NCSC-TG-008

Understanding Trusted Distribution

A Guide to Understanding Trusted Distribution in Trusted Systems

Library No. S-228,592

FOREWORD

"A Guide to Understanding Trusted Distribution in Trusted Systems," is the latest in the series of technical guidelines that are being published by the National Computer Security Center. These publications are designed to provide insight to the Trusted Computer Systems Evaluation Criteria requirements and guiance for meeting each requirement.

The specific guidelines in this document provide a set of good practices related to trusted distribution of the hardware, software, and firmware portions, both originals and updates, of automated data processing systems employed for processing classified and other sensitive information. This technical guideline has been written to help the vendor and evaluator community understand what trusted distribution is, why it is important, and how an effective trusted distribution system may be implemented to meet the requirements of the Trusted Computer Systems Evaluation Criteria.

As the Director, National Computer Security Center, I invite your recommendations for revision to this technical guideline. We plan to review this document biannually. Please address any proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000
Attention: Chief, Criteria and Guidelines
Patrick R. Gallagher ,Jr. 15 December 1988
Director
National Computer Security Center

ACKNOWLEDGMENTS

Acknowledgment is also given to all those members of the computer security community who contributed their time and expertise by actively participating in the review of this document.

1. Introduction

1.1 Purpose

The Trusted Computer System Evaluation Criteria (TCSEC) is the metric used for evaluating the effectiveness of security controls built into Automated Data Processing (ADP) systems. The TCSEC is divided into four divisions: D, C, B, and A, ordered in a hierarchical manner with the highest division, A, being reserved for systems providing the best available level of assurance.. Within division C through A are a number of subdivisions known as classes, which are also ordered in a hierarchical manner to represent different levels of security.

At TCSEC class A1, trusted distribution of the hardware, software, and firmware portions of the Trusted Computing Base (TCB) and their updates shall be provided. Trusted distribution includes procedures to ensure that all of hte TCB configuration items, such as the TCB software, firmware, hardware, and updates, distributed to a customer site arrive exactly as intended by the vendor without any alterations. Additionally, trusted distribution may include procedures that enable the customer site to determine that what was received at the site was actually sent by the vendor. The purpose of this guideline is to provide guidance to vendors of trusted systems on what trusted distribution is, why it is important, and how to select and implement an effective trusted distribution system to meet the TCSEC requirement.

Examples in this document are not to be construed as the only implementations that will satisfy the TCSEC requirement. The examples are merely suggestions of appropriate implementations. The recommendations in this document are also not to be construed as supplementary requirements to the TCSEC. The TCSEC is the only metric against which systems are to be evaluated.

This guideline is part of an ongoing program to provide helpful guidance on TCSEC issues and the features they address.

1.2 Scope

An important assurance requirement of TCSEC class Al is that the TCB software, firmware, hardware, and their updates be distributed to a customer site in a trusted manner. This guideline is to be used by vendors of trusted systems in the preparation of procedures, techniques, and equipment to establish trusted distribution between a vendor site and a customer site. This guideline will discuss trusted distribution as it relates to computer systems and products that are intended to meet the Al requirements of the TCSEC.

1.3 Control Objective

Trusted distribution focuses primarily on the assurance control objective of the TCSEC. The assurance control objective states:

"Systems that are used to process or handle classified or other sensitive information must be designed to guarantee correct and accurate interpretation of the security policy and must not distort the intent of that policy. Assurance must be provided that correct implementation and operation of the policy exists throughout the system's life cycle."[7]

Any alteration to the TCB at any time during the system life cycle could result in a violation of the system security policy. Assurance that the system security policy is correctly implemented and operational throughout the system life cycle is provided by different TCSEC requirements. At TCSEC class AI, trusted distribution, in conjunction with configuration management, provides assurance that the TCB software, firmware, and hardware, both original and updates, are received by a customer site exactly as specified by the vendor's master copy. Trusted distribution also ensures that TCB copies sent from other than legitimate parties are detected.

2. OVERVIEW OF TRUSTED DISTRIBUTION

2.1 Threats

The different divisions of the Trusted Computer System Evaluation Criteria (TCSEC) were developed to protect against threats that could be directed towards Automated Data Processing (ADP) systems. Each higher class is required to provide additional features and assurances over the next lower class, thus providing increasing levels of trust. At the C level and above, passwords and audit mechanisms provide ways to restrict access to a system and make users accountable for their actions. At the TCSEC B level, the addition of labeling mechanisms control access to data based on clearances of subjects and classifications of objects.

The class of system needed by a specific site should be determined by the types of threats that are faced by that site. Generally, the class of system is dependent upon the sensitivity level of the data that are being processed by the site and the clearance of the system users. According to the Guideline for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments[5], a risk index corresponding to the minimum clearance or authorization of system users and the maximum sensitivity of data processed by the system can be used to determine the minimum evaluation class required by a site.

The features and assurances in lower class systems protect against the threat that someone will tamper with a system while it is in operation, but it is at TCSEC class AI that the threat of subversion is addressed. Computer subversion is the name generally applied to deliberate, malicious modification of executable code or hardware within a computer system. The subversion can be accomplished at any time during the system's life from the earliest stages of design to the last day of its use. A component can be subverted either to permit later penetration or as an act of sabotage-to nullify or to degrade the system's capability. Forms of subversion include the trap door, the Trojan horse, and computer viruses. The threat of subversion exists at all classes; however, the benefit of providing assurance features to guard against it in lower class systems may not justify the cost of this type of protection.

There are basically two threats that trusted distribution protects against.

The first is the threat of someone tampering with a system during its movement from a vendor site to a customer site. Throughout this document the term "vendor site" will be used to mean the point from which the TCB hardware, software, and firmware to be distributed are sent. The term "customer site" is the point at which the distributed material is accepted. Specifically, any system component that participates in the enforcement of the security policy of the system is what needs to be protected. For example, someone may break into a delivery truck and insert malicious code into a trusted system before it reaches the customer site. The system or update being delivered, when installed at the site, will contain the harmful code that could cause compromise of the system's security policy. Trusted distribution may include protective packaging methods that protect against changes being made to a system (see Section 4.1 Protective Packaging). Trusted distribution may also include methods of detecting if a system and/or its updates have been accidentally or maliciously altered during or after distribution through validation tests (see Section 4.7 Site Validation).

The second threat protected against by trusted distribution is that the TCB is a counterfeit; that is the system or update did not come from the vendor site. Trusted distribution includes procedures for the distribution of TCB components, such as requiring the vendor to notify a customer site of an impending delivery. By doing this, trusted distribution protects against the threat of sites receiving systems that were not distributed by the vendor and provides assurance that the vendor was the actual sender of the product or update. Trusted distribution should be able to answer the question, "Was what I received really sent from the vendor or an imposter?" Without trusted distribution, all a penetrator needs to do is package a system or update containing a virus or Trojan horse so that it looks as though it came from an actual vendor. The receiving site, upon seeing the packaging, assumes that the system or update is genuine, unaware that it is really a counterfeit. To prevent this from happening, the vendor and customer sites may establish procedures requiring them to agree on when deliveries will be made and what they will contain.

2.2 Purpose of Trusted Distribution

Hostile attacks may occur on computer systems when they are in use, but it is also possible for computer systems to be attacked even before they are installed at a customer site. The TCSEC requires that assurance mechanisms be in place throughout the life cycle of a system to prevent modifications being made to the TCB which could adversely affect the security policy of a system. One such assurance requirement for class AI systems is trusted distribution. Trusted distribution maintains the integrity of the current TCB software, firmware, and hardware as well as any updates to these by ensuring that any changes made to the TCB during the distribution process do not go unnoticed.

"Trap doors can be inserted during the distribution phase. If updates are

sent via insecure communications - either U.S. Mail or insecure

telecommunications, the penetrator can intercept the update and subtly

modify it. The penetrator could also generate his own updates and distribute

them using forged stationery. "[3]

The main purpose of trusted distribution is to protect a trusted system as it is being distributed, and consequently to provide protection for the information that will be processed on the system. Trusted distribution provides assurance that a trusted system arrives at a customer site with all of its security properties intact and that the system or update that is received at the customer site is the, "same system or update which was produced from the master copy of the system evaluated against the TCSEC."[6] Any tampering with the TCB software, firmware, hardware, whether originals or updates, from the time they leave the vendor site to the time they arrive at the customer site may permit the security policy of the system to be circumvented.

Trusted distribution provides protection against tampering and a means of detecting that a system has been altered; it accomplishes this through physical devices (locks), electronic devices (encryption), and procedures (bonding of couriers). It also provides procedures for site validation so that if the protection mechanism[s] should fail, any modification to the TCB software, firmware, hardware, both originals and updates, will not go unnoticed. If sufficient trust can be placed in either the protection methods or the customer site validation, it is possible to use that method exclusively. If not, it may be necessary to apply techniques for both the protection of the shipment and validation.

2.3 Life-Cycle Assurance

Trusted distribution is one link in a chain of assurances provided by trusted systems. It is helpful to take a look at all of the other activities that take place to ensure that the system in operation is the one that the vendor and customer agree upon.

The following is a summary of the assurances that are needed to ensure that the product delivered to a customer site is operating under a correct implementation of the system's security policy:

- Assurance that the product evaluated is the one the manufacturer built
- Assurance that the product built is the one that was sent
- Assurance that the product sent is the one the customer site received.

Long before a system is boxed and prepared to be sent to a customer site, assurance needs to be provided that the system is being built as specified. The TCSEC class Al design specification and verification requirements require a formal top-level specification (FTLS) to be maintained that accurately describes the system. The FTLS is shown to be consistent with the TCB interface. Additionally, specification to code mapping provides assurance that the design has been properly implemented.

Configuration management provides control over the design and development of a system, ensuring that the system is built to specification. The main purpose of configuration management is to ensure that any changes to the system during design, development, or during the system life cycle "take place in an identifiable and controlled environment and that they do not adversely affect the implementation of the security policy of the TCB."[4] More information on configuration management can be found in A Guide to Understanding Configuration Management in Trusted Systems (NCSC-TG-006).

Once the system has been built, security testing shall be performed to ensure that the system works exactly as claimed in the system documentation. The security testing shall demonstrate that the TCB implementation is consistent with the FTLS.

Trusted distribution provides assurance that the security policy of a system is not violated during distribution of the system. For trusted distribution to be successful, the TCB shall have been under configuration management throughout the development process, ensuring that the integrity of the developer's master copy of the TCB has been maintained. Without configuration management in place during the design and development of a system, the assurance provided by trusted distribution will be suspect. True, it will still protect against any tampering with a system during delivery, but if the system being delivered has already been tampered with during development then the damage has already been done.

Once the system is in operation at a customer site, assurance shall be provided throughout the system life cycle that the security policy of the system is correctly implemented. Configuration management continues throughout the system life cycle ensuring that any changes to the system take place in a controlled environment. It is said that "a chain is only as strong at its weakest link," and if any of these assurances fails during the system life cycle, the probability that the security policy of the system could be violated increases.

2.3.1 Assurance for Different Types of Production

Not every distribution is as simple as having the entire computer system designed, developed, and assembled in a vendor's facility and then shipped to a customer site. Most computer systems, particularly large-scale computer systems, comprise several parts which are produced separately and need to be assembled.

The distribution process for a trusted system may be as simple as shipping from vendor sites to customer sites, or may be as complex as from vendor to central sites to other sites, or from software development center sites to other sites, etc. If development is done at different sites and then integrated at yet another site, the pieces of the system transferred between these sites during development should be subject to the same trusted distribution requirements as the final TCB product. The item, at the point of transfer to a customer site, should be a true reflection of the vendor's master copy.

The manner in which the TCB components are handled prior to distribution will have an impact on the trusted distribution process. The following is a recommendation for how a vendor may provide assurance before the components are actually shipped. "There are basically two types of production that companies employ: mass production, and production per request basis. In either case, there will probably be idle time where the system(s) will be waiting for delivery probably in some type of warehouse. Strict accounting procedures and physical controls must be placed on the system(s) both during the delivery to and stay in the warehouse to ensure that no unauthorized modifications are made. For example, controls must exist which log any entry into the warehouse, authorizations for the alteration of any system or range of serial numbers within the warehouse must be properly documented, etc." The "trusted warehouse" spoken of in the preceding paragraph is not a TCSEC requirement, but when considering that trusted distribution really extends further than just providing assurance from vendor loading dock to customer site loading dock, it should be considered. The assurance that trusted distribution provides is dependent on a system not being altered before being loaded onto a delivery truck. The control of the system during "idle time" should be performed by configuration management practices, emphasizing the importance of configuration management in trusted distribution.

3. THE TCSEC REQUIREMENTS FOR TRUSTED DISTRIBUTION

This section lists the TCSEC requirements for trusted distribution. These requirements have been extracted from the TCSEC and have been listed separately and numbered. How these requirements can be met will be discussed in the following sections of this document. This section is designed to serve as a quick reference for the TCSEC requirements for trusted distribution.

Trusted distribution is required at TCSEC class Al, and the requirement can be broken down into two parts.

Requirement 1 - "A trusted ADP system control and distribution facility shall be provided formaintaining the integrity of the mapping between the master data describing the current version of the TCB and the on-site master copy of the code for the current version."[7]

Requirement 2 - "Procedures (e.g., site security acceptance testing) shall exist for assuring that the TCB software, firmware, and hardware updates distributed to a customer are exactly as specified by the master copies."[7]

4. IMPLEMENTATION METHODS

This section describes various implementation methods that can be used to establish a trusted distribution system and the advantages and disadvantages of each method. When choosing a protective packaging system or a customer site validation process, remember that some devices or techniques provide a higher degree of protection than others. The higher the threat to the distribution system, the greater the need for more stringent measures or multiple levels of trusted distribution methods. In many situations, multiple methods for trusted distribution should be used, such as a protective packaging system during distribution and site validation upon receipt. This layered approach will counter the insider threat or the threat of collusion where employees themselves alter the contents of a package before it is distributed. Each situation that requires trusted distribution is unique and requires that the system be addressed individually.

For a National Computer Security Center Al evaluation, a vendor must submit a plan that describes the trusted distribution method(s) for the system under evaluation. This plan should include a description of the procedures to be followed and the mechanisms (type of packaging) to be used for distribution of both initial versions and updates. Any deviation from the trusted distribution plan submitted could jeopardize the evaluation rating.

There are other requirements in the TCSEC which are related to trusted distribution, namely those concerning configuration management. A vendor

should be sure that the system sitting on the loading dock is the system that the vendor thinks it is. At TCSEC class Al, the configuration management system shall include, "a combination of technical, physical, and procedural safeguards" to be "used to protect from unauthorized modification or destruction the master copy or copies of all materials used to generate the TCB."[7] All of the implementation methods that follow are contingent upon prior performance of configuration management, ensuring that the system has not been maliciously altered before being distributed.

A related concern that plays a part in trusted distribution is that communication should be established between the vendor and customer sites for both the initial and updated distribution of the TCB software, firmware, and hardware. The procedures used should include agreement between the vendor and customer sites as to the methods to be used for distribution and the time frame in which the distribution will be made. The sender (the vendor) and receiver (the customer) should be uniquely identified prior to distribution for the trusted distribution system to function successfully. It is essential that this identification be made and that procedures be in place for manufacturers to notify users of pending shipments. Included in this identification should be the unique identification of every component to be shipped. This identification will allow for the detection of any system configuration changes. Additionally, the customer should have procedures in place that will keep the customer advised of the latest changes from the vendor. At a minimum the customer should enforce a policy that forbids the use of any new TCB software, firmware, or hardware without prior notification from the vendor of the most current change, to include the date each change to the TCBo was sent and the means by which the TCB software, firmware, and hardware was sent.

Another concern is the reliance on the individuals involved in the design, development, manufacturing, and distribution of the trusted system. Each individual who is involved in the system prior to and during distribution should be subject to review that would verify his or her trustworthiness and reliability. Particularly for distribution, all individuals who play a significant role in the establishment of the control at the shipping end, or the validation at the receiving end should be worthy of the trust placed in them to perform their roles reliably. Without this step, any process for protection is subject to an insider compromise.

4.1 Protective Packaging

Protective packaging is a way of wrapping an item so that it cannot be opened and resealed without leaving some obvious indication that the package has been tampered with. Protective packaging can be provided to limit access to the TCB software, firmware, and hardware during shipment and to guarantee their delivery in an unaltered form. Protective packaging ranges from simple shrink wrapping to complex fiber-optic techniques. The wrapping for shipments should allow the sender and the package contents to remain anonymous. Techniques

such as double wrapping the materials to be distributed or an absence of exterior markings when using shrink wrapping could accomplish this. The technique used for packaging the TCB components for distribution shall be documented in the trusted distribution plan.

Protective packaging not only limits access to the materials being distributed, but also aids in protection against environmental factors, such as dust and water. It is not possible to present every protective packaging technique; however, the examples that follow are provided to present some of the methods that are currently in use.

4.1.1 Shrink Wrapping

Shrink wrapping is one method of trusted distribution which consists of enclosing the product in a plastic film. This method may be used for TCB hardware, software, or firmware, but since it does involve the use of heat, it should not be used for computer-related equipment that is very sensitive to heat.

When heat is applied to the plastic film in shrink wrapping, the film contracts, or shrinks, forming a tight seal around the product. If the shrink-wrapped seal is broken, this is an indication that the product being shipped has been tampered with. Not only is shrink wrapping used for the trusted distribution of TCB components, but many industries including the food and drug industry use shrink wrapping to provide consumer protection that products have not been tampered with. Additional special shrink-wrap techniques are available that may increase the reliability of the shrink wrap.

The size and construction of the materials to be packaged are important considerations when selecting a shrink-wrapping technique. For example, shrink wrapping products the size of mainframe central processing units (CPUs) or mainframe disk drives is currently not done because of their large size. Techniques will need to be improved to make shrink wrapping a feasible packaging option for these types of products.

4.1.2 Active Systems

The use of active systems for protective packaging is a viable method for the distribution of TCB software, firmware, and hardware. This method was originally intended to secure personal computers and electronic equipment. Conceptually, an active system could include looping a fiber-optic cable through a latch on the opening of a container and attaching the cable to a control unit via an alarm. An active system provides assurance that a package cannot be entered without triggering the alarm.

An advantage to the active systems method is that there is a real-time notification of any tampering with the TCB hardware, software, or firmware as they are being

delivered. It is very possible that anyone tampering with the product could be caught before having a chance to modify the system. This real-time notification can be circumvented, though, by interfering with the alarm so that the signal will not be picked up. In these cases, the break-in will be detected but not until the delivery truck reaches its destination. True, it will presumably be too late to catch those responsible for the attack, but the detection provided by active systems will prevent an altered component from being used that could result in a security policy compromise.

4.1.3 Tamper-Resistant Seals

The use of tamper-resistant seals is another method of protective packaging that may be used to protect the distribution of large TCB software, firmware, and hardware items. One example of a tamper-resistant seal for large items shipped by truck is a special-purpose truck seal. This device generates a random 4-digit number when installed on a truck door. When the door is opened a new random number is generated. The device is encased in metal and epoxy resin to prevent tampering. By sealing the truck at the vendor facility and sending the number to the customer site by secure means, it is possible for the user to determine whether or not the truck cargo has been opened.

Other forms of locking devices and seals, such as a high impact security lock or company registered seals, can also be applied before shipment and verified prior to opening. The different sealing devices used provide different degrees of assurance and should be selected based on the needs of the item being distributed.

4.2 Couriers

The use of a courier service is a possible way to establish the trusted distribution of TCB software, hardware, firmware, both originals and updates. Couriers provide the advantage of constant surveillance of the materials they are transporting. The use of couriers increases the reliability of any delivery system and can easily be used in conjunction with other protective methods such as locking devices and protective packaging.

There are several commercial firms that can supply bonded services, or manufacturers may use their own internal courier service, if available. Within the military, the Defense Courier Service (DCS), formerly known as the Armed Forces Courier Service (ARFCOS), is an alternative.

It is possible to transport the most sensitive materials by means of couriers.

The TCB products to be distributed should be considered to be as sensitive as the data they are being used to process and should be treated accordingly. Depending upon the sensitivity of the material to be distributed, the vendor

and/or customer site may want to establish regulations regarding who may act as a courier, what type of materials they may transport, and where the material may be delivered. A partial list of guidelines for the use of courier service is provided below.

Persons acting as couriers should be trusted to the level of the

material they are transporting

- · Material should remain in their personal custody at all times
- · Vendor as consignor should be responsible for the safety of the material
- · Vendor should notify the customer site of the nature of the shipment, the means of the shipment, number of seals (if used), and the anticipated time and date of arrival by separate communication at least 24 hours in advance of the arrival of the shipment in order that the customer site may take appropriate steps to receive and protect the shipment.

For the use of a courier service to provide trusted distribution successfully, assurance should exist that the TCB software, firmware, or hardware is not modified while stored in a warehouse before being picked up by the courier. Otherwise, the assurance provided by the courier will have been defeated.

4.3 Registered Mail

Registered mail can be part of the trusted distribution of TCB hardware, software, and firmware to a customer site without any undetected disclosure or loss. Although registered mail alone is not sufficient for meeting the TCSEC trusted distribution requirement, it does not preclude it from being a part of the trusted distribution process. The reason that registered mail alone does not satisfy the TCSEC requirement is that although the customer site has to verify its identity before being allowed to receive a package via registered mail, the sender does not have to show any form of identification to mail a package. This can result in the scenario detailed earlier in which someone can duplicate a vendor's wrapping and markings and mail a malicious update or system. Provided that the registered mail is supplemented by other adequate mechanisms to compensate for its shortcomings, such as an unforgeable internal signature to ensure the identity of the sender, it can meet the trusted distribution requirement and provide assurance that what was delivered through the mail actually came from the vendor.

When sending TCB software, firmware, hardware, originals or updates, via registered mail, the products should be considered to be as sensitive as the data they are being used to process and should be treated accordingly. Some procedures to be observed when using registered mail for trusted distribution include:

- · Material to be transmitted should be enclosed in opaque inner and outer containers
- · If the material is in a hard-copy form and is of such size as to permit the use of envelopes for wrapping, the contents should be protected from direct contact with the inner container by a cover sheet or by folding inward.

4.4 Message Authentication Codes

Message Authentication Codes provide an effective means for transmitting segments of TCB software. The banking system is one of the largest users of electronic distribution, and has successfully used Message Authentication Codes for several years. A Message Authentication Code employs an encryption process for a data stream and from this process develops a unique code that is appended to the data stream. It is important to note that only the appended code is actually encrypted, and the message remains in plaintext. The process, repeated by the recipient, must then produce the identical code.

If the codes are not the same, this is an indication that the code being

transmitted has been tampered with. The length of the appended code can vary,

but the strength of the process is directly related to the length of the code. As with

all encryption-based processes, the management and protection of the key ancinor

algorithm is a critical factor that shall be addressed in the design documentation.

4.5 Encryption

Encryption of the entire text is an effective way of protecting data from compromise or modification attacks. Encryption has the advantage not only of preventing undetected changes to the TCB software, but also of preventing viewing of the code for any person without the key. Encryption of TCB software with public or private key techniques is a viable method of trusted distribution, provided that the keys are properly managed, protected, and changed at frequent intervals. In the event that the keys are compromised, it would be possible to alter the TCB software without detection of the alteration.

As stated before, the success of encryption is dependent upon the protection of the key. For this reason, the key should be subject to some form of trusted distribution, such as courier, to ensure that it is not compromised. Encryption provides a significant increase in the quality of assurance; however, management of the system, for example, key generation and distribution, can

become a very complex and time-consuming activity that needs to be well defined in the design documentation.

4.6 Site Validation

Site validation is validation by the customer site that the TCB hardware, software, and firmware received are exactly as specified in the master copy. Site validation is most commonly performed on the TCB hardware items that are shipped, but TCB software and firmware items should also be subject to some type of validation testing upon receipt. Site validation includes methods for validating that a system has not been tampered with during its movement from vendor site to the customer site. Site validation provides a second layer of assurance for trusted distribution. In the event that any of the TCB components were altered during distribution, site validation procedures should detect the alteration before the system is installed and any compromise of security policy can take place.

4.6.1 Checksum Programs

Checksum programs provide an acceptable means to detect TCB software and firmware changes during electronic or physical distribution. In this validation method, a group of digits are summed and then checked against a previously computed sum to verify that no digits have been changed since the last summation. Any difference in the two sums would indicate that the piece of software being checked had been modified. The following is taken from the Final Evaluation Report of SCOMP [2] and describes how SCOMP used the checksum method for software distribution.

"When a site purchases a SCOMP system, a description of the desired configuration must be sent to Honeywell. A set of configuration files are then set up and the desired release, with the site specific configuration files, is generated. A checksum algorithm is then applied to the executable code. The executable code is sent to the site along with a checksum generation program. The checksum that was originally generated is then sent to the site. The site can run the checksum generation program and compare the result with the checksum delivered through the mail. The two checksums provide a means whereby the site can ascertain that the system that they received was the same system that Honeywell sent to them."[2] It should be noted that there are ways to improve this approach. The checksum program should not be distributed with the TCB software. Trusted distribution implementing checksums should consist of sending one package containing the checksum generation program and checksum result and another package containing the TCB software. Both packages should be protected by appropriate means of trusted distribution such as courier or registered mail. Anyone having access to both the checksum generator and the TCB software could retrieve the output from the checksum program through a print command and alter the system so that the change would go unnoticed by saving the original checksum value, modifying the system, and running the

checksum program until it matches the original checksum, adding modules to inconsequential areas of the system when necessary. It may take some time to get the checksum of the modified software to equal the original checksum, but with a 16-bit or smaller checksum it may be a practical method for modifying TCB software.

Additionally, current AI systems should enhance their checksum implementation by using cryptographically protected checksums. Encryption of the checksum and result increases the assurance provided, by preventing anyone from viewing the checksum result. It also provides protection against the scenario described above because no one would be able to view the checksum result without possessing the proper cryptographic key.

A disadvantage to this implementation is that a checksum program will not limit viewing of the TCB software; it will, however, provide a level of assurance that the transmission has not been altered.

4.6.2 Inventory

An inventory is a minimal way of performing customer site validation of TCB hardware. Although this will not meet the TCSEC requirement for trusted distribution, it may provide an acceptable level of assurance for some sites. An inventory is a simple means of inspecting for the presence or absence of a piece of hardware. It consists of an inspection to see if each piece of equipment listed on the inventory arrived at its destination. The assurance provided by an inventory may be increased by inspecting the lower level elements of the TCB hardware. These elements would include such things as circuit boards and chips.

The disadvantage of conducting a physical inventory is that many different hardware families use some of the same hardware components, and a physical inventory of hardware at each end of the distribution chain will not detect the substitution or change of these similar components in the hardware. It will, however, serve to detect any gross discrepancies between the items sent and received.

The advantage of performing an inventory is that it provides a quick method of checking that the TCB components sent were the ones requested. The assurance it provides will be minimal, but a simple oversight or error in shipping or the loss of an item may be detected in this manner. A copy of the invoice should always be in a sealed envelope and a second copy should be sent by alternate means, such as a courier, so that any invoice tampering can be easily detected.

4.6.3 Engineering Inspection

An engineering inspection provides a more thorough check than an inventory and may satisfy the TCSEC requirement for trusted distribution of TCB hardware components. It differs from an inventory in that it is a detailed inspection by a qualified technician in a specific area. The technician should be capable of detecting any changes to the inspected equipment that would affect the TCB. Engineering inspections should be provided for critical parts of the TCB hardware to ensure that the components of the hardware are present and unchanged, such as ensuring, for example, physical location and serial numbered parts, are as specified.

A disadvantage to an engineering inspection is that it can be very time-consuming and it may not be possible for a technician to inspect all of the TCB hardware components because of the locations and construction of the equipment being inspected. This time element may be offset by a simplified version of this safeguard consisting of a confidential agreement between the vendor and the customer as to which parts of the TCB hardware are to be inspected in detail. This will reduce the amount of effort to a reasonable level and, if the specific components are properly identified, will provide an acceptable level of assurance that no changes have been made.

5. SAMPLE IMPLEMENTATION

5.1 Trusted Distribution of Hardware, Firmware and Software

The preceding sections of this document have addressed different methods that may be used for trusted distribution, but none has explicitly stated what will satisfy the TCSEC class Al requirement for trusted distribution. The following paragraphs describe sample methods for meeting the trusted distribution requirements. It should be noted that these are not the only methods that will satisfy the requirement. Through the guidance offered in this document, it is hoped that vendors will be able to investigate other creative methodologies to satisfy the trusted distribution requirement.

When a system is directed to be transported, an acceptable methodology would be the use of a bonded courier service. The courier would accompany and be responsible for the safety of the system. Alternate methodologies would be protective packaging (protecting against unauthorized modifications), registered mail, and, specifically on software, the use of encrypted checksums.

Upon arrival of the system at the purchaser's site, the success of the protective packaging methods provided by the vendor should be validated. It is, however, the vendor's responsibility to provide either the documentation or the manpower to assist the purchaser in determining if the methods used were successful. Additionally, it is the purchaser's responsibility to provide configuration management for the system throughout the remaining life cycle of the system.

5.2 Trusted Distribution of Documentation

Trusted distribution shall be provided for the distribution of the TCB hardware, software, and firmware. It can also be said that trusted distribution is required for all of the TCB configuration items as identified in the configuration management plan for a system. When speaking of configuration items, one should include the documentation for the system. Although not required by the TCSEC, the documentation and configuration records for a TCSEC class AI system should be delivered to the customer site through trusted distribution. In the event that these documents are altered during distribution, it is possible that the system could be configured in a manner that would violate the security policy of the system. For instance, documentation on a TCB mechanism could be altered to allow the mechanism to be used in a harmful way. Trusted distribution of the documentation of the system will ensure that the documentation has not been altered during distribution and accurately describes the system.

6. SUMMARY OF TRUSTED DISTRIBUTION

Trusted distribution is necessary to ensure that the TCB software, firmware, and hardware developed by a vendor arrive at a customer site exactly as specified by the master copy that has been evaluated against the TCSEC. Modification of any TCB software, firmware, or hardware, originals and updates, could result in a compromise of the system's security policy. Trusted distribution is a part of the life-cycle assurance required for trusted systems that ensures that the security policy of a trusted system remains intact throughout the life cycle of the system. Trusted distribution provides assurance that the TCB components will not be altered during their distribution from a vendor to a customer site. Generically, this process of end-to-end control can be broken down into three stages: post-production, transit, and delivery. Along with configuration management and the other assurance requirements of the TCSEC, assurance is provided that no violation of a system's security policy can occur.

Trusted distribution includes methods of protecting the TCB components during distribution, and in the event of alteration, methods of detecting that the system has been altered before it is installed and compromise of the security policy occurs. In the latter case, TCB software containing a virus could be distributed to a customer site by an imposter with the intentions of compromising the data processing facilities.

Advances in the ways of attacking a system and an increase in insiders committing crimes necessitate greater degrees of protection to be provided ADP systems. Therefore, a successful trusted distribution system should consist of dual methods of protection and detection and should not rely on any one technique.

GLOSSARY

Check Sum

A check in which groups of digits are summed, usually without regard for overflow, and that sum checked against a previously computed sum to verify that no digits have been changed since the last summation. [9]

Configuration Item

The smallest component of hardware, software, firmware, documentation, or any of its discrete portions, which is tracked by the configuration management system. [4]

Configuration Management

The management of security features and assurances through control of changes to a system's hardware, software, firmware, and documentation throughout the development and operational life of the system. [8]

Encryption

The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process (two-way encryption).

[8]

Fiber-Optic Latches

An active system method available for trusted distribution. In this method, a fiber optic cable is looped through a latch on the opening of a container and attached to a control unit. The control unit sends a light signal through the cable. If the light is interrupted by the cutting or damaging of the cable in any way, an alarm is set off. The alarm can be audible or telemetric.

Formal Top-Level Specification

A top-level specification that is written in a formal mathematical language to allow theorems showing the correspondence of the system specification to its formal requirements to be hypothesized and formally proven.[7]

Message Authentication Code

A cryptographically computed number which is the result of passing a message through the authentication algorithm using a specific key. Lengths of from 8 to 16 hexadecimal characters can be used.[1]

System Life-Cycle

The period of time that a system is in existence, including its design, development, implementation, transportation, installation, maintenance, and disposal.

Trap Door

A hidden software or hardware mechanism that can be triggered to permitsystem protection mechanisms to be circumvented. It is activated in some innocent-appearing manner; e.g., special "random" key sequence at a terminal. Software developers often introduce trap doors in their code to

enable them to reenter the system and perform certain functions.[8]

Trojan Horse

A computer program with an apparently or actually useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process to the detriment of security or integrity. [8]

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system-including hardware, firmware, and software-the combination of which is responsible for enforcing the security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The

ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy. [7]

REFERENCES

1. American National Standards Institute, Financial Institution Key Management (wholesale), X9.9, 1982.
2. Department of Defense Computer Security Center, "Final Evaluation of SCOMP, Secure Communications Processor, STOP Release 2.1," CSC-EPL-85-001, September 23,1985.
3. Karger, 2LT Paul A. and Schell, Maj. Roger R., Multics Security Evaluation,

Vulnerability Analysis, Electronic System Division, ESD-TR-74-193, June 1974.

4. National Computer Security Center, A Guide to Understanding Configuration Management in Trusted Systems, NCSC-TG-006, March 28,1988.

5. National Computer Security Center, Computer Security Requirements Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-003-85, 1985.

6. National Computer Security Center, Criterion Interpretation Discussion #943, September 1986.

7. National Computer Security Center, DoD Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985.

8. National Computer Security Center, Glossary of Computer Security Terms, NCSC-TG-004, 1988.

9. Sippl, Charles J., Computer Dictionary, Howard W. Sams & Co., Inc. Fourth Edition, 1985.