patterns and processes for the design and implementation of services within a net-centric environment. NCSF defines additional specialized aspects of the information communication space with frameworks that are organized along interoperability concepts, principles, patterns and processes.

https://www.ncoic.org/images/technology/frameworks/Net_Centric_Services_Framework_V2.pdf

4.1.9 Framework 9: NCOIC Net-Centric Information Framework (NCIF)

The NCOIC Net-Centric Information Framework defines the concepts and principles governing the use of information in a net-centric environment. It acts as a starting point for the development of domain, mission and system-specific information specifications that may be part of any large-scale information systems development activity.

https://www.ncoic.org/images/technology/frameworks/10921_NetCentInfoFrameworkV1.01.pdf

4.2 Standards and Guidelines

There are two types of standards and guidelines for cybersecurity.

- Government standards, such as:
  - National Institute of Standards and Technology (NIST) in U.S.
  - Federal Information Processing Standards (FIPS) in U.S.
  - Military Standards (MIL-STD or MIL-SPEC) in U.S.
  - Nomenclature of Territorial Units for Statistics (NUTS) in Europe
  - European Committee for Standardization (ECS/CEN)
  - European Committee for Electrotechnical Standardization (CENELEC)
  - European Telecommunications Standards Institute (ETSI)
- Open standards by technical communities, such as:
  - Institute for Electrical and Electronics Engineers (IEEE)
  - Internet Society (ISOC)
  - World Wide Web Consortium (W3C)
  - Internet Engineering Task Force (IETF)
  - Internet Architecture Board (IAB)
  - American National Standards Institute (ANSI)
  - International Organization for Standardization (ISO)

4.2.1 Government Standards

As examples of government standards, NIST publishes excellent computer / cyber / information security and guidelines, recommendations and reference materials at: http://csrc.nist.gov/publications/PubsSPs.html

There are 100+ standards, grouped into three series of special publications.

- NIST Special Publication 800 Series, Computer Security

    - NIST's primary mode of publishing computer / cyber / information security guidelines, recommendations and reference materials
- NIST Special Publication 1800 Series, Cybersecurity Practice Guides
    - A new subseries, created to complement the SP 800s, targets specific cybersecurity challenges in the public and private sectors and provides practical, user-friendly guides to facilitate adoption of standards-based approaches to cybersecurity
- NIST Special Publication 500 Series, Computer Systems Technology
    - A general IT subseries used more broadly by NIST's Information Technology Laboratory (ITL)

4.2.2 Open Standards by Technical Communities

As examples of open standard by technical communities, the Institute of Electrical and Electronics Engineers (IEEE) and Internet Engineering Task Force (IETF) publish many excellent cybersecurity standards.

- IEEE 1888.3-2013, Standard for Ubiquitous Green Community Control Network: Security
    - IEEE Standard for Ubiquitous Green Community Control Network: Security supports enhanced security management functions for sustainable computing. Included are security requirements, system security architecture definitions and a description of authentication and authorization. The standard helps avoid unintended data disclosures to the public and unauthorized access to resources.
- IEEE 1686-2013, Standard for Intelligent Electronic Devices Cyber Security Capabilities
    - IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities defines the functions and features to be integrated into intelligent electronic devices for critical infrastructure protection programs. Access, operation, configuration, firmware revision and data retrieval are addressed.
- IEEE P1711, Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
    - IEEE Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links specifies a practice that can protect the integrity and confidentiality of communications over phone lines, radio waves, fiber optics and more. The protocol could be implemented in new equipment or when retrofitting existing systems.
- IEEE P2030.102.1, Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems

  - IEEE Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems promotes the security of control systems deployed by electric utilities in four basic steps: defining functional requirements based on needs; selecting open-source specifications to meet those requirements; developing interoperable configuration profiles for the specifications; and testing and validating the configurations. The proposed standard would allow for functionality to be applied at the device level on a case-by-case basis. It offers guidelines that would make it easier for utilities to procure and implement secure systems, provide adequate security controls and minimize efforts to configure devices that support cybersecurity functions.
- IEEE P802.1AEcg, Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices
  - IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment: Ethernet Data Encryption Devices facilitates secure communication over publicly accessible networks for which security has not already been defined.
- IETF RFC 6749, OAuth Authorization Protocol
  - OAuth is an authorization protocol and is not primarily used to identify a user. OAuth provides a simple way to verify the access level of a request for a Web service. It provides a mechanism for application users to delegate access to a third-party (application backend services that will perform actions in the background) to work on behalf of the user.

4.3 Roles, Responsibilities and Authorizations (RRAs)

Roles, responsibilities and authorizations can be somewhat abstract (e.g., service provider or user) or refer to specific job titles for an organization (e.g., incident manager, threat management, forensics or senior information security officer).

4.3.1 Abstract RRAs

Service Providers (SP)

- A service provider is an entity that provides Web services. Examples of service providers include application service providers (ASP), storage service providers (SSP) and internet service providers (ISP).
- A service provider relies on a trusted identity provider (IdP) or security token service (STS) for authentication and authorization. In the Web Services Federation (WS-Federation) model a service provider is called a “relying party” (RP). In Security Assertion Markup Language (SAML), the XML standard for

exchanging data, the security domains that information is passed between are a service provider and an identity provider. SAML's service provider depends on receiving assertions from a SAML authority or asserting party, a SAML identity provider. Other service provider technologies important to identity management include software-as-a-service (SaaS), software offered using an application service provider (ASP) model and cloud computing providers.

Identity Providers or Brokers

- An identity provider, sometimes called an identity service provider or identity assertion provider, is an online service or website that authenticates users on the Internet by means of security tokens, one of which is SAML 2.0. In the WS-Federation Model, an Identity provider is a security token service. Service providers depend on an identity provider or security token service to do the user authentication. OAuth is an important protocol for IdP services as most major Web services are also identity providers, mainly through the use of OAuth. These include Google, Facebook, Yahoo, AOL, Microsoft, PayPal, MySpace and Flickr, among many more. Furthermore, all major email providers offer OAuth identity provider services.
- An identity provider can be described as a service provider for storing identity profiles and offering incentives to other SPs with the aim of federating user identities. It should be noted, however, that identity providers can also provide services beyond those related to the storage of identity profiles.
- An identity provider is responsible for: providing identifiers for users looking to interact with a system; asserting to such a system that such an identifier presented by a user is known to the provider; and possibly providing other information about the user that is known to the provider. This may be achieved via an authentication module, which verifies a security token that can be accepted as an alternative to repeatedly explicitly authenticating a user within a security realm.
- An example of this could be a website that allows users to log in with Facebook credentials and Facebook acts as an identity provider. So Facebook verifies that the user is an authorized user and returns information to the website (e.g., username and email address). Similarly, if a site allows login with Google or Twitter credentials, then Google and Twitter act as identity providers.
- In perimeter authentication, a user needs to be authenticated only once (single sign-on). The user obtains a security token that is then validated by an identity assertion provider for each system that the user needs to access.

Service Provider versus Identity Provider

- “Provider” is a generic way of referring to both IdPs and SPs. There are overlaps when it comes to defining identity providers versus service providers. According to the Organization for the Advancement of Structured Information Standards (OASIS), the organization that created SAML, an identity provider is defined as, “a kind of provider that creates, maintains and manages identity information for principals and provides principal authentication to other service providers within a federation, such as with web browser profiles.”
- A service provider is “a role donned by a system entity where the system entity provides services to principals or other system entities” and a federation is “an association comprising any number of service providers and identity providers.”
- In simple terms, and as they relate to identity management, an identity provider can be described as a service provider for storing identity profiles and offering incentives to other SPs with the aim of federating user identities. It should be noted, however, that Identity Providers can also provide services beyond those related to the storage of identity profiles.

Security Token Service (STS)

- Security tokens, sometimes called identity tokens, authentication tokens or even software tokens, play a major role in identity management, as they are the device of choice for authenticating and authorizing a user’s identity or “digital identity.”
- A security token service, sometimes mistakenly referred to as a secure token service, is the web service that issues security tokens. An STS is inextricably linked to website security, as it issues security tokens as they are defined in the WS-Security specification. In essence, an STS is a website trust identity provider. A SAML assertion in website trust is a kind of security token.

Threat Actor

- A threat actor is an entity that is partially or wholly responsible for an incident that impacts (or has the potential to impact) the security of an organization.

Alice and Bob

- Alice and Bob are commonly-used names for participants in security scenarios that involve cryptography. Alice represents Person A and Bob is a placeholder for Person B.

4.3.2 RRAs for Commercial and Civil Government Organizations

Typical roles, responsibilities and authorizations in a large commercial enterprise include the following.

Incident Management, Threat Management and Forensics

- These front-line defenders manage networks and mobile devices. Examples of their work are: managing networks to keep attackers out; testing other networks to assess their security and advising on making them less vulnerable; managing during incidents; analyzing events; and analyzing new malware / production of countermeasures.

Risk Analysts and Management

- Risk analysts and managers work to understand which threats will have the worst business impact and advise senior leaders in non-technical language why and how they should spend on reducing these risks. Risk managers may be non-technical or technical staff. Some risk-management personnel audit networks and ensure compliance and legal issues are addressed.

Policy Makers and Strategists

- Policy makers and strategists define how a company deals with different security risks, meets its legal obligations and gets policies implemented. The private sector has chief information security officers, who are often supported by a team. Government typically refers to them as IT security officers and departmental security officers.

Operations and Security Management

- Operations and security managers protect data on networks, laptops and mobile devices. They may manage encryption and other protective measures like firewall rules.

Engineering, Architecture and Design

- Engineering, architecture and design personnel typically design secure code and applications, architect secure systems and create new cyber security tools.

Education, Training and Awareness

- Education, training and awareness specialists train newcomers, keep experts up to date and enable staff or customers to benefit fully from the technology they use.

Research

- Research personnel may have a highly technical focus or be more policy or psychology oriented. Their work can include complex models to help understand and manage risks, or new technologies and ways to apply them to reduce risks. Often, they are looking for the next “big thing.”

Legal

- Lawyers and legal personnel provide expert advice and prosecution of data security and Internet crime. Their work is growing, given the increasing levels of crime and penalties for organizations that don’t sufficiently protect data.

4.3.3 RRAs for Military Organizations

The U.S. Department of Defense (DoD) Instruction # 8510.01 establishes cybersecurity policy and assigns responsibilities for DoD information technology systems, including responsibilities for the following functions.

- Principal Authorizing Official (PAO)
- DoD Senior Information Security Officer (SISO)
- DoD Component chief information officer (CIO)
- Authorizing Official (AO)
- Authorizing Official Designated Representative (AODR)
- Security Control Assessor (SCA)
- Program Manager (PM) or System Manager (SM)
- Information System Security Manager (ISSM)
- User Representative (UR)
- Risk Management Framework/Technical Advisory Group (RMF/TAG) Representative

4.4 Authentication Technologies

Communities need the ability to exchange between each other’s credentials by multiple and different methods. Authorization determines if the person, once identified, is permitted to have the resource, privilege or access. This is usually determined by finding out if that person is a part of a particular group, has paid admission or has a particular level of security clearance. Authentication is any process to verify that someone is who they claim they are, and identifies the participant of the session. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition or fingerprint. An example of authorization is showing a boarding pass at an airport and gaining access to the airline seat, or showing that your name appears on the guest list at an exclusive party.

You have probably used Windows, Forms and Basic (username/password) authentication protocols to verify your identity to the web service. WS-Federation is one such protocol that facilitates single sign-on (SSO) and brokering of identity between federation partners. This allows an individual to use a resource in a partner company if there is a trust established between the individual’s company and the partner company.

Authentication methodologies help determine: the process and methodology used by the federated community of identity providers for accepting the different digital identities; how one manages access to information based on that knowledge; and the processes used to share that information with the different roles. Suggested authentication methodologies include the following.

Cognitive Fingerprints

- Cognitive fingerprints evaluate a user’s behavior to provide a threat score (via a risk engine) to a user, which can be used as an input to the KeyVOMS tool to provide privileges/capabilities to a user. Reference:
    - KeyVOMS: https://wiki.openstack.org/wiki/KeyVOMS
    - Cognitive Fingerprints: http://securityaffairs.co/wordpress/34372/digital-id/cognitive-fingerprints-authentication.html

Integrated Access Control and Data Provenance

- Integrated Access Control and Data Provenance Modeling is a technical pattern by the University of Texas at Dallas that offers a solution to secure the complex net-centric application systems related to trustworthiness and security. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=7106544

NIST Cybersecurity Whitepapers on Authentication Technologies

- Measuring Strength of Authentication http://www.nist.gov/nstic/NSTIC-strength-authentication-discussion-draft.pdf

- Measuring Strength of Identity Proofing http://www.nist.gov/nstic/NSTIC-strength-identity-proofing-discussion-draft.pdf

- Attribute Metadata and Confidence Scoring http://www.nist.gov/nstic/NSTIC-attribute-confidence-metadata-discussion-draft.pdf

4.5 Authorization Technologies

Once identity has been authenticated, communities need the ability to authorize data sharing.

Authorization deals with access rights of the identity that is associated with the current session or context of the request. For example, Microsoft SharePoint uses role-based authorization, whereas WS-Federation utilizes claim-based authorization to evaluate the rights of a user session. The popular authorization method for web service APIs today revolves around OAuth, which allows third-party applications to perform operations on behalf of users.

With the complex mesh of internal and external applications, organizations are looking for the best method to secure access and make authorization decisions. There has been a lively debate in the IT community as to whether role-based access control (RBAC) or attribute-based access control (ABAC) is best suited for authorization management. There also exist RBAC / ABAC hybrids, as shown below in “Error! Reference source not found.”

4.5.1 Authentication Methodologies

Suggested authentication methodologies include the following.

Role-Based Authorization Control

- Role-based access control is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees and can implement mandatory access control (MAC) or discretionary access control (DAC). RBAC is sometimes referred to as role-based security. RBAC is a policy-neutral access control mechanism defined around roles and privileges. The components of RBAC, such as role-permissions, user-role and role-role relationships, make it simple to do user assignments. A NIST study demonstrated that RBAC addresses many needs of commercial and government organizations. RBAC can be used to facilitate administration of security in large organizations with hundreds of users and thousands of permissions. Although RBAC is different from MAC and DAC access-control frameworks, it can enforce these policies without any complication. Its popularity is evident from the fact that many products and businesses are using it directly or indirectly.

Attribute-Based Access Control

- Attribute-based access control is a model that evolves from RBAC to consider additional attributes in addition to roles and groups. In ABAC, it is possible to use attributes of the user (e.g., citizenship, clearance), resource (e.g., classification, department, owner), action and context (e.g., time, location, IP).
- ABAC is policy based, since it uses policies rather than static permissions to define what is allowed or not allowed.

Claim-Based Authorization Control (CBAC)

- Claim-based authorization control is an access-control paradigm that uses the claims to make access-control decisions to resources. In Windows, CBAC is built on the conditional access control entry (ACE) feature, not only to use the user claims, but also to use the resource claims, which are referred to as resource properties, in order to make access-control decisions.
- ACE is an entry in an access control list (ACL) that contains a set of user rights and a security identifier (SID) that identifies a principal for whom the rights are allowed, denied, or audited

Discretionary Access Control

- Discretionary access control (DAC) is a type of access control used as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)".
- Discretionary access control is commonly discussed in contrast to mandatory access control (MAC, sometimes termed non-discretionary access control).

Occasionally a system as a whole is said to have "discretionary" or "purely discretionary" access control as a way of saying that the system lacks mandatory access control. On the other hand, systems can be said to implement both MAC and DAC simultaneously, where DAC refers to one category of access controls that subjects can transfer among each other, and MAC refers to a second category of access controls that imposes constraints upon the first

Mandatory Access Control

- Mandatory access control refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) ports, shared memory segments, input/output (IO) devices, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object is tested against the set of authorization rules (aka policy) to determine if the operation is allowed. A database management system, in its access control mechanism, can also apply mandatory access control; in this case, the objects are tables, views, procedures, etc.

Access Control List

- An access control list, with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects as well as what operations are allowed on given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file object has an ACL that contains “Alice: read, write; Bob: read,” this would give Alice permission to read and write the file and Bob to only read it.

4.5.2 Authentication Tools

Authentication tools include KeyVOMS

- KeyVOMS is a method for authentication / authorization in a distributed environment to provide privileges and capabilities to computer users.

- A virtual organization (VO) is a security and collaboration context that is not exclusively associated with any one physical organization or site. A VO has members that are assigned roles / attributes that grant privileges. VO participants contribute resources (e.g., data and services). KeyVOMS is an example of a trusted, third-party VO management system.
- KeyVOMS is a re-purposed OpenStack Keystone service augmented with three pre-defined roles: VOMS administration, VO administration and VO site administration.
- KeyVOMS uses a modular, WSGI-based VO policy enforcement point (PEP), a component that serves as the gatekeeper and front door to a digital resource. When a user tries to access a file or other resource on a computer network, the PEP will describe the user’s attributes to the policy decision point (PDP), request a security decision and enforce that decision.

4.6 Human Interoperability Framework

4.6.1 Human Dimensions

Human interoperability is the understanding of the cognitive framework that permits the smooth transfer or exchange of information between humans, humans and systems, and human-social networks.

- Human-Human Interactions (e.g., hastily formed rapport)
- Social Networks (e.g., social media and information sharing)
- Human-System (e.g., interoperability between human, technologies and processes)
- Human-Machine Interface (e.g., cognitive match between sender and receiver)

Human interoperability permits governments and/or non-government organizations to rapidly build synergism that is reliable, effective and trusted in a net-centric environment among mission partners.

4.6.2 Cognitive Framework

Human-Human

The focus is on the interactions between humans (e.g., face-to-face, phone conversations, texting).

- Establish and sustain rapport for positive outcomes between parties.
    - Building an immediate, sustainable rapport and trust:
        - Minimizes misunderstandings and delays
            - Allows for parties to understand the intent of the message with minimal distortion, deletion and generalization of the original or intended message
        - Permits extraction and exchange of accurate information
            - Knowing how to ask questions based on the cognitive process being used by the sender so that accurate and trusted information can be retrieved quickly
        - Permits immediate repair of non-rapport communication transactions before, during and after conflicts or crisis
- Barriers
    - Limited experts in non-verbal communications hinders sustainable rapport and trust
    - Limited experts in native language that augments the non-verbal communication (knowing both minimizes interpretation, which can lead to negative outcomes)
    - Limited experts in strategic communication
    - Limited experts in negotiation, leadership skills and strategic planning and operations
- Examples
    - During a crisis, leadership should be able to assess which team members will be effective in assigned roles and which members will be liabilities.
    - By knowing how to assess non-verbal and verbal cues rapidly, rapport and trust can be established in hastily formed teams or networks within the first 5-10 minutes, followed by behavioral characteristic assessment.
- Solutions
    - Extensive training in the various forms of non-verbal and verbal cues identifies the cognitive-behavioral indicators of how parties are interacting within a specific context. The results give insight to social or cultural ramifications that need to be addressed.
    - Neuro-behavioral communications experts in the field and in the command control room
    - Strategic communications and planning experts that incorporate the first two solution bullets

Social Networks

The focus is on the interactions between humans within social networks.

- Establish and sustain rapport and trust across social networks.

  - Minimizes misunderstandings and delays
    - Allows for parties to understand the intent of the message with minimal distortion, deletion and generalization of the original message
    - Identifies the processes that are “compatible” for reliable, effective and trusted human-social networks
  - Permits extraction and exchange of accurate information
    - Knowing how to ask questions based on the sender’s mental process so that accurate and trusted information can be retrieved quickly
  - Permits immediate repair of communication transactions (rapport) before, during and after communication conflicts
    - Allows governments and non-government organizations to rapidly build synergism amongst mission and non-mission partners that is reliable, effective and trusted
- Assess policy, doctrine, standards and procedures pertaining to social networks and information sharing.
- Barriers
  - Language
    - Limited experts in the non-verbal communications
      - Understanding the universal language of non-verbal communication permits sustainable rapport and trust
    - Limited experts in native language or dialect
    - Limited experts in strategic communication
  - Cultural
    - Limited experts with knowledge of the culture or subcultures
  - Political
    - Limited experts with knowledge of the political environment
  - Policy/Legal
    - Limited experts with knowledge of the policy and legal aspects involving roles and functions of the various parties for information sharing (e.g., in-country versus foreign, agency 1 versus agency 2)
    - Policies must be flexible and adaptive to dynamic changes (e.g., neuro cyber security and critical infrastructure)
- Examples
  - After Hurricane Katrina in 2005, critical social networks broke down. People left critical posts to be with family, which was an unexpected behavior.
  - The lack of understanding by the general public delayed the response by the Department of Defense in providing assistance.
- Solutions
  - Form a matrix of cognitive, behavioral and social experts who can provide assistance before, during and after a crisis.
  - During a crisis, a cognitive / behavioral / social team should be formed to provide immediate support to leadership and first responders.

  - Team should be led by an individual with an engineering or business background and experienced in strategic and analytical integrated solutions to support field operations and/or a centralized command post.

Human-System

The focus is on the human interactions with the system and/or network process.

- Assess human factor indicators / attributes that contribute to trust or mistrust factors of the human-system interaction.
- Assess enablers / inhibitors for sharing information and behaviors across diverse cultural domains.
- Assess data integrity with respect to human point of entry and point of failure.
- Assess policy, doctrine, standards and procedures pertaining to human-systems for information sharing, alignment, adaptability, agility, integrity and cognitive framework.
- Barriers
  - Engineers and computer scientists being the experts of the system process for human interoperability
- Solutions
  - From the cognitive-behavioral-social expert matrix, identify a column for system / network process and interoperability experience.
  - Consider having these experts generate a study for first two bullets.
  - Consider having this group be part of field exercises to assess the last two bullets.

Human-Machine Interface

The focus is on graphical user interface for cognitive matching (when the receiver understands the message as intended by sender).

- Establish flexible and adaptive guidelines for best practices in developing user interfaces.
- Barriers
  - Instead of human factor experts, computer scientists and engineers construct user interfaces.
  - Developers consider user interface design the least significant piece of a system, network or website. It is, in fact, one of most important pieces of the infrastructure. It is this end point where humans interact with the rest of the ecosystem/environment and where most of the inherent errors occur.
- Solutions
  - Incorporate human factor experts into the design and operational teams and policy review teams.

4.7 Use Cases

Use cases are helpful for focusing a cybersecurity design and for testing to verify functionality. Three use cases are presented.

4.7.1 Air Traffic Management

Air traffic management includes the following system of systems (SoS).

- System Wide Information Management (SWIM)
  - The U.S. Federal Aviation Administration (FAA) System Wide Information Management (SWIM) provides easy access to a wide range of air traffic control and management information, allowing users of the National Airspace System (NAS) to tap into the information they need, when they need it, through a single connection.
  - Automatic Dependent Surveillance–Broadcast (ADS-B)
    - The FAA Automatic Dependent Surveillance–Broadcast is the more precise, satellite-based successor to radar. ADS-B Out uses GPS technology to determine an aircraft's location, airspeed and other data, and broadcasts that information to a network of ground stations, which relays the data to air traffic control displays and to nearby aircraft equipped to receive the data via ADS-B In. ADS-B In also provides weather and traffic position information to be delivered directly to the cockpit.
  - Air Traffic Decision Support Systems
    - Air traffic decision support tools suggest and help implement faster and more effective responses to evolving conditions by sharing share data among stakeholders who develop collaborative solutions. They enable data collection for performance measurement and metrics reporting, which improve air traffic flow and overall airspace system capacity.

Activities of Aircraft

Activities of aircraft and air traffic control are shown in Figure 4-2 and Figure 4-3.

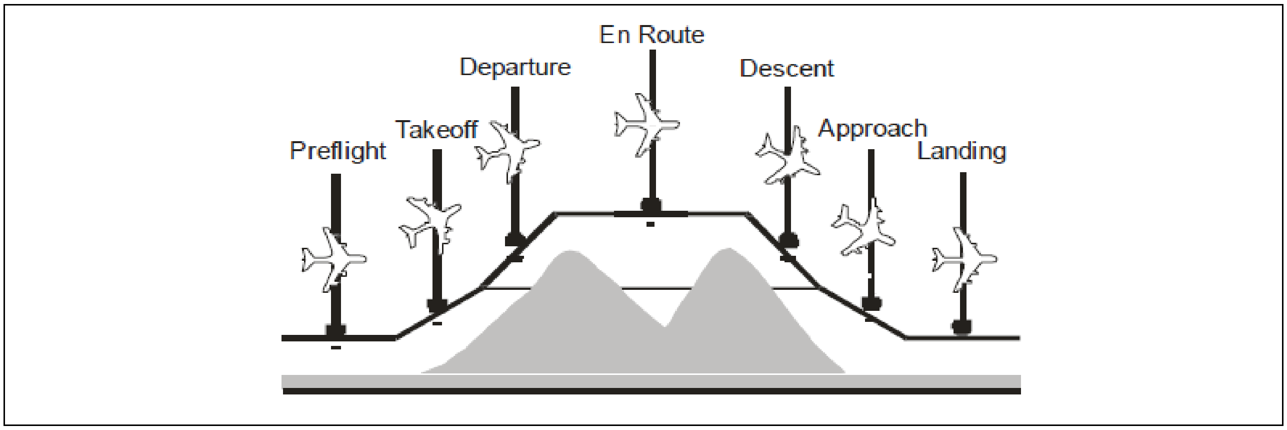


Figure 4-2. Activities of Aircraft in Air Traffic Management.

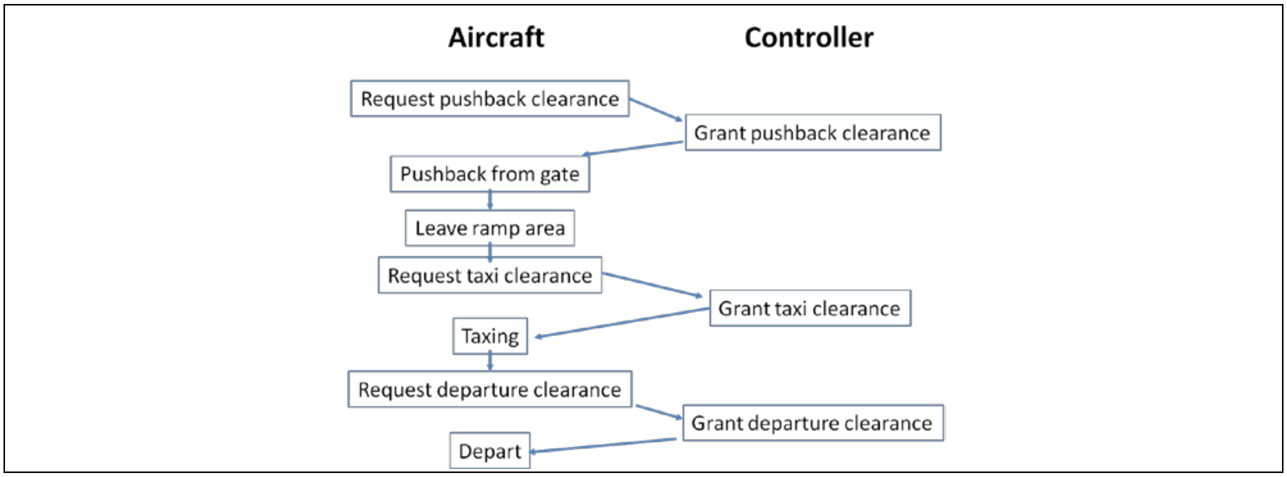


Figure 4-3. Handshake of Aircraft Request and Controller Approval in Air Traffic Control.

4.7.2 Disaster Response

The use case for disaster response is best shown using the U.S. Department of Defense Architecture Framework to describe architectures that ensure a common understanding. This is shown in Figure 4-4 through Figure 4-6.

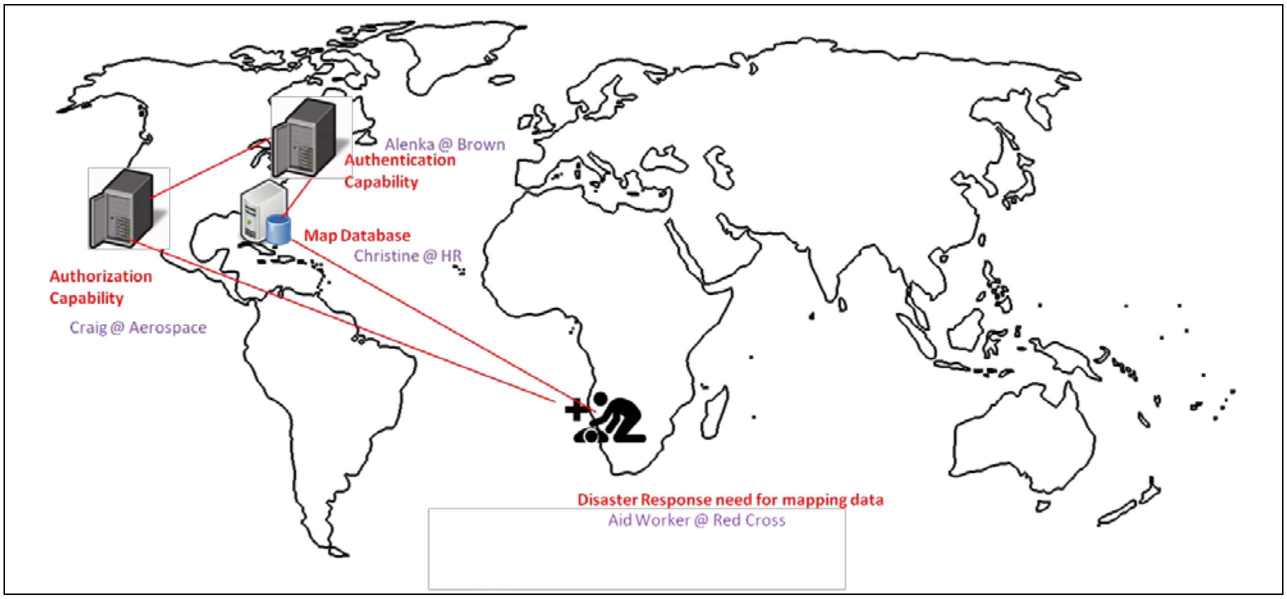


Figure 4-4. Operational View of Disaster Response: Authentication and Authorization (OV-1).

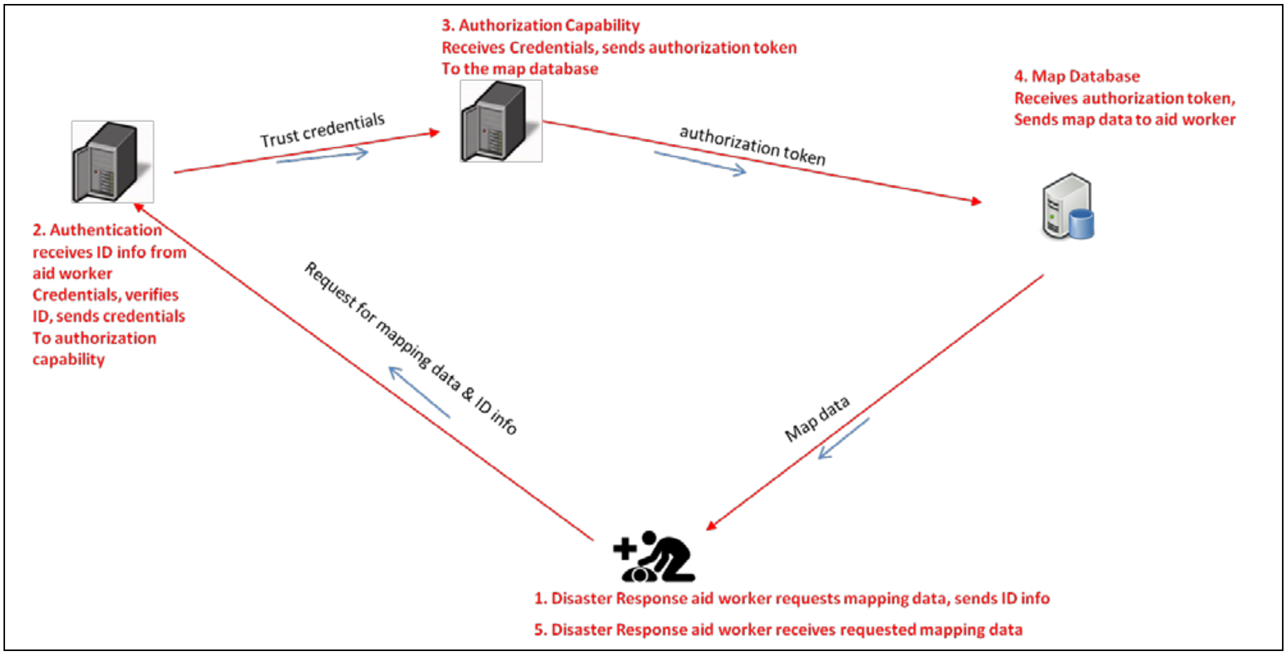
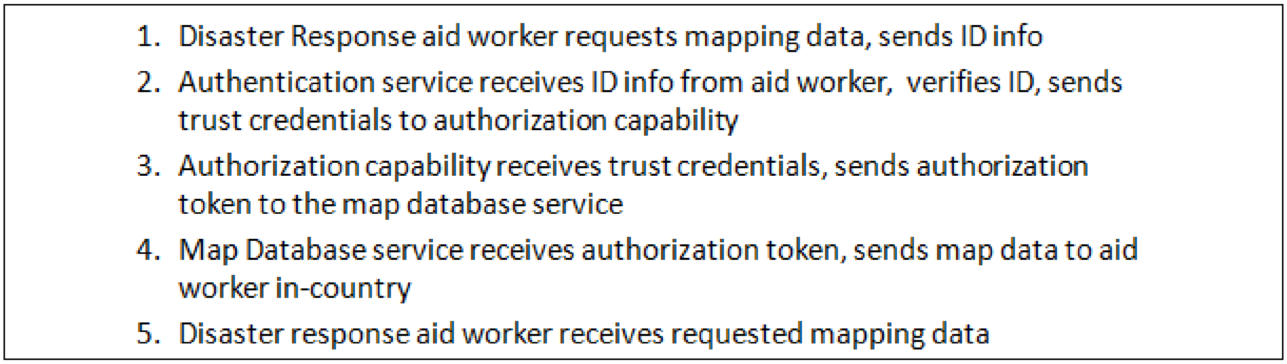

3. Authorization Capability
Receives Credentials, sends authorization token
To the map database
4. Map Database
Receives authorization token,
Sends map data to aid worker
Trust credentials
authorization token
2. Authentication
receives ID info from
aid worker
Credentials, verifies
ID, sends credentials
To authorization
capability
Request for mapping data & ID info
Map data
1. Disaster Response aid worker requests mapping data, sends ID info
5. Disaster Response aid worker receives requested mapping data

Figure 4-5. Message View of Disaster Response: Authentication & Authorization (SV-2).



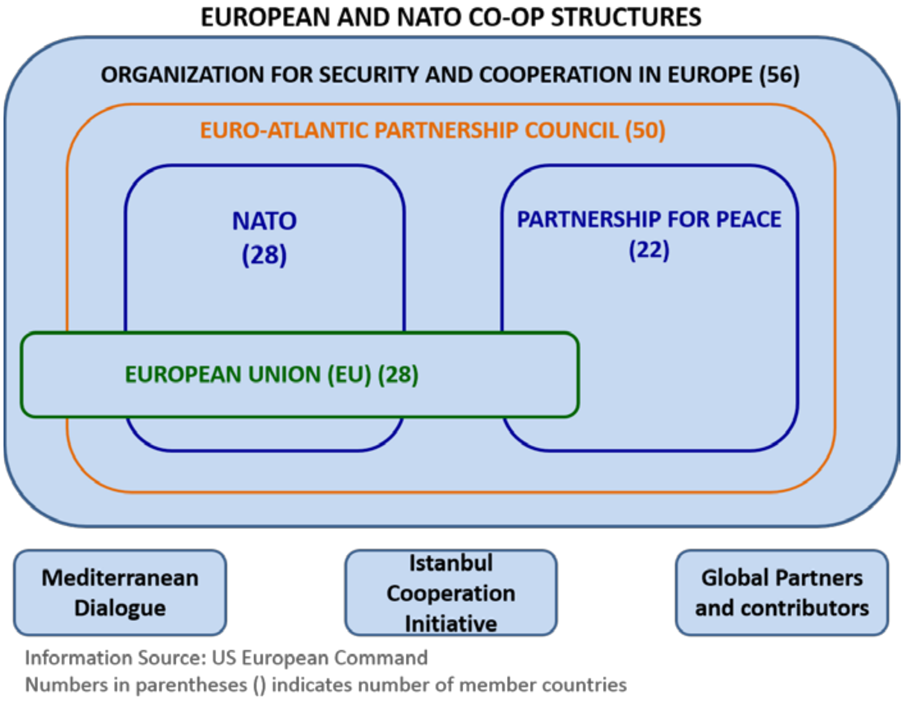
1. Disaster Response aid worker requests mapping data, sends ID info
2. Authentication service receives ID info from aid worker, verifies ID, sends trust credentials to authorization capability
3. Authorization capability receives trust credentials, sends authorization token to the map database service
4. Map Database service receives authorization token, sends map data to aid worker in-country
5. Disaster response aid worker receives requested mapping data

Figure 4-6. Event View of Disaster Response: Authentication and Authorization (OV-6C).

4.7.3 U.S. Department of Defense European Command (EUCOM) Use Case

Coordination among government and non-government organizations within Europe and individual countries within Europe. Figure 4-7 illustrates the complexity of possible cooperative structures within a EUCOM use case.

- Refugee support across borders – Humanitarian Operations Support to European Reinforcement Initiative (ERI)
- Disaster response and emergency response efforts
- Healthcare support across borders
- Search and rescue efforts as needed across Europe
- Support interagency partnering
- How to connect military to civilian society
- How to disconnect when done / needed


EUROPEAN AND NATO CO-OP STRUCTURES
ORGANIZATION FOR SECURITY AND COOPERATION IN EUROPE (56)
EURO-ATLANTIC PARTNERSHIP COUNCIL (50)
NATO (28)
PARTNERSHIP FOR PEACE (22)
EUROPEAN UNION (EU) (28)
Mediterranean Dialogue
Istanbul Cooperation Initiative
Global Partners and contributors

Information Source: US European Command
Numbers in parentheses () indicates number of member countries

Figure 4-7. European / NATO Cooperation Structures

4.8 Threat Modeling

Threat modeling is useful for focusing a cybersecurity design and for testing to verify functionality. It is also useful for conducting experiments and exercises.

A methodology is shown below for conducting threat modeling.

- Document missions and metrics for system performance and mission success (all stakeholders)
- Document threat models
- Document use cases
- Develop virtual testbed to model the system of systems
- Conducts tests on virtual testbed and measure SoS functionality across four conditions
    - No cyber threats versus no security controls
    - Various cyber threats versus no security controls
    - No cyber threats versus various cyber security control

  - Various threats versus various cyber security controls

Examples of cybersecurity threats and experimentation/exercises are shown below.

- Cybersecurity threats to air traffic control systems
  - During cybersecurity exercises, the United Kingdom National Air Traffic Control Services (UK NATS) performed simulated cyber attacks into the UK air traffic control system.
    - During the exercise, the cyber hackers shut down UK's air traffic control by hacking into the human resources (HR) department of the UK air traffic control system and firing all of the air traffic controllers, such that none showed up for work.
    - The cyber attackers succeeded by exploiting gaps in the government infrastructure. While much of the air traffic control infrastructure was well protected, the HR server wasn't secure (the weak link).
- Cybersecurity threats to seaport security
  - During cybersecurity exercises, the cyber hackers shut down the port by hacking into the security card system for the thousands of union workers use to gain access to the dock. Thus, by taking down the security card system, all dock workers were prevented from driving onto docks and the port was shut down.
  - Even worse, due to the confusion caused by thousands of angry union workers and security guards not able to get to work and clogging the roads leading to the port, hackers inadvertently allowed terrorists the ability to gain access to toxic chemicals and explosives stored at the port, which allowed them (in the simulated exercise) to explode a dirty bomb and shut down the entire port city.
- Cybersecurity threats to automobiles are shown in Figure 4-8. (Source: Center for Automotive Embedded System Security, http://www.autosec.org)

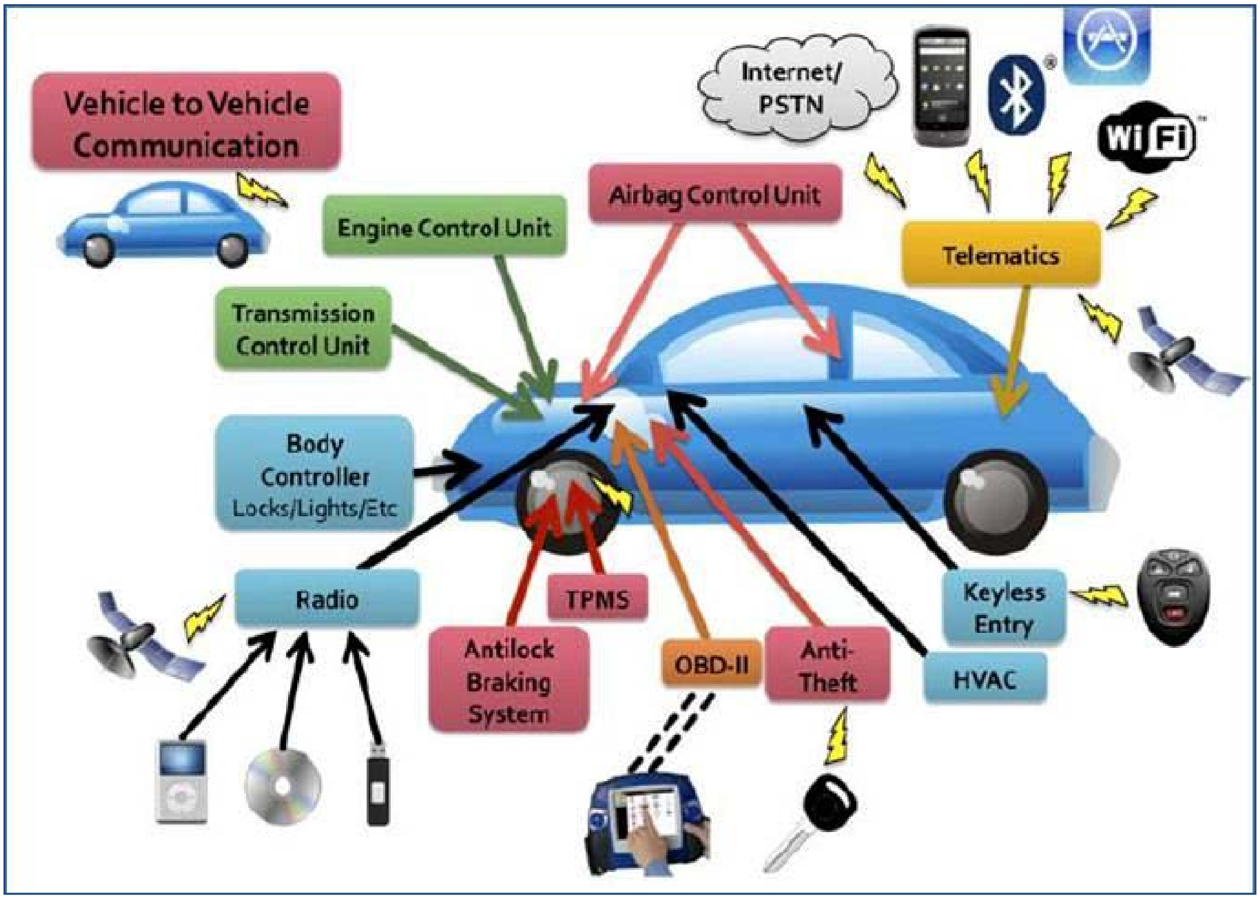


Figure 4-8. Automotive Cybersecurity Attack Surfaces.

4.9 Layered Security and Defense in Depth

Layered security or layered defense describes the practice of combining multiple mitigating security controls to protect resources and data. The term bears some similarity to defense in depth, a term adopted from a military strategy that involves multiple layers of defense (e.g., castle moat, outer walls, draw bridge, etc.) that resist rapid penetration by an attacker but yield rather than exhaust themselves by too-rigid tactics. As the incursion progresses, resources are consumed and progress is slowed until it is halted and turned back. The use of the term defense in depth in cybersecurity assumes more than merely technical security tools deployment. It also implies policy and operations planning, user training, physical access security measures and direct cybersecurity personnel involvement in dealing with attempts to gain unauthorized access to information resources. Within a defense-in-depth security strategy, layered security is often merely a delaying tactic used to buy time to bring security resources to bear to deal with a malicious security cracker's activities.

A definition of layered security is combining multiple mitigating security controls to protect resources and data. Layered security is an example of the Swiss cheese model or cumulative act effect used in risk analysis and risk management and shown in Figure 4-9 (adapted from D. Orlandella and J. T. Reason's Swiss cheese model). In this model, security systems are likened to multiple slices of Swiss cheese, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the fact that it must pass through "holes" in the defenses (i.e., not be trapped and detected by each different defense). These defenses are of different kinds and locations are "layered" behind each other. Therefore in theory, lapses and weaknesses in one defense do not easily allow a risk to materialize, since other defenses also exist to prevent a single point of weakness.

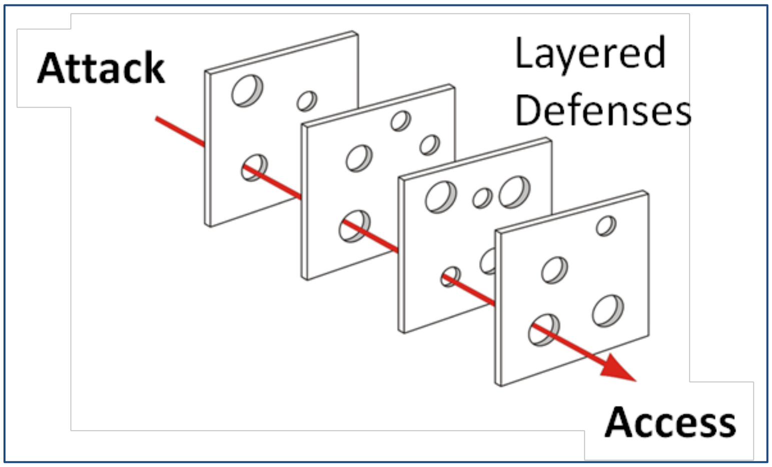


Figure 4-9. The Swiss Cheese Model for Layered Defenses.

The techniques for layered security

- Technical security tools deployment
- Policy and operations planning
- User training
- Physical access security measures
- Information assurance personnel directly involved in monitoring and preventing cyber attacks

Within a defense-in-depth security strategy, layered security can be a delaying tactic used to buy time to bring security resources to bear to deal with a cyber-attack.

There are two strategies for layered security.

- Enterprise layered security strategy
  - Workstation application whitelisting
  - Workstation system restore solution
  - Workstation and network authentication
  - File, disk and removable media encryption
  - Remote access authentication
  - Network folder encryption
  - Secure boundary and end-to-end messaging
  - Content control and policy-based encryption
- Consumer layered security strategy
  - Extended validation (EV) secure sockets layer (SSL) certificates
  - Multifactor authentication
  - Single sign-on
  - Fraud detection
  - Risk-based authentication
  - Transaction signing and encryption
  - Secure web and e-mail
  - Open fraud intelligence network

4.10 Rules and Conditions For Graceful Lowering (Degradation) of Security Controls

Since cybersecurity controls and postures will need to be changed over time, there is a need for rules or triggers for managing changes to the security controls. These triggers, conditions and protocols control the when and why for changing the security controls (e.g., from high to medium after a natural disaster).

Rules

- Methodology a data manager or data supplier follows: the how (e.g., change the rules so that the data manager should provide access to data when requestor only has driver’s license number, whereas manager would normally require key card and biometric)
- How to authenticate requestor without normal credentials
- How to authorize data sharing without normal credentials

Goals for Rules and Conditions

- Create rules that are granular and specific to drive cybersecurity solutions into implementation on a disaster response cloud-based virtual solution

- Create rules that permit the adaptive management of trust and access in a dynamic and evolving disaster scenario
- Create rules that are portable and can be geospatially and temporally translated across event types places and times
- Create rules that support a virtual organization construct, where people can be assigned roles and granted adaptively managed access to data, software services and communications channels, based on many types of circumstances
- Create rules that can manage monitoring and access management in trust federations
- Create rules that can be implemented in open fashion for the functional blocks that represent
  - Monitoring
  - Activity behaviors
  - Trust level
  - Event severity level
  - Access management parameters
  - Cloud brokerage functionality