(1)

INFOSEC Product Integration

M 92B0000054

June 1992

Thomas J. Brando
Karen L. Johnson

MITRE
Bedford, Massachusetts

INFOSEC Product Integration

M 92B0000054
June 1992

Thomas J. Brando
Karen L. Johnson

Contract Sponsor N/A
Contract No. N/A
Project No. 028A
Dept. G117

Approved for public release;
distribution unlimited.

MITRE
Bedford, Massachusetts

PREFACE

This paper was accepted for presentation at the IEEE Military Communications Conference (*MILCOM '92*), 11–14 October 1992, in San Diego, CA.

INFOSEC PRODUCT INTEGRATION

THOMAS J. BRANDO and KAREN L. JOHNSON

The MITRE Corporation
202 Burlington Road, Bedford, MA 01730-1420

ABSTRACT

MITRE's Information Security Center funds a set of activities referred to as the Core Program that are designed to strengthen the Center's technical capabilities and increase its body of practical knowledge, thereby enhancing its ability to support its sponsors. The INFOSEC Integration Lab is the cornerstone of the Core Program and provides a testbed for assessing commercially available trusted products, for demonstrating software prototypes developed at MITRE, and for integrating both trusted and untrusted products into complete systems. In this paper, we describe our secure product assessment philosophy, the commercially available products we have assessed, and the prototypes we have developed. Then we present a scenario we use to demonstrate a number of secure capabilities we have implemented in the lab, namely: (1) secure unitary login via Kerberos with modifications developed at MITRE that extend Kerberos to heterogeneous environments and provide a graphical user interface; (2) access to distributed single-level and multilevel databases via the Distributed Query Processor, a proof-of-concept application developed at MITRE; (3) secure transport of sensitive information across unsecured channels via a number of endorsed commercial COMSEC devices; and (4) secure transport of sensitive information between networks operating at different security levels via a prototype low-to-high guard developed at MITRE.

1. INTRODUCTION

MITRE's Information Security Center funds a set of activities referred to as the Core Program that are designed to strengthen the Center's technical capabilities and increase its body of practical knowledge, thereby enhancing its ability to support its sponsors. The INFOSEC Integration Lab is the cornerstone of the Core Program. The lab provides a setting for assessing the functionality, utility, and performance of trusted products. The focus of our product assessments is primarily on commercially available products that represent potential solutions to our sponsors' networked systems security problems. Immediate feedback to vendors has already resulted in improvements in the trusted products that are currently available.

The lab is also a testbed for integrating trusted and untrusted products into complete, secure, networked systems. This requires resolving interoperability issues between products that provide different security services or use different mechanisms to provide common services. Software prototypes are also developed to demonstrate needed capabilities not yet available commercially, to provide the glue that is necessary to integrate existing products, and to experiment with new mechanisms for building more secure and integrable systems.

The lab permits us to demonstrate to our sponsors how their security needs can be met using commercial off-the-shelf hardware and software as well as proof-of-concept software prototypes developed at MITRE. To this end, we design and develop networked configurations to simulate existing or planned environments and demonstration scenarios that serve as a context in which these secure capabilities can be shown. This paper describes our recent assessment and integration efforts and presents one scenario that we use to demonstrate a number of secure capabilities to our sponsors.

2. INFOSEC PRODUCT ASSESSMENTS AND SYSTEM INTEGRATION

Product assessments have traditionally focused on throughput and security vulnerabilities. These attributes are generally the focus of component testing performed by vendors and formal evaluators. We wish to complement vendor and evaluator efforts by transitioning from component testing to integrated systems testing. This section presents an overview of our INFOSEC product assessment philosophy and discusses previously assessed commercial products and MITRE prototypes developed to provide integrated secure system solutions.

2.1 INFOSEC Product Assessment Philosophy

Limited resources and the impracticality of investigating every possible attribute of a product have led us to an assessment philosophy that advocates the careful selection of product attributes to test, namely, those that are most significant to our sponsors. The emphasis of our assessment work has focused on system functionality and determining a product's impact on system performance and operation. These are the attributes that are believed to be of most interest and concern to our sponsors. However, we will continue to perform throughput and vulnerability tests as warranted.

Current assessments focus on the functional aspects of a security product; although we do some verification of the security services provided by a device, we do not try to determine the strength of its security mechanisms. The intent is to determine how usable a security product is, what issues are associated with its use, and what impact it will have on an existing system or network. An assessment includes a documentation review, the development of a set of attributes to test, a test plan and integrated system test configuration, and the actual test procedures performed in our integration testbed.

Over the past few years, several product assessments have been performed in the Integration Lab. In addition, to address security issues as they have evolved, MITRE has prototyped solutions to various common security problems. In order to support real system requirements, we have integrated selected products and prototypes with existing user applications to demonstrate secure networked environments. Complete system integration such as this has allowed us to examine the impact of security on existing systems as well as to improve our product integration capabilities.

2.2 Commercial Products

Previously assessed COMSEC devices include the Tracor Ultron SSP3110 SCSI Bus Encryptor, Wang Trusted Interface Unit, Xerox Encryption Unit, and Motorola Network Encryption System. Each has been endorsed by the Commercial COMSEC Endorsement Program and uses a Type-1 cryptographic algorithm to encrypt classified data up to and including TOP SECRET data. Each of these products has been integrated into the lab to demonstrate multiple implementations of single-level data protection.

To address issues involved in implementing and integrating trusted networks, assessments were performed on the Verdix Secure Local Area Network, the Digital Ethernet Secure Network Controller, and the AT&T 3B2 network interface.

In looking at trusted applications, we focused on database management systems (DBMSs). We chose to assess Secure SYBASE and Digital Equipment Corporation's SERdb. Because standard SYBASE is currently being used by MITRE sponsors, both the standard and secure versions of SYBASE have been integrated into the lab to examine interoperability issues between them. Both SYBASE products are demonstrated in conjunction with the Distributed Query Processor prototype described below. As part of the SERdb assessment, a generic set of test scenarios was developed for testing commercial multilevel secure DBMSs.

Other trusted applications we assessed include the Massachusetts Institute of Technology's Kerberos and Trusted Information System's implementation of Privacy Enhanced Mail. Both products were integrated into the lab to investigate their implementations of secure distributed authentication and secure mail, respectively. The Kerberos assessment involved the implementation of a prototype that is described below.

Much of our assessment work is performed using beta versions of these products. This allows us to provide feedback to vendors before a product is formally released. Immediate feedback to vendors on integration problems or on absent security features necessary to support mission requirements has resulted in improved security products.

2.3 MITRE Prototypes

MITRE has developed a number of prototypes to support the integration of trusted components to meet mission system security requirements. In particular, we have addressed an important user requirement for distributed authentication (unitary login), an interim solution for interfacing systems processing data at different security levels using guards, and other distributed systems issues including distributed DBMSs.

The Kerberos Authentication Protocol developed at the Massachusetts Institute of Technology and available from a number of commercial sources features a unitary authentication service for network connections and provides authentication and privacy of all messages. Kerberos currently requires a homogeneous environment in which all hosts must run the authentication protocol in order to interoperate. Extensions to Kerberos were prototyped in our lab to provide interoperability between hosts in a heterogeneous environment. Communication between hosts that support Kerberos and hosts that do not is less secure because passwords are passed in the clear between them. However, the convenience of unitary login is extended to non-Kerberized systems, and the user is informed whenever the extended login procedure is invoked. The modifications we made to Kerberos support communication between hosts using rlogin.

MITRE also implemented a graphical user interface in the form of soft buttons that display all of the systems available to the user and allow the user to access those systems without using a command-line interface.

A low-to-high guard was prototyped to provide a low-cost solution for automating database updates between the Linked Ops/Intel Centers in Europe (LOCE) and the Intratheater Intelligence Communications Network (IINCOMNET). The guard platform is a 286 or 386 IBM PC/AT or compatible. The operating system is Trusted Information Systems' Trusted XENIX, which has been evaluated as meeting the Trusted Computer System Evaluation Criteria B2 requirements. The guard provides separate network interfaces for different security level classifications and supports separate instantiations of the network software for each interface. The security policy of the operating system prevents the flow of information from high to low. The guard currently supports the FTP file transfer protocol and has been integrated into the lab to demonstrate multilevel data protection.

A Distributed Query Processor (DQP) was originally prototyped for Rome Laboratory to operate in a homogeneous environment to support trusted distributed DBMSs. The DQP was modified and implemented in our lab to operate in a heterogeneous environment. The DQP implements two secure distributed query processing algorithms for the join operation: a nondistributed join algorithm and a distributed join algorithm. The DQP provides a facility for users to query distributed single-level and multilevel databases and obtain authorized responses to their queries. The distribution of data is transparent to the user. The DQP determines the locations of involved relations and transmits queries to the corresponding sites. Responses obtained from individual sites are assembled before delivery to the user.

To explore issues related to the development of trusted applications, a trusted X Window System was prototyped. This effort identified the difficulty involved in designing the security mechanisms to support the trusted windowing systems requirements for Compartmented Mode Workstations (CMWs). Further investigation into the integration of trusted applications focuses on better support for trusted applications by the underlying trusted base. Specifically, we are developing a trusted mail application and editor to validate enhancements to a trusted operating system that support fine-grained labeling. Fine-grained labeling in a trusted operating system removes the burden of trust from the application. The trusted mailer, editor, and operating system enhancements are being implemented on the prototype CMW developed at MITRE.

The development of proof-of-concept prototypes has consistently provided a means by which to demonstrate viable solutions to current and potential security-related problems. These prototypes continue to serve as reference points from which new security products are being developed.

3. Demonstration of Integrated INFOSEC Products

3.1 Introduction

In order to provide a context in which to demonstrate the use of commercial products and MITRE prototypes, we developed the following demonstration scenario with the assistance of members of the U.S. Air Force and intelligence communities. The demonstration scenario is designed only as a context in which a given set of secure capabilities can be shown and is not meant to be a faithful representation of current C^3I practice in the field. Figure 1 shows the network configuration for this demonstration.

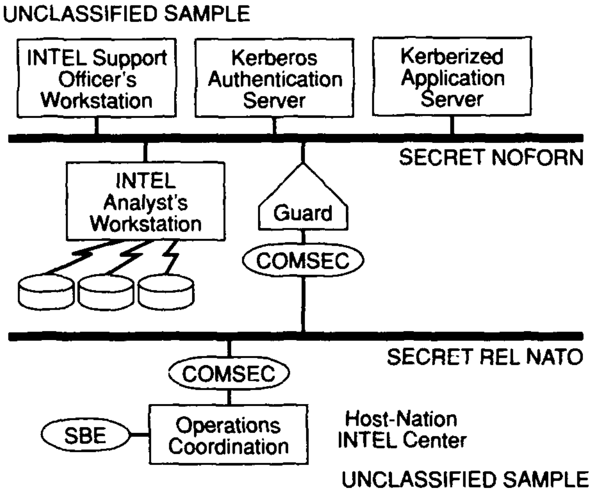

Figure 1. Demonstration Scenario

The demonstration is centered around an intelligence support officer for an Air Force squadron. One of the applications the INTEL officer uses is a penetration analysis tool called Improved Many-on-Many (IMOM) that is part of Sentinel Byte—a wing-level collateral intelligence support system. In the demonstration, the INTEL officer uses IMOM to plan the route for an air mission over Kuwait, given the known locations of surface-to-air missiles and antiaircraft artillery batteries in the area. Since the safety of the mission depends critically on the accuracy of the weapons system location information used to plan it, the INTEL officer would like to base his plans on the latest information available.

In the demonstration scenario, the INTEL officer receives weapons system location updates from two sources. The first source is an intelligence analyst working on the same base as the INTEL officer. The analyst is responsible for retrieving new weapons system location information from multiple sources and making that information available to our INTEL officer. The second source is a U.S. representative at a NATO host-nation INTEL center. After receiving a computer tape containing weapons system location information, the NATO representative transmits a copy of that information to the INTEL officer. After receiving each update, the INTEL officer revises his flight plan to avoid new threats.

This scenario allows us to demonstrate a number of secure capabilities. We demonstrate commercially available software that provides a secure unitary login capability that is not only convenient for the INTEL officer but, more importantly, also protects his passwords from possible disclosure. We also demonstrate a proof-of-concept application developed at MITRE that provides access to distributed single-level and multilevel databases. By allowing access to a traditional single-level database as well as a newer multilevel database, this application allows existing systems to be integrated with each other and with newer systems as they come on line.

We demonstrate commercial COMSEC devices that have been endorsed by the National Security Agency for transmitting classified information up to and including TOP SECRET data across unsecured channels. This eliminates the necessity of using secured, and often unavailable, communication lines. We also demonstrate a MITRE prototype guard application that enables the secure transport of classified information between networks operating at different security levels. This permits an automated connection between these networks and eliminates a costly "air gap."

3.2 Demonstration Part I: Unitary Login

The demonstration begins with the INTEL officer working at a conventional UNIX workstation. Typically, the officer accesses several systems from his workstation. Each time a system is accessed, the INTEL officer's password is sent in the clear from his workstation to the remote system. This exposes his password to possible interception by eavesdroppers.

There are other possible threats to password security when users have access to multiple systems. To avoid having to remember multiple passwords, some people use the same password for all of their accounts. But if that one password is disclosed, the security of all systems is compromised. To help remember multiple passwords, some people write them down. But unless a password list is stored in a secure container, those passwords are at risk.

These threats to password security can be countered using a workstation running an authentication protocol like Kerberos, which features unitary login in conjunction with secure authentication. The Kerberos authentication server provides a key distribution service and a ticket-granting service.

When the INTEL officer logs into a Kerberos workstation, the password he enters is used to decode a message that contains an authentication ticket obtained from the Kerberos authentication server. If the password he enters is correct, the ticket obtained from the decoded message can be used to gain access to the network services the officer is authorized to use.

When the INTEL officer wants to access a remote system, his authentication ticket is automatically used to obtain a special ticket that authenticates him to the remote system. All the messages involved in establishing a connection to a remote system are encrypted. This includes messages exchanged between the INTEL officer's workstation and the ticket-granting service to obtain the special ticket required for authentication to the remote system as well as messages exchanged between the INTEL officer's workstation and the remote system to establish the connection.

An authentication protocol like Kerberos offers two advantages. The first is unitary login, which means the INTEL officer only needs to remember a single password, regardless of how many systems he needs to access. The second advantage is secure authentication, which means that all authentication messages that identify the INTEL officer when he logs into Kerberos or accesses a remote system are encrypted, thus protecting sensitive password information from possible disclosure to eavesdroppers.

With our extended version of Kerberos, when the INTEL officer wants to connect to a system that is not running Kerberos, the ticket-granting service returns the INTEL officer's password for that system instead of a ticket. The password is then transmitted to the remote system on the INTEL officer's behalf. Thus, the extended system maintains the appearance and convenience of unitary login, although passwords are passed in the clear between the INTEL officer's workstation and remote systems that are nu. running Kerberos.

Having securely logged into the application server via Kerberos, the INTEL officer invokes the IMOM application and uses IMOM to determine the safety of a route selected to strike a target area and return. In the demonstration scenario, IMOM verifies that the current route lies a safe distance from all known threats. At this point, the INTEL officer is notified of incoming information that may impact the safety of the current route.

3.3 Demonstration Part II: Distributed Query Processing

An update on the location of weapons systems in the INTEL officer's area of interest is provided by an intelligence analyst located somewhere on the same base. To obtain the latest information available, the analyst periodically queries three databases using a distributed database application called the Distributed Query Processor, or DQP, developed at MITRE. The DQP allows a user to access information that may be fragmented among geographically distributed single-level or multilevel databases. Given a query from the user, the DQP queries the relevant databases at the user's security level, combines the retrieved information, and makes the results available to the user.

The analyst requests updated weapons system location information from the DQP using a stored query tailored specifically to the information the INTEL officer needs to run IMOM. The DQP accesses three databases on the analyst's behalf. Two are single-level databases containing SECRET information. The third is a multilevel database with information up to and including TOP SECRET. Because the analyst is running at the SECRET level, however, only information up to that level is retrieved.

The analyst talks to a DQP that runs on his application server. That DQP talks to other DQPs that are running on the remote database servers. When the analyst submits a query to the local

DQP, it evaluates alternative strategies for satisfying that query and selects the one it expects to minimize communication costs.

The DQP can access traditional single-level databases as well as newer multilevel databases. For our demonstration, the DQP communicates with a standard SYBASE server and with two SYBASE Secure SQL servers. The servers and the DQP run on untrusted networks. In the future, these applications will be ported to more trusted environments as they become available in the lab.

The DQP stores the results of the query for updated weapons location information in a disk file that is accessible to the IMOM application. Once the update is available, the INTEL officer instructs IMOM to determine the safety of the planned route. The update identifies a new missile launcher, and IMOM indicates that a segment of the route is within the range of the new threat. Knowing this, the INTEL officer plans a new route to avoid the new threat.

3.4 Demonstration Part III: Endorsed Commercial COMSEC Devices

Weapons system location updates may also come from host-nation INTEL centers. A United States representative at a NATO host-nation INTEL center receives a computer tape containing weapons system location information. The information was written onto the tape using a Tracor Ultron SCSI Bus Encryptor, which automatically encrypts data as it is written. Once the data is encrypted, the tape itself is unclassified and can be transported by an uncleared person or through the mail.

When the U.S. representative receives the tape, the data is retrieved using another Tracor Ultron SCSI Bus Encryptor. As it is read, the data is automatically decrypted and must again be handled as classified information. In order for this data to reach the INTEL officer, it must now be transmitted from the host-nation INTEL center to the INTεL officer's network. This presents two problems.

The first problem is that the communication link between the host-nation INTEL center and the INTEL officer's facility must be protected. If this link cannot be protected physically, the link can be secured using a pair of COMSEC devices such as Motorola Network Encryption Systems, Wang Trusted Interface Units, or Xerox Encryption Units, which automatically encrypt data as it is transmitted. The encrypted data is unclassified and can be transmitted over unsecured communication lines. Upon arrival at its destination, the data is decrypted by an identical device.

The second problem is that the host-nation INTEL center is a SECRET REL NATO facility, which means it processes SECRET information that can be released to cleared NATO personnel, while the INTEL officer is working at a SECRET NOFORN facility, which means it processes SECRET information that cannot be released to foreign nationals. Unrestricted communication cannot be allowed between these two networks. Although it is acceptable for information to flow from SECRET REL NATO to SECRET NOFORN, it is not acceptable for information to propagate in the opposite direction. This problem is addressed by a low-to-high prototype guard developed at MITRE.

3.5 Demonstration Part IV: Prototype Guard

MITRE prototyped a low-to-high guard to facilitate automated database updates between LOCE—the fusion center for intelligence data in Europe—and IINCOMNET—a system that connects U.S. Air Force intelligence organizations in Europe at the collateral level. The guard runs on Trusted Information Systems' Trusted XENIX and is a trusted application whose purpose is to enforce a secure network separation that permits one-way communication between networks operating at different classification levels.

For our demonstration, the guard is partitioned into a low side, which runs at SECRET REL NATO, and a high side, which runs at SECRET NOFORN. When data is received on the low side of the guard, it is retransmitted out the high side. When the acknowledgment is received on the high side, a one-byte acknowledgment is created that carries no additional information. This new acknowledgment is transmitted out the low side. Thus, information is allowed to pass from the network on the low side of the guard to the network on the high side of the guard, while information is prohibited from propagating in the opposite direction.

Our U.S. representative initiates a conventional file transfer session with the guard and transfers the weapons system location update. A pair of COMSEC devices between the host-nation INTEL center and the guard protects the data from possible disclosure to eavesdroppers. The guard passes the data onto the INTEL officer's network, while ensuring that no information can propagate back to the network at the host-nation INTEL center.

When the update arrives, the INTEL officer instructs IMOM to use the new information to determine the safety of his revised route. The update identifies three new antiaircraft artillery batteries, and IMOM indicates that a segment of the revised route is within the range of the new threat. Knowing this, the INTEL officer again revises the route to avoid the new threat.

4. Concluding Remarks

During the course of our assessment and integration efforts, we have exposed a number of systems integration problems with commercial INFOSEC products. We have addressed many local area network security issues with regard to the usability of these products, such as: capabilities and limitations, interoperability, functional and documentation deficiencies, and impact on overall system functionality, performance, and operating procedures. We have participated in the resolution of these problems by providing input to the vendors of these products. In addition, we have prototyped solutions to several secure networking problems. Prototyped solutions have addressed the need for distributed authentication in heterogeneous environments, guards for multilevel secure data transfer, distributed DBMSs in multilevel environments, and support for the development of trusted applications. We have subsequently demonstrated the system integration of these commercial products and prototype solutions in useful networked configurations.

The INFOSEC Center's Integration Lab continues to serve as a testbed for integrating trusted and untrusted components into complete, secure, networked systems. The current lack of guidance, requirements, and regulations demands that secure product integration continues in order to uncover existing and unforeseen problems. As we continue to raise important questions, address outstanding issues, and resolve existing problems, we hope to influence the development of secure networking standards relevant to real-world requirements.

An effort is currently underway to establish an interactive security testbed working group. The number of existing security testbeds such as ours is growing. Representatives from different groups supporting security testbeds will meet on a regular basis to discuss network integration issues. The outcome of such discussions will expedite the resolution of existing problems and provide information of significance to developers of network security standards.

Acknowledgments

The authors wish to acknowledge all who contributed to the work described in this paper, especially: Judy Furlong and Sharon Kass, for installing and extending Kerberos version 4; Dr. Harvey Rubinovitz, for developing and integrating the Distributed Query Processor into the lab; Lisa Mitchell and Richard Parker, for their guidance in system integration issues; and the many MITRE employees and Air Force personnel who helped us develop the demonstration scenario. Special thanks are due Harriet Goldman, our project leader, for her support and direction of our assessment and integration efforts.

The work described above was funded by The MITRE Corporation's Information Security Center at Bedford, MA.

Bibliography

Bellovin, S., and M. Merritt, 1991, "Limitations of the Kerberos Authentication System," Paper presented at USENIX Winter 1991, Dallas, TX.

Berger, J. L., J. Picciotto, J. P. L. Woodward, and P. T. Cummings, 1990, "Compartmented Mode Workstation: Prototype Highlights," *IEEE Transactions on Software Engineering*, June 1990, pp. 608–618.

Department of Defense Trusted Computer System Evaluation Criteria, DOD 5200.28-STD, December 1985.

Gosselin, M. J., 1991, "The Development of a Low-to-High Guard," *Proceedings of the 14th National Computer Security Conference*, pp. 157–166.

Graubart, R. D., J. L. Berger, and J. P. L. Woodward, 1991, *Compartmented Mode Workstation Evaluation Criteria, Version 1*, DDS-2600-6243-91, Defense Intelligence Agency, Washington, DC.

Kohl, J. T., 1991, "The Evolution of the Kerberos Authentication Service," Paper presented at the Spring 1991 EurOpen Conference in Tromso, Norway.

Miller, S., B. Neuman, J. Schiller, and J. Saltzer, 1991, "Section E.2.1 – Kerberos Authentication and Authorization System," *Project Athena Technical Plan*, Cambridge, MA: Massachusetts Institute of Technology.

Picciotto, J., 1990, *Trusted X Window System, Volume 1: Design Overview*, MTP-288 Volume 1, The MITRE Corporation, Bedford, MA.

Picciotto, J., 1990, *Trusted X Window System, Volume 2: Security Services Client Detailed Design*, MTP-288 Volume 2, The MITRE Corporation, Bedford, MA.

Picciotto, J., and D. F. Vukelich, 1991, *Fine Grained Labeling, Volume 1: Operating System Support*, MTP-387, The MITRE Corporation, Bedford, MA.

Rubinovitz, H. H., and B. M. Thuraisingham, 1990, *Secure Distributed Query Processor, An Overview*, MTR-10969, Volume 1, The MITRE Corporation, Bedford, MA.

Rubinovitz, H. H., and B. M. Thuraisingham, 1990, *Secure Distributed Query Processor, Implementation Details*, MTR-10969, Volume 2, The MITRE Corporation, Bedford, MA.

Rubinovitz, H. H., and B. M. Thuraisingham, 1991, "Implementation and Simulation of Secure Distributed Query Processing Strategies," *Proceedings of the Summer Computer Simulation Conference*, July 1991, Baltimore, MD.

Rubinovitz, H. H., and B. M. Thuraisingham, 1992, "Design and Implementation of a Distributed Query Processor for a Trusted Distributed Database Management System," Paper accepted for publication in the Journal of Systems and Software.

Steiner, J., C. Neuman, and J. Schiller, 1988, "Kerberos: An Authentication Service for Open Network Systems," Paper presented at USENIX Winter 1988, Dallas, TX.

Woodward, J. P. L., 1987, *Security Requirements for System High and Compartmented Mode Workstations*, DDS-2600-5502-87, Defense Intelligence Agency, Washington, DC.