Enterprise-Level Security: Securing Information Systems in an Uncertain World

William R. Simpson

Adversaries continue to penetrate U.S. information technology networks, and in many cases, they have infiltrated the online environment, jeopardizing the confidentiality, integrity, and availability of enterprise information and systems. A multitude of network-related incidents have shown that the fortress model of securing information systems—hard on the outside, soft on the inside—falsely assumes that the boundary between hard and soft can prevent all types of penetration. Given this vulnerability of boundaries, network attacks are pervasive, and nefarious code is present even in the face of system sweeps to discover and clean readily apparent malware.

Early calculations show that ELS-enabled applications can save 90–95 percent of recurring man-hours and eliminate up to 3 weeks of time used for access request processing.

Information Security at the Enterprise Level

Members of all branches of the military must have access to the systems and information they require to execute their missions. The current authorization paradigm requires a cadre of highly privileged administrators to maintain user account permissions for every system and data source required. Human errors, delays in request processing, and credential misuse add to the enormous risks these people face daily. Further aggravating the challenges to successful mission execution and future operations is the determined presence of malicious actors in the contested environment.

Enterprise-level security (ELS) is a web-based security architecture designed to select and incorporate technology into a cohesive set of policies and rules for an enterprise information system. The ELS architecture is based on core security tenets that reflect the enterprise's overall goals and security philosophy. From these tenants, requirements for core security operations are derived to support information sharing within and outside the enterprise.

ELS provides application- and data-level security and is a viable, scalable alternative to current access control management. The initial standup of ELS will cost approximately 75 percent of the annual recurring costs for the current process, and will save thousands of system administration man-hours.

The techniques the architecture employs are resilient, secure, extensible, and scalable. ELS has been tested and is mature in its development. ELS has been named as a potential solution to the identity and access management needs of the Department of Defense's Joint Information Environment, and it is ready to become that solution.

Tenets Guide Decisions and Contribute to Security Principles

ELS is a capability designed to counter adversarial threats by protecting applications and data with a dynamic attribute-based access control solution. ELS helps provide a high-assurance environment in which information can be generated, exchanged, processed, and used. ELS design is based on a set of high-level tenets that are the overarching guidance for every decision made, from protocol selection to product configuration and use (see box). From there, a set of enterprise-level requirements are formulated that conform to the tenets and any high-level guidance, policies, and requirements.

The basic tenets used at the outset of the ELS security model are as follows:

0. Malicious entities are present
1. Simplicity
2. Extensibility
3. Information hiding
4. Accountability
5. Specify minimal detail
6. Service-driven rather than a product-driven solution
7. Lines of authority should be preserved
8. Need-to-share as overriding need-to-know.
9. Separation of function
10. Reliability
11. Trust but verify (and validate)
12. Minimum attack surface
13. Handle exceptions and errors
14. Use proven solutions
15. Do not repeat old mistakes

Current paper-driven access control processes for enterprise operations are plagued with ineffectiveness and inefficiencies. Given that tens of thousands of government and military personnel transfer locations and duties annually, delays and security vulnerabilities are introduced daily into operations. ELS mitigates security risks while eliminating much of the system administration required to manually grant and remove user and group permissions to specific applications/systems. Early calculations show that ELS-enabled applications can save 90–95 percent of recurring man-hours and eliminate up to 3 weeks of time used for access request processing. While perimeter-based architecture assumes that threats are stopped at the front gates, ELS does not accept this precondition and is designed to mitigate many of the primary vulnerability points at the application using distributed security architecture. The ELS design addresses five security principles that are derived from the basic tenets:

- *Know the players* by enforcing bilateral, end-to-end authentication.
- *Maintain confidentiality* through end-to-end unbroken encryption (no in-transit decryption/payload inspection).
- *Separate access and privilege from identity* by means of an authorization credential.
- *Maintain integrity* by ensuring that you receive exactly what was sent.
- *Require explicit accountability* by monitoring and logging transactions.

Know the Players

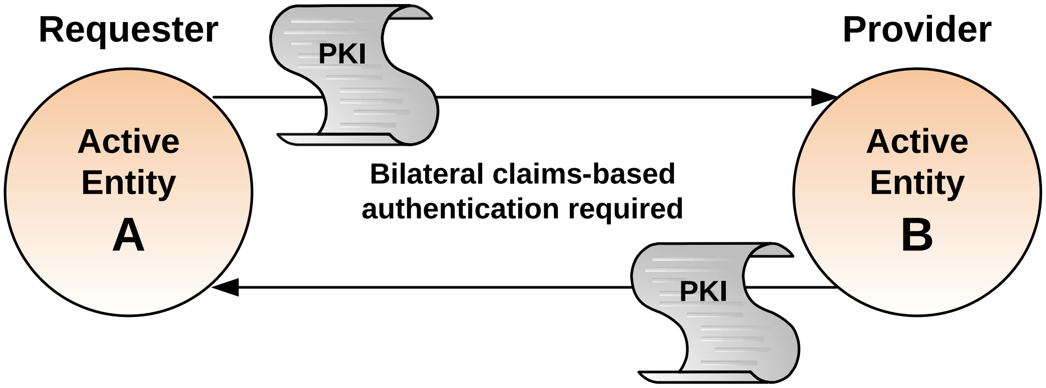
In ELS, the identity certificate is an X.509 public key infrastructure (PKI) certificate.[1] This identity is required for all active entities, both person and non-person (such as a type of service, as shown in Figure 1). PKI certificates are verified and validated. Ownership is verified by a holder-of-key check. Supplemental (in combination with PKI) authentication factors may be required from certain entities, such as identity-confirming information or biometric data.

Maintain Confidentiality

Figure 2 shows that ELS establishes end-to-end Transport Layer Security (TLS) encryption (and never gives away private keys that belong uniquely to the certificate holder).[2]

Separate Access and Privilege from Identity

ELS can accommodate changes in location, assignment, and other attributes by separating the use of associated attributes from the identity. Whenever changes to attributes occur, claims are recomputed based on new associated attributes, allowing immediate access to required mission information. As shown in Figure 3, access control credentials use the Security Assertion Markup Language (SAML).[3] SAML tokens are signed, and the signatures are verified and validated before acceptance. The credentials of the signers also are verified and validated. The credential for access and privilege is bound to the requester by ensuring a match of the distinguished name used in both authentication and authorization credentials.



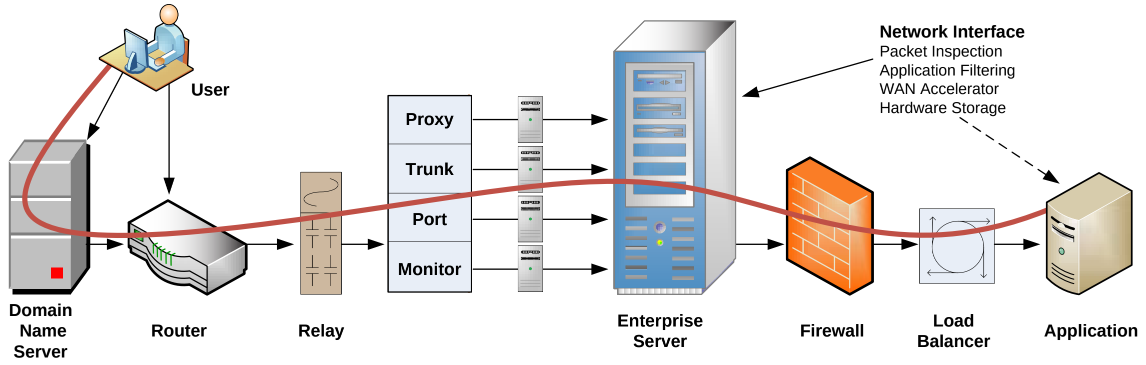
Note: Active Entity A or B may be a user, a web application, a web service, an aggregation service, an exposue service, a token server, or any other entity that can request or provide service.

Figure 1. Bilateral Authentication

[1] The X.509 standard defines the format of public key certificates used in internet protocols. PKI certificates are one of several X.509 certificate types.

[2] The TLS family of Internet Engineering Task Force (IETF) Standards are laid out in a series of Request for Comment (RFC) publications.

[3] The Organization for the Advancement of Structured Information Standards (OASIS) provides an open set of standards for SAML.



Note: WAN stands for Wide Area Network.

Figure 2. End-to-End TLS Encryption

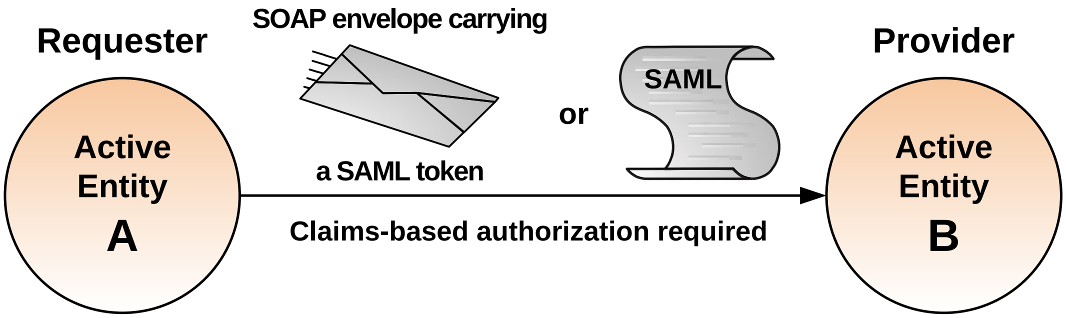
Maintain Integrity

Integrity is implemented at the connection layer by use of end-to-end TLS message authentication codes (MACs) and other integrity measures (Figure 4). Chained integrity, where trust is passed on transitively from one entity to another, is not used since it is not as strong as end-to-end integrity. At the application layer, packages (SAML tokens, etc.) are signed, and signatures are verified and validated.

ELS has been shown to be a viable, scalable alternative to current access control schemas. ELS allows users access without accounts by computing targeted claims for enterprise applications (using enterprise attribute stores and asset-owner-defined claims for access and privilege).

Require Explicit Accountability

As shown in Figure 5, ELS monitors specified activities for accountability and forensics. The monitor files are formatted in a standard way and stored locally. For enterprise files, a monitor sweep agent reads, translates, cleans, and submits to an enterprise relational database for recording log records, periodically or on-demand. Local files are cleaned periodically to reduce overall storage—and to provide a centralized repository for help desk,



Note: SOAP stands for Simple Object Access Protocol.

Figure 3. Claims-Based Authorization

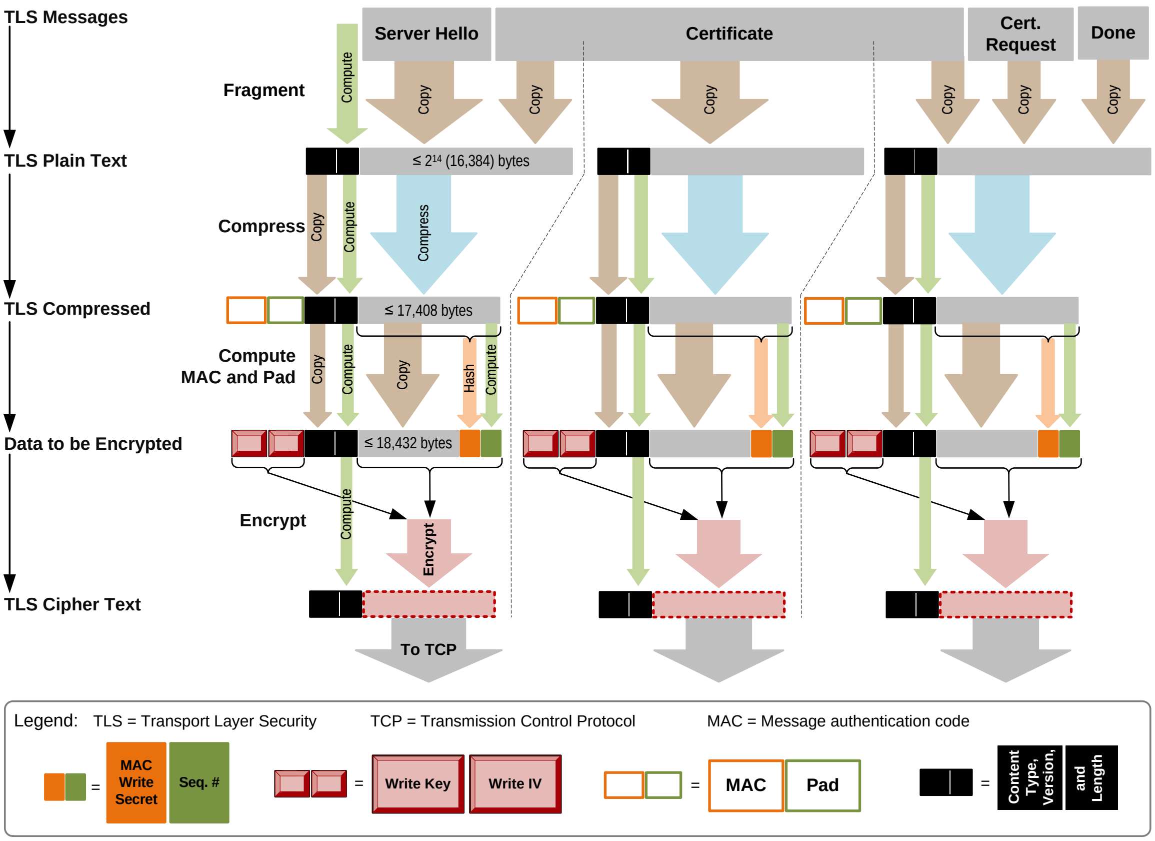


Figure 4. MAC and Other Integrity Measures

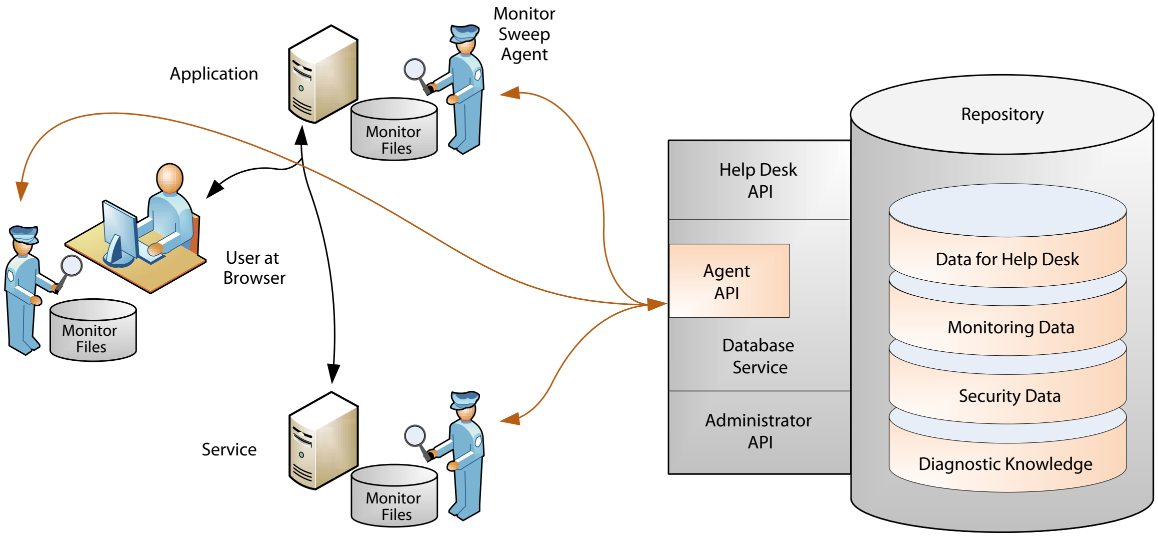
forensics, and other activities. The details of this activity are provided in designated technical profiles (Simpson and Chandersekaran 2010; Chandersekaran and Simpson 2011).

The ELS will reach initial operating capability in a production environment in fiscal year 2018 or fiscal year 2019. Major functionalities have been implemented, and initial penetration testing at the National Cyber Range has found no significant architectural problems. Additional detailed vulnerability testing is planned for future test events.

Authorized users will have immediate access to the application once it is operational. Within the U.S. Air Force alone, system administration requirements will decrease by an estimated 90–95 percent, and user delays for access will dwindle from weeks to hours.

Results of claims-generation tests conducted in late 2013 for 1.2 million unique users show that claims may be generated at 215 million generations per hour. These tests were based on assumptions of 119,614 claims being generated with an average time to generate a claim of 2.0 seconds and an average claim retrieval time (using the ELS process) of 33 milliseconds. These figures are well within the quality of service expected for this user group.

Scaling tests conducted in mid-2012 indicate that a single Secure Token Service (STS) can handle 800



Note: API stands for Application Programming Interface.

Figure 5. Accountability through Centralized Monitoring

SAML tokens per second, which is 50,000 per minute, or 250,000 every 5 minutes. If one STS request every 5 minutes per user is the maximum anticipated (peak sustained rate), then 4 STSs are needed per 1,000,000 users in the enterprise. A planning figure of 10 STSs per 1,000,000 users allows for anticipated redundancy, locality, surges, and load balance latencies.

This is readily achievable and can easily be scaled to larger enterprises. The application handler code to process SAML tokens has been generated for inclusion with .Net and Java applications and services. It has also undergone initial testing.

These test results were documented as the result of a carefully crafted spiral development process that includes:

- Fully encrypted unbroken end-to-end communications (TLS with message authentication codes);
- Bilateral PKI authentication for all enterprise entities;
- SAML-based approaches for access and privilege (the SAML creation and utilization are hardened for vulnerability mitigation);
- Embedded SAML handles for consistency in application;
- Claims-based access and privilege approach, as opposed to attributes and roles;
- Defined federation and delegation processes; and
- Virtualization inspection handlers (in process).

A full implementation began in 2012 with a spiral-based rollout leading to pathfinder applications, testing and evaluation, and application to the Joint Information Environment, which is in process.

Path Ahead

ELS provides a foundation for implementation throughout the Air Force, and the ELS team continues to capture enterprise use cases and define their associated technical solutions. As baselines are established, ELS will be fine-tuned to meet needs identified by evaluation of applications from other military components and environments, such as command and control and tactical.

Development will continue, and with additional testing and feedback, ELS will be hardened and operationalized for enterprise operation. Other elements of ELS, including the handler code installed on servers, will be hardened according to Defense Department policies and provided to developers of new applications and services. Application and service developers will be integrated into the process so that they understand what is expected with ELS, and assistance will be provided through hands-on support and additional documentation of the ELS process.

The ELS web-based security architecture is based on core security tenets and reflects the enterprise's overall goals and security philosophy. The United States must continue to advance its security posture by protecting the applications and data at the source. It is in this vein that ELS was conceived—a superior way to provide secure, scalable access control for the enterprise.

References

Chandersekaran, C., and W. R. Simpson. 2011. "A Multi-Tiered Approach to Enterprise Support Services." Presented at the 1st International Conference on Design, User Experience, and Usability, part of the 14th International Conference on Human-Computer Interaction (HCII 2011), Orlando, Florida, July 2011. https://doi.org/10.1007/978-3-642-21675-6_45.

Simpson, W. R., and C. Chandersekaran. 2010. "An Agent Based Monitoring System for Web Services." Presented at the 16th International Conference on Information Systems Analysis and Synthesis (ISAS 2010), Orlando, Florida, April 6–9, 2010.

William (Randy) Simpson, a Research Staff Member in the Information Technology and Systems Division of IDA's Systems and Analyses Center, holds a doctorate in aerospace engineering from Ohio State University.

This article is derived from *Enterprise Level Security: Securing Information Systems in an Uncertain World* (Boca Raton, FL: CRC Press, Taylor and Francis Group, 2016).