SECURITY MODELING FOR PUBLIC SAFETY COMMUNICATION SPECIFICATIONS

Daniel W. Gambel
Mitretek Systems Inc.
7525 Coleshire Drive
McLean, VA 22102-7400

Abstract

Public Safety communications are based on unique specifications distinct from military and commercial services. This type of communications serves fire, law enforcement, and emergency services. The current specifications are being upgraded under the auspices of APCO Project 25, a federally funded effort, to establish specifications for the new technologies.

APCO Project 25 aims to specify a single digital communications technology which will meet Federal, state, and local government requirements for public safety services. It must meet the full range of communications requirements including conflicting needs for both secrecy and public access.

The examination of the potential for modeling the security grew out of a concern for the multiplicity of security policies which were required to support the varied missions, and the need for single units to switch between policies with high confidence of enforcement of the selected policy configuration.

This paper proposes an approach to validation of the specifications for APCO Project 25 with an appendix which reviews the field of security modeling as it relates to the problem.

Keywords

Composition, evaluation, modeling, wireless communication, digital communication, security, cryptography, trust, system engineering, integration, specification, interface

Introduction

The year is 1846. A territorial US Marshall and his small band of men find themselves boxed in, completely surrounded, heavily outnumbered, and with virtually no hope of escape. In utter frustration, the Marshall screams, “Where’s the dang cavalry when you need them?”. It is a 150 years later, times are different, society has changed, and technology has advanced, but, the public safety official of today feels much of the same frustration when facing a major disaster - where and how do I get the right support when I need it. This present day frustration primarily stems from the long-standing issues of communications interoperability and radio coverage. Virtually every public safety agency across the country operates a wireless network of some

fashion or another, but these networks were developed independently to serve the needs of the particular agency employing them. Connectivity to and interoperability with other public safety agencies has assumed secondary importance and has long been disregarded.

Recognizing the need for interoperability and improved efficiencies, (APCO) Project 25 was created in 1989 as a joint Government and industry effort to develop a set of technical standards for the next generation of digital public safety communications services in which the Land Mobile Radio (LMR) is the main ingredient. Project 25 covers all of the parts of an LMR-based communications system. It is a networked system which includes portable radios for hand held operation, mobile radios for vehicular operation, base stations for fixed installations, console operator positions, computer equipment, other supporting equipment, and extensions into other networks which may or may not be wireless.

While maintaining interoperability as the core, Project 25 also adopted the general goals of maximizing radio spectrum efficiency, providing user friendly interfaces, ensuring competition in life-cycle procurements, and enabling a graceful migration to new technologies within a short time. It is the advent of a new paradigm for LMR use. Project 25 defines a standard system model with open interfaces to make the new paradigm work. A description of common parameters, concepts, system elements, and critical system interfaces is contained in APCO Project 25 System and Standard Definitions, Telecommunications Systems Bulletin (TSB) 102.A, Telecommunications Industry Association (TIA), November 1995.

"FEDSIM PUBLIC SAFETY WIRELESS NETWORK PROJECT 25 SECURITY TEST AND EVALUATION REPORT", Dated November 1996

The Association of Public-safety Communication Officials (APCO) created APCO Project 25 to define, create, and adopt standards which would permit migration of public safety communication from analog to digital communication formats by the year 2000. This project created a body of documentation establishing the criteria for the next generation of public service communications.

Project 25 had four major objectives. These were: (1) provide enhanced functionality with equipment and capabilities focused on public safety needs, (2) improve spectrum efficiency, (3) ensure competition among multiple vendors through Open Systems Architecture, and (4) allow effective, efficient, and reliable intra-agency and inter-agency communications.

However, the correctness and completeness of the security requirements necessary to support these objectives do not appear to have been validated during development of the specification. Since products will be built to meet the standard, an assessment of the correctness and completeness of the specification in regard to security was required. A risk assessment of the specification was conducted under FEDSIM which identified a need for being able to model the security of the products, before they were built. This modeling effort was necessary to ensure the standards were adequate, before manufacturers invested in developing products which could then be examined for adequacy.

Generic model for Project 25 security services

The Project 25 standard defines the services required for public safety communications. These services together must satisfy the public safety needs. Among these needs are what appear to be classical security requirements. Specifically, the standard should support the public safety need for reliable service, confidentiality on protected communications, and reasonable quality of the service provided. These are closely aligned with the security

community's view of Confidentiality, Integrity, and Availability requirements, although with a different priority and perspective on each.

The digital services standard consists of a set of services which the digital communications product may provide. Notable during an analysis of the standard is that there does not appear the concept of "always invoked". Instead, the standard services are available, only optionally invoked. The status and control data for such invocation is carried in the header portion of the transmission. There is good reason for this approach. Public safety communications are monitored by service providers such as towing companies. When a need arises for the service, the monitor triggers the response. Thus an officer need only report the accident, towing service is provided without further coordination. If the confidentiality portion of the standard were always invoked, then the towing service coordination would be an additional public safety requirement.

As stated earlier, there is a need to provide security validation of the standard before significant investment in products. The manufacturers today can build products to the standard without such an evaluation, however, there may be significant security problems embedded in that product.

There are a number of attributes which appear to be relevant to the security services which are needed to sustain APCO Project 25. These attributes can be validated through test and evaluation methods, but that would require production of the equipment to be subjected to such a test. However, the security community has evolved methods for assessing policy, requirements, and specifications which may support the evaluation of standards.

The latest evolution in this security community effort [BELL96] concludes that a significant benefit can result from evaluating the specification to which a product is built since a significant portion of traditional evaluation effort is normally spent in understanding the product specification. When this approach is combined with the security composition approach documented in [GAM95] there is reasonable expectation that the Project 25 standards can be validated from a security perspective.

The combination of the two modeling views is that since specifications or standards can be evaluated in the absence of products, and that those standards can undergo decomposition and be reliably recombined, then Project 25 standards can be evaluated with value added.

The added value to Project 25 from such an endeavor would be to ensure that the standards are complete with regard to ensuring reliable service, on-call confidentiality service, and with a consistent view of the integrity of the public safety network.

Current minimum security services which are suspected to be missing from the specification are:

1. Availability of the Interfaces: This attribute defines the requirement for a given vendor to ensure specified interfaces are actually incorporated into the product. The assessment of the standard should address the completeness of this attribute in the standard. Later testing will assure that he interfaces integrated into the product meet interoperability requirements.

2. Availability of the Services: Defines the service levels incorporated into the vendor's product.
3. Control or management traffic: Communications specified for purposes other than operational mission communications.
4. Cryptographic Keys: Services which coordinate or provide the encryption keys used for individual transmissions.
5. Identity of the receiver: Services which are aware of or establishes the identity of the user who is the intended destination for the transmission sequence.
6. Identity of the sender: Services which are aware of or establishes the identity of the user who initiates the transmission sequence.
7. Knowledge of the location of the physical equipment: Services which establish or are dependent upon the geographic or geopolitical location of the actual equipment.
8. Location of the receiver: Services which establish or are dependent upon the geographic or geopolitical location of the recipient of a transmission.
9. Location of the sender: Services which establish or are dependent upon the geographic or geopolitical location of the sender of a transmission.
10. Temporal Continuity: Services which create or enable the establishment of a system wide basis for time.

In addition, the specific minimum essential services which are to be developed are prescribed in the specification as:

1. Confidentiality
2. Authentication
3. Key Management

Evaluating the above services in a formal context should serve to permit evaluation of the products which purport to meet that specification in a reasonable time frame. Such abbreviated evaluation time will permit rapid fielding of adequately secure products for public service wireless communications.

Summary

The Bell approach is the first integrated approach in the application of generic system requirements to specific products. It is clear that this is a step toward having multi-vendor public safety wireless services and products that will operate as anticipated by Project 25 at the interface to other Project 25 products.

Appendix: Review of Security Modeling

Modeling of computer system behavior has been a significant element of establishing the behavior characteristics of the programs and products which result from the modeling effort. The security model effort began in the early 1970's and culminated in the adoption of the DoD Trusted Computer System Evaluation Criteria, now a DoD standard for secrecy attributes in an information system product suite. In the early 1980's a communications modeling effort was undertaken which led to the International Standards Organization adoption of the Open System Interconnect model of seven (7) communication layers.

Recent efforts in formal modeling have generated a number of approaches to modeling the composition of components to form systems. Some of these approaches are limited to a particular security policy, e.g. McCullough's restrictiveness property [MCCU88], while others are limited to a particular organizational view, e.g. the hierarchical model of Lam and Shankar [LAM91]. A more general approach has been taken by Abadi and Lamport [ABAD90], whose composition theorem permits expression of a variety of component properties, and allows both parallel (peer-to-peer) and sequential (hierarchical) composition. Hemenway and Gambel have discussed a number of such approaches with respect to how they address various issues which arise in modeling composed systems [HEME92]. It should be noted that although extensive work has been done in creating formal models for composing systems, very little work has been done in applying any of the models to the integration of real systems.

In 1995, work was undertaken by D. Elliot Bell [BELL96] to apply the modeling technique to industry standards as a generic model interpretation. This effort describes a process by which the attributes of the generic (standard compliant) system are validated as compliant with specified security properties..

Security Model Framework

The initial security model which is generally accepted was based on a mathematical representation [BLP73] of the DoD security policy regarding secrecy. This mathematical foundation has served for the past two decades as the foundation for conceptual work on computer secrecy. It addresses the secrecy attribute. Services such as authentication and accountability are less amenable to mathematical statement and have been largely ignored from a formal perspective.

Communications model framework

The communications model framework is likewise one of mathematical derivation. Lam and Shankar [LAM91] created a mathematical model of communications services where the essence of the service could be represented by a description of the behavior observed at the interface between services.

Recent work extends the boundary condition used on the OSI abstraction to provide the theoretical foundation for a similar notion that services performed within a layer are

reliable if, and only if, they preserve the established boundary condition. This notion is particularly useful in the conceptual understanding of encryption services.

Encryption algorithms are autonomous in relation to the communications interface which uses the algorithm. On the other hand, the communications service must be able to depend on the consistent performance of the encryption algorithm. Thus the interface defines the desired observed behavior, while the services expect input or present results to the interface without disclosing the context of how that data presentation was derived. In a like manner, the key management services can be isolated from the encryption service which uses the key. In this context, the key variable is presented at the interface to the algorithm concurrent with the data to which the key variable is to be applied. The key management software is assumed to have behaved correctly, and the encryption algorithm is assumed to have behaved correctly. Currently, there is validity in presenting a key variable for data which was derived by the same algorithm in a prior operation. (Key encryption Key).

System Composition

Although the model discipline for security and communication is well established, these models are applicable to products only when the product is developed in a top-down fashion. The reason for this approach is that the product manufacturer establishes a vertically integrated product line based on a single application of the model. The resultant product can be shown to be clearly consistent with the model and to demonstrate implementation of the generic attributes upon which the model is based. However, when integrating two or more products from different vendors, the structure tends to disintegrate rapidly.

The decision choices made by each vendor lead to different definition of services which support the interface, and to different implementations of the interface. The result is that examination of the product documentation and model does not permit integration. There are several reasons for this as described by Gambel and Hemenway (GAM95]. The primary reason for integration failures is the use of dissimilar nomenclatures for items visible at the interface. Thus a value “FREQ” offered by one product might be “Frequency” by another product. This lack of standard label means that the interface is confused at best. Since the re-labeling also may be such that the identical name is used for two different logical items, there is really a significant potential for misunderstanding.

In addition, there are situations where optional items are implemented, and sometimes differently. This means that what is offered at the interface differs in content from the adjacent product. In most cases there is a many-to-many or one-to-many relationship offered at the interface. This means the service of one product must be mapped to the services of the adjacent product. This mapping becomes the second significant effect of vendor implementations of the interface.

Third, there is frequently a difference in magnitude of the services offered. Thus the security service “AUDIT” may be dependent upon authenticated identification for correct operation. If the level of authentication is inadequate at the interface then the request service can be seen to fail the compliance requirement *ALTHOUGH IT MAY FUNCTION*

APPARENTLY CORRECT. The model is completely satisfied at both sides of the interface but fails to meet the overall policy invoked by the model.

Generic Model Approach

Bell [BELL96] proposes a generic approach to stating compliance with standards using commercial products. In his approach, there is a replacement for the Descriptive Top Level Specification (DTLS) with the generic standard. Thus the standard becomes the DTLS in the assurance chain of the model. Any product which is developed to meet the specification must be designed to also meet the generic DTLS. He has used this approach to define the generic model for POSIX and SQL products

From the Generic DTLS a set of minimal functional requirements is extracted. There are three tables extracted from the specification. First, a set of trust services visible at the interface are defined and prescribed. Second, a set of modules are defined which provide the trust service and must meet the prescribed interface. The last table lists the rules or transitions that must be applied when a service makes that call at the interface.

The result of the Bell approach is that the vendor has a rigid set of specifications which meet the standard. But in addition, the services can be mathematically or formally evaluated to ensure that the specification meets both the services required and the security assurance and functionality required. This effort performed once on the specification service to support many products and reduces the time for product evaluation.

References

[ABAD90] Abadi, Martin, and Lamport, Leslie. Composing Specifications. Research Report 66: Digital Systems Research Center, October 1990.

[BELL96] Bell, D.Elliott. Generic Model Interpretations: POZIX1 and SQL, Proceedings of the 1996 National Computer Security Conference, October 1996.

[BLP73] D. E. Bell and L. J. La Padula. Secure Computer Systems: Mathematical Foundations, MTR-2547, Vol. 1, The MITRE Corporation, Bedford MA, 1 March 1973.

[GAM95] Gambel, Daniel and Hemenway, Judith. The Use Of Generic Architectures In System Integration. Proceedings from the National Computer Security Conference 1995

[HEME92] Hemenway, Judith and Gambel, Daniel. Issues in the Specification of Composite Trustworthy Systems. Proceedings of the 4th Annual Canadian Computer Security Symposium, Ottawa: May 1992.

[LAM91] Lam, Simon; Shankar, A.U., and Woo, Thomas. Applying a Theory of Modules and Interfaces to Security Verification. Proceedings of the 1991 IEEE Symposium on Research in Security and Privacy.

[MCCU88] McCullough, Daryl. Noninterference and the Composability of Security Properties, Proceedings of the 1988 IEEE Symposium on Security and Privacy.