# Technical Perspectives on Cyber Security and Information Assurance R&D

*Part II provides technical perspectives on the cyber security and information assurance R&D topics identified in Part I. The R&D topics are grouped into eight broad categories. Each technical perspective, prepared and reviewed by agency officials with expertise in the topic, describes the topic and its importance, the state of the art, and gaps in current capabilities.*

## 1. Functional Cyber Security and Information Assurance

The R&D topics in this category address technologies and capabilities that minimize the impact of compromises or potential compromises of data, networks, and systems, or that enable them to prevent, detect, resist, or respond to attacks. Topics in this category are:

- Authentication, authorization, and trust management
- Access control and privilege management
- Attack protection, prevention, and preemption
- Large-scale cyber situational awareness
- Automated attack detection, warning, and response
- Insider threat detection and mitigation
- Detection of hidden information and covert information flows
- Recovery and reconstitution
- Forensics, traceback, and attribution

### 1.1 Authentication, Authorization, and Trust Management

**Definition**

Authentication is the process of verifying the identity or authority of a network or system user (which can be a human user or a computer-based process or device) through a secure means such as digital signatures, passwords, tokens, or biometric features. Authorization, which takes place after authentication, refers to the privileges granted to an authenticated user who has requested access to services or resources. (Section 1.2 discusses access control in greater detail.) Authentication and authorization are interdependent; authorization to use a network or system resource frequently includes establishing the identity of the user requesting access (e.g., identity-based authentication) or verifying that a trusted third party has certified that the user is entitled to the access requested (e.g., credential-based authentication). Privilege is a security attribute shared by users whose identities have been authenticated. Cross-domain credentialing allows distinct systems, connected across a network, to provide access based on the secure identification procedure performed by one of the other networked systems. Trust management consists of making assessments of sets of credentials to determine whether they constitute adequate evidence for authorization.

### Importance

Authentication is fundamental to all information security because it connects the actions performed on a computer to an identified user that can be held accountable for those actions. The expanding means available for accessing networks make security breaches and uncontrolled user access a growing concern. As enterprise IT systems continue to grow in complexity and number of users, authorization technologies that enable authenticated users to be assigned varying levels of system access privileges will play an increasingly critical role in security management.

### State of the Art

Authentication of a user is based on one or more of three factors: a physical attribute (e.g., fingerprint or biometric data), an artifact (e.g., an automatic teller machine [ATM] card or cryptographic token), and/or a data key (e.g., a password). Each has advantages and disadvantages. The best-known and most common authenticators are conventional static passwords. Compromised static passwords, however, are a common vulnerability because users are careless about keeping their passwords secret, password security policies (such as mandatory format rules and periodic changes) are difficult to enforce, and malicious attackers have technological and social tools for discovering and accessing passwords. The use of multi-factor authentication methods may increase assurance. For example, an ATM might require both an ATM card and a password or personal identification number to provide a higher level of assurance than is provided by either factor alone.

Biometric technologies for authentication use measurements for identifying people – for example, their fingerprints, voice, retinal scans, or even handwriting – that can be used in IT authentication. But biometric data raise privacy issues that may in some instances limit their usage. Moreover, while biometric authentication can be used to provide stronger assurance of identity beyond that achievable with static passwords, biometrics are also susceptible to compromise. For example, recent experiments with artificial fingers have shown that fingerprint recognition devices can be fooled.

### Capability Gaps

The current technologies described above all have limitations that frustrate efforts of system security managers to increase overall security levels for networks, systems, and information. Next-generation concepts that both streamline and harden authentication, authorization, and trust management technologies and tools are needed to help mitigate vulnerabilities associated with changing network dynamics and increased security threats. Specific R&D needs include:

**Device authentication:** Device authentication requires equipping devices with characteristics that can be reliably recognized. For devices and associated processes that generate requests, authentication using cryptographic protocols may be required. Some of these protocols have been developed, but there has been little experience with deploying them and building systems that make good use of them.

**Scalable authentication:** Federated identities are a capability that enables organizations to share trusted identities across the boundaries of their networks – with business partners, autonomous units, and remote offices. These technologies offer the prospect of scalable authentication needed for scalable trust management. However, there are continuing challenges in defining common authentication identities and, more important, in the forms of authorization that the inter-domain authentication will support. This problem has been partially addressed in some of the most common application areas such as the use of credit cards for electronic commerce on the Internet. However, scalable authentication, or global-scale identity management, remains a challenge (e.g., see the *Hard Problem List,* INFOSEC Research Council, November 2005, for elaboration).

## 1.2 Access Control and Privilege Management

### Definition

Access control and privilege management begin with the administrative and mechanical process of defining, enabling, and limiting the operations that users can perform on specific system resources. The permission or limitation of operations is based on the business rules or access policies of the organization.

Access control policies are enforced through a mechanism consisting of a fixed system of functions and a collection of access control data reflecting the configuration of the mechanism. Together, these map a user's access request to the decision of whether to grant or deny access. The access control data include a set of permissions, each indicating a user's authorization to perform an operation (e.g., access, read, write) on an object or resource. Permissions are not individually specified. They are organized in terms of, and mapped through administrative operations or a predefined set of rules on to, a set of user, subject (process), and resource attributes associated with a specific type or class of policy.

For example, under an access control management approach called Role-Based Access Control (RBAC), permissions are defined in terms of roles that are assigned to users and privileges that are assigned to roles. Other approaches include label-based access control mechanisms that are defined in terms of labels applied to users, processes, and objects, and discretionary access control mechanisms that are defined in terms of user identifiers, user groups, and access control lists.

### Importance

Although access control is often specified in terms of limitations or protections, the ability of an organization to enforce access control policy is what ultimately enables the sharing of greater volumes of data and resources to a larger and more diverse user community.

### State of the Art

Various security mechanisms now exist for enforcing secure access within host operating systems and across heterogeneous bodies of data. In an attempt to streamline the management of access control, RBAC models and more recently an RBAC standard have been developed. RBAC offers administrative efficiency and the capability to intuitively administer and enforce a wide range of access control policies.

In RBAC, permissions are associated with roles and roles are assigned to users in order to grant user permissions corresponding to those roles. The implementation of this basic concept greatly simplifies access control management. Roles are centrally created for the various job functions in an organization, and users are assigned roles based on criteria such as their positions and job responsibilities. Users can be easily reassigned roles. Roles can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. For example, if a user moves to a new function within the organization, the user can be assigned to the new role and removed from the old one with associated privileges updated automatically. In the absence of RBAC, the user's old privileges would have to be individually identified and revoked, and new privileges would have to be granted.

Although RBAC represents a clear improvement over simple table lookup models of the access control matrix (data structures such as access control lists), the RBAC model does not solve all access control and privilege management problems. Discovering and defining roles and mapping roles to enterprise resources and applications, commonly referred to as role engineering, are costly and difficult. Although the development of best practices and tools to ease the transition to RBAC would be helpful, these capabilities provide only an interim solution to the research objectives described below. Ultimately, access control should be redefined and re-engineered from the ground up to reflect the increasing scale and complexity of networks and systems of systems. The goal should be a redefinition that preserves access control advancements while providing a generalized context to accommodate well-known and ad hoc access control policies, is easy to deploy and manage, and is safe in its configuration.

## Capability Gaps

To move toward the next generation in access control and privilege management technologies, advances in three separate but related R&D areas are needed: 1) scalable access control data management methods and tools; 2) flexible access control mechanisms capable of enforcing a wide variety of access control policies; and 3) methods and techniques for defining safe and secure access control configurations.

**Scalable access control data management:** Many organizations have hundreds or even thousands of systems, hundreds to hundreds of thousands of users, and thousands to millions of resources that must be protected. Managing access control data across these systems, users, and resources is a monumental task and perhaps the most expensive and error-prone of all security disciplines.

Identity-based access control models work well for small workgroups. But as the number of groups and users and the number and variety of resources they need to access grows to an enterprise- and cross-enterprise scale, access control information stored in applications, databases, and file systems grows so large that managing and controlling access changes can overwhelm even the most knowledgeable administrators. Visualizing and reasoning about a virtual ocean of access control data become impossible. For example, many enterprises are unable to make even the simplest queries, such as what system accounts exist for a given user. Consequently, organizations have resorted to implementing poor administrative practices such as account sharing and cloning of permissions, resulting in permissions becoming over-distributed and difficult to manage.

**Flexible access control mechanisms:** One size does not fit all access control policies. Access control mechanisms are as diverse as the types of business practices and applications that need to enforce them. An access control mechanism that meets the policy requirements within one market domain may be inappropriate in another.

Effective access control mechanisms provide a context for policy configuration, embodiment, and enforcement. Policy configuration refers to the administrative operations of creating and managing access control data. Embodiment refers to the storage of access control data that reflect the policy. Enforcement applies access control data so that users and their processes adhere to the access control policy. Since the mid 1970s, security researchers have sought to develop access control models as abstractions of access control systems. When implemented, the models provide a generalized context that supports a wide collection of policies, while adhering to an agreed-upon set of security principles such as least privilege (restricting a user to the minimum privileges needed to complete authorized tasks) and separation of duty (assigning roles and privileges such that no single user can perform multiple sensitive tasks). Revocation (removing privileges previously granted to principals) is also a key feature of these models.

The process for users to specify rich policies remains challenging. This is partly a user-interface problem and partly a problem of designing an intuitive model through which security configuration options can be conveyed to users. Some progress has been made in designing flexible mechanisms, though challenges remain (e.g., implementing least privilege or revocation on a wide-scale basis is difficult). These mechanisms have not yet been widely deployed.

**Safety:** In the context of access control, safety is the assurance that an access control configuration will not result in the leakage of a privilege to an unauthorized user. Safety is fundamental to ensuring that the most basic access control policies can be enforced. Unfortunately, there is a tension between the need for safety and the desire for flexibility. The safety of an access control configuration cannot be specified using a general access control model. Consequently, safety is achieved either through the use of limited access control models or the verification of safety via constraints. Currently, almost all safety-critical systems use limited access control models because constraint expression languages are too complex for easy administrative use. However, researchers have determined that most constraints belong to one of a few basic types (e.g., static, dynamic, or historical).

Therefore, a key research goal is to develop ways to formulate constraints that allow the safety of access control configurations to be ensured, while having these constraints be flexible enough to support practical applications.

## 1.3 Attack Protection, Prevention, and Preemption

### Definition

An attack is an attempt to gain unauthorized access to a network's or a system's services, resources, or information, or to compromise a network's or a system's integrity, availability, or confidentiality. Network or system owners can adopt practices and technologies that improve resistance to attacks or that prevent attacks from disrupting communications or operations, or from compromising or corrupting information.

### Importance

Attack protection, prevention, and preemption are essential functional cyber security capabilities. Their goal is to provide an enterprise-wide capability to intercept a malicious attack, thereby preventing disruption, compromise, or misappropriation of networks, systems, or information. Robust attack protection, prevention, and preemption capabilities help mitigate threats and reduce the ability of adversaries to exploit vulnerabilities.

There are two different attack protection, prevention, and preemption strategies. The proactive strategy shields healthy network or system components or services to prevent them from becoming contaminated, corrupted, or compromised. The reactive strategy temporarily isolates compromised network or system components or services to prevent them from contaminating, corrupting, or compromising healthy assets. To be effective, both the proactive and the reactive security capabilities need to be deployed at all levels of enterprise systems.

In addition, attack protection, prevention, and preemption capabilities should be governed by a flexible, adaptable concept of operations. Not all attacks have the same scope or operational impact. Accordingly, the configuration and operation of the attack protection, prevention, and preemption capability should change in accordance with attack severity and intent (i.e., the approach must be adaptable to the nature of the attack and the assets being attacked).

### State of the Art

A variety of laws, regulations, and/or institutional policies require agencies and other organizations to be able to respond to security incidents, prevent disruption to normal operations, and isolate compromised networks and systems. Many current commercial offerings are primarily limited to reactive intrusion-detection tools using signature- and rule-based algorithmic techniques, which use preset identification rules to distinguish authorized from unauthorized access. These tools are labor-intensive to use, require constant updating, and provide only limited protection. Even though updates are released much more quickly today than in the past, the result is an arduous configuration control and patch management task.

For example, major vendors are constantly issuing updates and patches to operating systems or applications to fix security holes. In some instances, these updates and patches reopen existing vulnerabilities or create new ones while fixing the targeted problem. Many organizations, such as those operating safety-critical infrastructure systems, have policies that require all upgrades and patches to be thoroughly tested before being deployed to operational systems. But hackers now are also able to reverse-engineer patches to discover the vulnerabilities and rapidly launch attacks that exploit them before the patches can be widely deployed. This becomes a recurring cycle as new upgrades and patches are released more frequently and reverse engineering methods used by hackers improve.

### Capability Gaps

Amid these security conditions, reactive capabilities and manual responses are inadequate. Automated responses that operate in milliseconds and emphasize preemption and prevention are needed, along with

next-generation systems that are fundamentally more robust and resilient. Furthermore, organizations need to abandon the view that any single product can secure its IT infrastructure. Rather, the focus should be on developing an integrated set of tools and techniques that provide a comprehensive, layered, enterprise-wide attack protection, prevention, and preemption solution.

Proactive behavior-based systems may offer the best option for developing the next generation of attack protection, prevention, and preemption capabilities. These systems will not depend on signatures or rules to identify attacks. Proactive behavior-based tools identify precursor events early in the attack timeline. These systems, when the technologies mature, will provide the capability to identify and preempt unknown and novel attacks. Some research has been done in this area, and early attempts at behavior-based responses are starting to emerge in commercial products. This work should be continued with the goal of making robust products available, and it should be expanded to include the capabilities highlighted below.

Protection is needed at all layers of a protocol stack, such as the seven-layer International Standards Organization (ISO)/Open Systems Interconnect (OSI) Technical Reference Model (TRM) (see box below). Current attack preemption R&D primarily addresses Layer 3 (network layer) attacks generated by outsiders. Additional protection, prevention, and preemption features and functionality that are needed include a host-based intrusion prevention capability that is independent of the platform, operating system, and applications.

Related research is needed to increase and verify the robustness and resilience of networks, systems, and components to withstand attacks, especially unknown or novel attacks. Work is also needed to improve the ability of networks, systems, and components to

### ISO/OSI Technical Reference Model Layers

**Layer 1 – Physical**
This layer conveys the bit stream – electrical impulse, light or radio signal – through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards, and other physical aspects.

**Layer 2 – Data Link**
At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control, and frame synchronization. The data link layer is divided into two sublayers: the Media Access Control layer and the Logical Link Control layer.

**Layer 3 – Network**
This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control, and packet sequencing.

**Layer 4 – Transport**
This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.

**Layer 5 – Session**
This layer establishes, manages, and terminates connections between applications. It sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.

**Layer 6 – Presentation**
This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. It works to transform data into the form that the application layer can accept, and it formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

**Layer 7 – Application**
This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Tiered application architectures are part of this layer.

*Source: Cisco Systems, Inc.*