EVALUATION ISSUES FOR AN INTEGRATED "INFOSEC" PRODUCT

Frank L. Mayer, William C. Barker, Theresa K. Haley,
J. Noelle McAuliffe, Daniel F. Sterne, Lynne S. Vidmar

Trusted Information Systems, Inc.
3060 Washington Road
Glenwood, Maryland 21738

ABSTRACT

In recent years it has been recognized that the protection of classified and sensitive information in an distributed, automated processing environment requires a total "information security" (INFOSEC) solution, combining both communications and computer security technologies into an integrated security solution. While the need for INFOSEC solutions is clearly recognized, the commercial availability of true INFOSEC products is extremely limited or non-existent. This paper discusses the evaluation issues involved in an effort to take evaluated COMSEC technology and evaluate trusted system technology, and integrate them into an evaluable INFOSEC product.

1. BACKGROUND

The proliferation of commercially available products for the protection of sensitive and classified information is becoming a reality with the successes of the National Security Agency (NSA) Commercial Communications Security (COMSEC) Endorsement Program (CCEP) and the National Computer Security Center (NCSC) program to evaluate commercially available trusted systems. In recent years, these security communities have come to realize that both arms of the information security (INFOSEC) problem, i.e., COMSEC and computer security (COMPUSEC), are necessary to ensure the complete protection of information. However, the commercial availability of true INFOSEC products is nearly non-existent, despite the successes of the COMSEC and COMPUSEC halves of the problem.

Trusted Information Systems, Inc. (TIS), in early 1988, began an internally-funded effort to integrate available COMSEC technology with available trusted system technology into an information security (INFOSEC) product called the Trusted Workstation (TWS). Specifically, the TWS integrates the NSA approved cryptographic device GILLAROO [1] and the TIS' Trusted XENIX" trusted operating system [2] into a single, evaluable product. The Trusted XENIX operating system was chosen because of its targeted B2 rating (as defined by the Trusted Computer System Evaluation Criteria (TCSEC) [3]), commercial availability, and its support for a hardware architecture compatible with the GILLAROO device (i.e., the PC AT). The intent of the TWS is to demonstrate that COMSEC and trusted systems technologies can be integrated into a functional INFOSEC product that is available today, using today's best available technology, in a relatively short period of time. It is our intent to have the TWS product re-evaluated by both the communications and computer security organizations within the NSA to ensure that neither the GILLAROO nor the Trusted XENIX evaluations have been invalidated by the TWS integration effort.

The purpose of this paper is to examine the evaluation issues that arise with such an undertaking based upon our experiences with the TWS.

2. OVERVIEW OF THE TWS

The primary objective for integrating the GILLAROO device within a trusted computing environment is to prevent unauthorized or inappropriate disclosure of sensitive or classified information by untrusted application software via the GILLAROO communications port. The major component of the GILLAROO system is an add-on board for an IBM® PC AT compatible computer architecture. The GILLAROO system also includes a plain/cipher switch, an interface for a KOI-18 tape reader device and an RS-232 asynchronous communications port (see Figure 1). The plain/cipher switch provides a system user with the ability to determine whether data leaving the computer is encrypted. The GILLAROO device must be keyed with paper tape keying material via the KOI-18 before being used for communication. The communication software provided with the GILLAROO system is written for the DOS operating system. GILLAROO is designed to allow users, utilizing ordinary personal computers, to communicate classified information over non-secure communication channels.

The general scenario for operation from the user perspective is:

1. Key the GILLAROO device with keying material approved for the level of classified data to be transmitted.

2. While in plain text mode, establish the necessary communication channel (e.g., direct modem-modem connection, via DDN or other wide-area network).

\*XENIX is a trademark of Microsoft Corporation.

\*When this effort originated, Trusted XENIX was an IBM product under the name Secure XENIX. TIS has recently acquired the system and renamed it Trusted XENIX.

© 1989 Trusted Information Systems, Inc.

TH0287-3/90/0000/0271$01.00 © 1990 IEEE 271
3. When ready to transmit classified information, switch the GILLAROO device into cipher mode and send information.

4. Return to plain text mode and discontinue communication.

In essence, the GILLAROO device is designed as a cryptographic switch, which resides between a personal computer processing classified data and an unprotected communications line, with the intent of ensuring that all classified data is safely encrypted before transmission.

Logically, two data streams, plain text and cipher text, are handled by the GILLAROO device. On output from the computer, data sent to the GILLAROO device is encrypted (or not) before transmission based upon the position of the plain/cipher switch. On input to the computer, data received by the GILLAROO device is decrypted (or not) depending upon the contents of the data itself. In other words, decryption is data driven whereas encryption is determined manually via the plain/cipher switch. Between the communications software on the computer and the GILLAROO device, the plain and cipher data streams are interleaved with each other on a byte-by-byte basis. System software is responsible for separating the two data streams.

In terms of multilevel security (which is afforded by a B2 trusted system), it is necessary that high-level data is not transmitted in the clear and that incoming decrypted data (which supposedly was high-level data generated by another workstation) is not mislabeled as low-level data. The basic security policy for the TWS is centered on the notion that the GILLAROO device’s two logically separate data streams, cipher text and plain text, each have different associated sensitivities. To accommodate this security policy view, the protection mechanisms introduced into Trusted XENIX abstract the GILLAROO device into two distinct objects, called PLAIN and CIPHER, which correspond with the plain text and cipher text data streams (see Figure 2). Hence, the philosophy of protection is simple; each object is labeled with its sensitivity and access to these objects is determined in a fashion comparable to other Trusted XENIX objects.

The labels for both the PLAIN and CIPHER objects are site settable, allowing the TWS to be configured into many different operational environments. As with all devices in Trusted XENIX, the GILLAROO device has an associated maximum and minimum security level, referred to as g_low and g_high. By definition, the level of the PLAIN object is the same as that defined by the security administrator for g_low. The presumption is that g_low reflects the level of protection afforded the communication channel attached to the GILLAROO device’s RS-232 external connection, and therefore the sensitivity of all plain text data sent or received via the device. For example, if the GILLAROO device is used to communicate via a commercial telephone system, g_low (and therefore the level of the PLAIN object) would be unclassified. The security level for the CIPHER object is set to the level of the current encryption key, which is loaded by an authorized user. The presumption here is that the current key determines the security level at which the GILLAROO device, in cipher mode, is approved to protect information from unauthorized disclosure. The TWS security policy requires that the key level be within the inclusive range of security levels defined by g_low and g_high.

In order to provide this view of the GILLAROO device, some set of additional trusted software was added to the Trusted XENIX trusted computing base (TCB). This code extends the Trusted XENIX reference monitor to address the additional GILLAROO objects; however, it does not modify the TCB’s existing interface or structure. The additional TWS trusted code consists of a small kernel device driver to provide a trusted interface to the XENIX device and a number of non-kernel trusted processes. For more information on the TWS design philosophy and protection policy, see [4].

3. EVALUATION STRATEGY

Any credible integrated INFOSEC product must reaffirm the evaluation results of the COMSEC and trusted systems technology used in the product, plus provide assurance for the correctness and completeness of any extensions introduced. From the onset of the TWS effort, the issue of ‘re-evaluation’ for the TWS as a single integrated product has been a principal concern. In January 1988, after over a year of informal and formal interaction with representatives of several NSA INFOSEC organizations, TIS formally submitted a request for evaluation of the TWS as an INFOSEC product. Given that any single COMSEC or trusted system evaluation takes several years to complete, it was clear that a re-evaluation for the TWS must rely heavily upon past results in order for the re-evaluation effort to be practical and economical. The TWS evaluation strategy is two-fold:

(1) Demonstrate that the modifications required for the TWS integration are all outside the "COMSEC boundary," and
(2) Have the TWS re-evaluated by the NCSC as a trusted network component based on a previously evaluated trusted operating system.

In essence this is a “divide and conquer” strategy. For reasons discussed in the next section, we believe that the TWS integration effort does not require any further COMSEC evaluation or re-certification effort. Thus our first objective is to remove any concern that the NSA COMSEC evaluation organization might have with the TWS. Once the COMSEC issues are resolved, we will be free to concentrate on the trusted system issues and the NCSC evaluation process.

The trusted system evaluation issues are somewhat more involved. Our primary thesis for the TWS design is that the extensions introduced into Trusted XENIX can be evaluated using the existing Trusted XENIX evaluation data as a basis. In essence, the intent is to argue two issues:

(1) The TWS modification did not, in any manner, lower the assurance level of the underlying Trusted XENIX TCB.

(2) Evidence could be provided that showed that the TWS modifications themselves provide an adequate level of assurance in conjunction with the Trusted XENIX TCB.

Thus, the evaluation issues for the TWS revolve around an examination of the additions to Trusted XENIX and an assessment of the impact of those additions.

4. COMSEC EVALUATION ISSUES

GILLAROO was endorsed by the National Security Agency as a Type I cryptographic product for protection of information at classification levels up to and including Secret. The GILLAROO device was originally endorsed with DOS-based communications driver software. The only COMSEC issue that was identified during preliminary evaluation of the TWS product proposal was whether GILLAROO was being employed in accordance with the terms of its endorsement. The general consensus from our informal discussions with the NSA COMSEC organization was that the TWS use of GILLAROO as an encrypted serial port was consistent with its NSA endorsement and that the TWS communications software does not further require COMSEC evaluation.

5. TRUSTED SYSTEMS EVALUATION ISSUES

Trusted XENIX is currently under formal evaluation as a B2 trusted operating system as defined by the TCSEC [5]. As such, the product is technically evaluated for use in a “stand-alone” mode only. The TWS goal is to extend this evaluation to include distributed operation by having the TWS re-evaluation conducted under the Trusted Network Interoperation (TNI) of the TCSEC [6], specifically as a network component as described in Appendix A of the TNI. This is a logical progression as the difference between Trusted XENIX and the TWS is the inclusion of the GILLAROO device and supporting software whose intent is to securely interconnect more than one system.

While the evaluation of the TWS is referred to as a “re-evaluation,” it is not the intent to evaluate the TWS (including the entire Trusted XENIX operating system) from nothing. Rather, in order to make the entire evaluation effort economically feasible, the intent is to have the TWS evaluation “catch up” to the Trusted XENIX evaluation such that the NCSC can apply its current knowledge from the ongoing Trusted XENIX evaluation to the TWS evaluation. Thus, we expect that the burden for the TWS evaluation is one of arguing that the modifications to Trusted XENIX are themselves secure and do not invalidate any of the previously evaluated Trusted XENIX protection features. This type of “piggy back” evaluation is unique to both the NCSC and our experiences, and is somewhat analogous to the NCSC Rating Maintenance Program (RAMP) [7] (which currently addresses systems as or below B1).

While the system modifications are relatively simple, the evaluation effort is expected to be somewhat more involved. Every TNI requirement must be examined and argued for its completeness. This examination includes not only the functional aspects of the system such as mandatory and discretionary access controls, but the assurance requirements such as formal modeling, descriptive top-level specifications (DTLS), covert channel analysis, and configuration management. Each of these issues must be addressed through a combination of TWS additional (and Trusted XENIX existing) features, documentation, and analysis results. The result is that the TWS are further compounded by the nature of the TWS product, which, when the evaluation issues where originally addressed, was based primarily upon products designed, developed, and supported by other companies.

In the remainder of this section, some of the specific evaluation issues identified during the TWS effort are discussed.

5.1 SECURITY ARCHITECTURE

The TWS is designed to meet the B2 assurance requirements. A central aspect of the B2 assurance requirements is a system architecture that is “internally structured into well-defined largely independent modules” and that incorporates the concept of least privilege. Since it is expected that the underlying Trusted XENIX TCB will meet the B2 system architecture requirements, the objective for the TWS is to ensure that the TWS product is technically evaluated for use in a “stand-alone” mode only. The TWS is designed to meet the B2 level of assurance for the Trusted XENIX TCB, which is somewhat more involved. The TWS extensions to Trusted XENIX consist of a set of device driver routines in the kernel and a number of non-kernel but trusted processes. Implementation of the GILLAROO driver routines were not difficult because the Trusted XENIX kernel is designed in such a way that device drivers may be easily integrated into the kernel. Within the TWS, access mediation for the GILLAROO device is performed in the GILLAROO device driver, which expands the access control policy of the Trusted XENIX kernel to encompass the GILLAROO plain text and cipher text data streams. Although the GILLAROO device driver depends upon the Trusted XENIX kernel, the Trusted XENIX kernel remains functionally and architecturally independent of the device driver. Thus, it is argued that the TWS extensions to the kernel remain faithful to the B2 security architecture requirements.

The TWS trusted processes are necessary to perform certain GILLAROO administrative tasks, such as loading the cryptographic key, in a trusted and reliable fashion. A trusted process can be thought of as a process executing with more privilege than the average user process, but with far less privilege than available to kernel trusted software. Because Trusted XENIX is flexible in providing the ability to incorporate additional non-kernel trusted processes into the system, the introduction of trusted processes was a relatively simple matter. The design and implementation of all TWS trusted processes was performed in a manner consistent with the design philosophy used for all Trusted XENIX trusted processes. To ensure compliance with the principle of least privilege, no privileges are explicitly given to the TWS trusted processes, other than those minimally required to perform their function.

In this manner, it is asserted that the TWS extensions to the Trusted XENIX TCB maintain a B2 level of assurance for the overall system architecture.
5.2 TESTING AND ANALYSIS

Because the TWS extends the Trusted Xenix TCB, it is necessary to re-examine the security testing and covert channel analysis results for Trusted Xenix, and provide additions to address the TWS modifications. We believe that, for the most part, additional security testing and analysis for covert channels can be performed on the TWS additional modules in isolation from the remainder of the Trusted Xenix TCB (except for those portions of the Trusted Xenix TCB for which the TWS code is dependent). With two important exceptions, this hypothesis was found to be true.

The first exception involves an examination of any intended change to Trusted Xenix or the Trusted Xenix TCB. In particular, it is possible that the TWS additions may have introduced potential illicit signalling channels into the underlying Trusted Xenix TCB as result of the extended interface provided by the TWS software.

The second and more significant exception is a result of the introduction of networking aspects to the analysis process. The underlying Trusted Xenix operating system is being evaluated B2 as a stand alone system under the TCSEC. The TWS extensions not only increased the functionality of the system, but also the configuration to include networking of trusted systems. In particular, we were forced to examine any potential covert channels which may be available across the network connection. This network aspect introduced significantly more complexity to the covert channel analysis, requiring a consideration of multiple GILLAROO equipped systems and passive "wire taps" signalling channels. Not surprisingly, most of the potential covert channels identified to date involve signalling between two separate TWS systems.

5.3 DOCUMENTATION

The documentation created for the TWS is structured as additions to the already existing documents and manuals for Trusted Xenix. In all cases, the intent is to discuss the extensions that the TWS modifications add to the underlying Trusted Xenix system. This documentation included the user level documentation, such as Security Features Users Guide and Trusted Facility Manual (TFM), and design documentation, such as the Descriptive Top-Level Specification (DTLS). Of this documentation, the TFM required the most effort primarily due to modifications necessary to address networking and cryptographic key management.

5.4 CONFIGURATION MANAGEMENT

For B2 systems, the TCSEC requires configuration management procedures to control changes to the TCB and associated documentation and test fixtures. For the TWS, the challenge is to devise an adequate configuration management process where the vast majority of protectional critical components (i.e., Trusted Xenix and GILLAROO) are outside TIS's control. Any change to either Trusted Xenix or the GILLAROO may require accompanying changes in the configuration of TWS. The central configuration management issue for successful TWS evaluation was finding a mechanism dealing with such changes. At the time this issue was originally being considered, TIS had no control over changes to either of these products. Therefore, our approach is to treat each actual change to Trusted Xenix (then Secure Xenix) or GILLAROO as a proposed change to TWS. In this light, a synthetic Product Change Request (PCR) is written for each such change. Following standard configuration management procedures, the changes is reviewed by the TWS Configuration Control Board (CCB), and then assigned to one or more members of the development team for an impact assessment. The central purpose of the impact assessment is to determine the extent to which the Trusted Xenix or GILLAROO changes will require changes in TWS. The CCB then reviews the completed impact assessment, and takes one of following actions.

1. If no TWS changes are required, the PCR is considered to have been implemented, and is closed.
2. If the required changes are of acceptable cost, the PCR is assigned to an engineer for implementation.
3. If the changes are unacceptably costly, the PCR is rejected and closed. In this case, the new version of Trusted Xenix or the GILLAROO is treated as an unsupported equipment configuration. Should this happen, TWS cannot continue to support subsequent revisions of Trusted Xenix or GILLAROO.

With Trusted Xenix now under TIS control, configuration management has become less complicated for TWS.

6. CONCLUSIONS

At the time of this writing, TIS has cleared all preliminary milestones with respect to entering into the NSA's INFOSEC evaluation process. As result of several preliminary technical discussions, an "agreement in principal" has been reached on all issues relating to COMSEC certification. In December 1988, the NCSC conducted a preliminary technical review of the TWS product and, as a result of this review, produced a preliminary technical report (PTR). The PTR constitutes the NCSC's initial assessment of the feasibility and utility of evaluating the TWS. The NCSC initial assessment was, for the most part, favorable. Several concerns were raised, most of which revolved around the dependencies between the TWS evaluation and the Secure Evaluation. Both the NCSC and TIS agreed that an evaluation of the TWS would not be economically feasible if conducted in isolation from the ongoing Trusted Xenix evaluation. However, there is strong indication from the NCSC that integration of COMSEC and trusted products is the right approach for developing INFOSEC products.

With the acquisition of Trusted Xenix (and the related evaluation activity), the future of a separate TWS evaluation has become uncertain. Nonetheless, we believe that the evaluation of the TWS, divorced from Trusted Xenix, is a viable proposition. The most difficult problem with such an undertaking is ensuring that the product can be evaluated where the majority of the protection critical aspects of the system is based upon proprietary data of a third party. In order to alleviate many of these concerns, it was necessary to form a relationship with IBM (and PE Systems) that allows for the sharing of proprietary information. Despite the problems of being a third party vendor, we believed that the integration of evaluated COMSEC and trusted system products is a reasonable, economical, and practical approach for developing INFOSEC products.

REFERENCES


