Open Software Foundation **C. Blauner (Bellcore)**
Request For Comments: 64.0 **J. Schindler (HP)**
October 1994 **OSF Security SIG**

SECURITY SIG STRATEGY DOCUMENT

1. INTRODUCTION AND OVERVIEW

This is, to some extent, a ''historical'' document. It is the product of the OSF Security SIG, and was originally produced and presented to OSF in October, 1992. This RFC version of the document is a reproduction of the original document — verbatim, except for minor editing (reformatting, clarification, correction of typographical errors), and the addition of this introductory paragraph and an Acknowledgements section. In particular, this document has not been substantively revised to take into account recent events, such as the course of technological progress over the last two years, or the 1994 re-organization of OSF and the introduction of Pre-Structured Technologies (PST's) into OSF's process model. It is anticipated, however, that this RFC will now become a ''living document'', and that such revisions will be undertaken in the future.

1.1. Background

Security and security controls are important attributes to Unix-based system environments. This is of particular importance when operating in an open, heterogeneous, networked environment. OSF technologies need to focus on the integration of all OSF technologies in a secure operating environment.

1.2. Purpose

The purpose of this security strategy document is threefold:

(a) Present to OSF the security requirements and recommendations of the OSF members active in the Security SIG. These requirements and recommendations are intended to assist OSF in developing current and future security activities across all OSF offerings.

(b) Provide guidelines and assist OSF in setting policy for ensuring consistent and interoperable security functionality which will be supported across all OSF offerings.

(c) Identify and define those specific areas that such a security strategy needs to address.

1.3. Scope

This document addresses three main *strategy areas*:

(a) Product implementation strategy.

(b) Evaluation strategy.

(c) Standards strategy.

Each of these three main strategy areas is further presented in two sections dealing with *timelines*:

(a) A section that addresses the *short-term* requirements (defined as a 1 to 3 year focus).

(b) A section that addresses the *long-term* requirements (defined as a 3 to 5 year focus).

Each of the three strategy areas identify specific *subjects*. These subjects are described and defined in both a short, high-level *overview*, and a more in-depth *definition* with *supporting rationale*.

1.4. Outline

We state the OSF global security strategy as follows:

> Provide security solutions across all OSF offerings that meet the current and future commercial requirements for information security.

As stated above, this global strategy statement is decomposed into the following outline of 3 strategy areas and their timelines (this serves also as the outline of the remainder of this document):

(a) Product Implementation Strategy

  (i) Short-Term (1 to 3 year focus)
    [a] Integrated Security Solutions
    [b] Distributed System Security Framework
    [c] Variety of Security Features
    [d] Variety of Security Policies
    [e] Ease of Use
    [f] Maintenance of System Attributes
    [g] Evaluatable Offerings
    [h] Exportability
    [i] Security Testing

  (ii) Long-Term (3 to 5 year focus)
    [a] Research/Technology Related
    [b] Requirements Focused
    [c] International Orientation
    [d] Commercial Market Applicability

  (iii) Implementation Considerations
    [a] Short-term: Approximately 85% of OSF security resources towards this.
    [b] Long-term: Approximately 15% of OSF security resources towards this (plus possible external funding options).

(b) Evaluation Strategy

  (i) Short-Term
    [a] Operating System: B1 (TCSEC), F(B1)/E3 (ITSEC), Commercial
    [b] Distributed System

  (ii) Long-Term
    [a] Operating System: B3 (TCSEC), F(B3)/E5 (ITSEC), Commercial
    [b] Distributed System

(c) Standards Strategy

  (i) Short-Term (Participation)
    [a] Identify Standards Applicable to or Impacting Security in OSF Offerings
    [b] Determine Those Security Standards Efforts able to Influence
    [c] Prioritize Efforts to Influence Applicable Security Standards

  (ii) Long-Term (Leadership)
    [a] Identify Areas of Interest for Security Standardization
    [b] Prioritize Efforts
    [c] Lead Effort to Push for Applicable Security Standards

1.5. Summary of Short-Term Product Implementation Strategy

This section summarizes our conclusions regarding the items listed as ''short-term product implementation strategy'' in the preceding section. We believe this is the core message of this document.

(a) Integrated Security Solutions

A consistent set of security features and assurances should be provided as an integrated part of all OSF offerings. All OSF offerings should be capable of enforcing a consistent security policy as defined by the end user or system vendor.

For example, the DCE, DME, and Motif offerings should provide security capabilities equivalent to the capabilities in OSF/1. Likewise, the principle of least privilege should be enforced consistently throughout all of OSF's offerings.

(b) Distributed System Security Framework

OSF should develop an end user oriented distributed systems framework centered around interoperability and portability of secure applications in different environments. Such environments should include single machine/ realm, and multiple realm internetwork (including non-DCE realms). This framework should allow for different security policies and address items such as: prevention, detection, recovery, and administration.

(c) Variety of Security Features

OSF should provide a variety of security features focused on commercial end user requirements. The metrics used for these commercial requirements should include TCSEC, ITSEC, and applicable commercial standards when available. The security features should be selectable.

(d) Variety of Security Policies

OSF should support a wide range of customer based information security policies. The supported policy elements should be derived from customer policy input and focused on actual threats. Customer usage or specification of a specific policy item should not require customer implementation of unrelated or unnecessary policy items. The security policies should be selectable.

(e) Ease of Use

The security features of all OSF offerings should be easy to use and manipulate in both distributed and single system environments. All security interfaces should be designed to prevent security and integrity errors due to the accidental or inadvertant misuse of security features and data. Security policies and features should be configurable/selectable by a system's security administrator in a simple and straightforward manner.

(f) Maintenance of System Attributes

All basic system attributes and general requirements should be maintained whenever the customer enables security functionality. The customer should not have to make major trade-offs between security and other system attributes (e.g., function, performance, serviceability, etc.).

(g) Evaluatable Offerings

All OSF offerings should be evaluatable under all applicable security evaluation criteria. This includes providing all necessary features, documentation, test suites, quality assurances, and appropriate configuration management practices. Specifically, the OSF/1 system and the Motif window management environment should be evaluatable under the TCSEC C2 and B1 criteria, the ITSEC F(C2)/E2 and F(B1)/E3 criteria, and equilivant commercial criteria as available. Other OSF offerings (e.g., DCE and DME) should offer features which are consistent with these criteria and should be evaluatable under the criteria as applicable.

The OSF offerings should also be evaluatable under a ''Fast Track'' (if available) evaluation process to minimize the evaluation time and effort.

(h) Exportability

OSF should ensure that the security features in its offerings are exportable and not restricted by U.S. State Department regulations. OSF should work toward making export regulations more conducive to international business.

(i) Security Testing

All system components should be analyzed and tested for potential security flaws including appropriate penetration analysis. This analysis and testing should be performed for all OSF offerings including those not targeted for formal evaluation. Security testing must be included in all interoperability testing. Testing must be conducted with the security features turned on, and with the appropriate combinations expected in a normal commercial environment.

2. SHORT-TERM PRODUCT IMPLEMENTATION STRATEGY

2.1. Integrated Security Solutions

OSF is currently working on 5 technologies: OSF/1, MOTIF, DCE, DME, and ANDF. Vendors are planning on using one or more of these products in various combinations. It is essential that these products function well in an integrated fashion. This is widely recognized. However, when security variants are considered, OSF has largely neglected this critical and essential point.

Specifically, OSF/1 is currently offered in 3 security configurations: basic, C2, and B1. By offering these configurations, OSF is able to provide a variety of security features and functionalities to meet end user requirements.

The powerful security features of OSF/1 are oriented toward access control and system auditing, and provide state-of-the-art system administrative controls to ensure the system integrity that is required in today's networked computer environment.

(Unfortunately, this marketing literature misses some key points. For example, when DCE, or MOTIF are added to any OSF/1 configuration, the C2 and B1 security is violated to such an extent that no security claims can be made. In fact, if even simple TCP/IP networking is added, the security of the system is denigrated to such an extent that even fundamental security is no longer guaranteed.)

(Another example is that the addition of Access Control Lists have been deemed essential for both OSF/1 and DCE. Unfortunately, the format of these access control lists, the API to them, and the user interface to them are different for OSF/1 and DCE.)

(It is unrealistic to believe that any reasonable use of OSF/1 will not include either MOTIF or DCE or TCP/IP networking.)

OSF should ensure that at least basic levels of integration are available at the three security levels offered by the base product: Base, C2, and B1. The product managers of each technology area: OSF/1, MOTIF, DCE, DME, and ANDF, should accept it as their responsibility to perform adequate, documentation, quality assurance testing, field testing, and other product related activities to ensure that each technology addresses the three security levels offered by the base product.

Least privilege should also be enforced in an integrated fashion. For example, the privileges should be coordinated so that the privileges required for one technology do not conflict with the security policy of another technology. For example, it should not be necessary to operate as root or superuser on OSF/1 in order to perform simple security tasks for DCE.

2.2. Distributed Security Framework

A picture of modern computing is clearly emerging in which work groups of heterogeneous systems connected via local and wide area networks interoperate with each other. For a variety of procedural, physical, and historical reasons, each of the systems and networks provide varying levels of trust (either implied or explicit).

OSF needs to recognize this in the development of each technology. This has largely been accomplished in the development of the base offerings. The base OSF/1 system (without the security enhancements) interoperates well with products from other vendors. However, in the area of secure offerings, OSF has neglected to keep pace. For example, OSF should ensure that DME is able to manage the DCE security attribites in the current complex networked environment.

The complex networked environment should take into account that not all systems will have the same level of trust associated with them. Some systems will be kept in locked rooms and provide high degrees of physical security while others are left in open cubicles where access is widely available in off hours. Some systems will run DCE while others will not.

Naturally, whether or not a given function is available for a given system, and if so, the level of trust associated with that function will depend on particular attributes of the components of the individual systems involved.

2.3. Variety of Security Features

Given the wide diversity of technology offerings in which OSF is engaged, we recommend that OSF include a wide variety of security features in these products. Though the NCSC has established an excellent vocabulary with the creation of the TCSEC di-graphs, it would be a grave mistake to neglect security features whose origin lies outside the TCSEC framework. As such, it is essential that the OSF products support the security features required by commercial customers. These features may be specified in existing or emerging security documents such as the ITSEC, MSR, Japanese Functionality Requirements or other important documents.

We recommend that OSF survey the complete market and actively seek out security requirements from non-DoD customers. It is our belief that a relatively small, incremental investment in security will result in features for product differentiation that will allow OSF to create and penetrate a burgeoning commercial market.

Examples of candidate technologies abound. As just one example, enhanced authentication protection is readily available to through the use of ‘‘challenge/response’’ type of smart cards.

We recommend that OSF structure the software in such a manner that the security features are individually selectable. This recommendation is based on customer feedback on products that have bundled all security features in such a way that the end user was forced to select all or nothing — similar to the current OSF offering. Under such an architecture, users would be allowed to select the security features they required.

In this manner, users would not be forced to perform auditing just because they wanted tighter password controls. They would not be forced to include ACL's just because they wanted privileges.

2.4. Variety of Security Policies

We also recommend that OSF provide the ability for users to tailor their security policy. In addition, we recommend that OSF ensure that each policy can be used independently of other policies that may or may not be installed. For example, it should be possible to include the MAC policy without necessitating that the DAC policy be in effect.

Perhaps more importantly, we recommend that OSF undertake a customer survey to determine if commercial users prefer other security policies or variations of the existing MAC and DAC policies.

The OSF Security SIG has received significant comments that other policies may be more applicable outside the federal government. Integrity may be far more useful in non-DoD contexts based on our initial feedback. While the DoD places great value on keeping information ‘‘secret’’, commercial customers place far greater emphasis on ensuring that the data (e.g., bank balances, customer invoices) are changed only in accordance with an integrity policy.

2.5. Ease of Use

Computer systems are used by commercial users for a variety of reasons. One of the primary reasons is that it allows organizations to conduct their day-to-day activities in a more efficient and timely manner. The security features on all OSF product offerings must be ‘‘easy to use’’ and not interfere with a user's normal everyday business activities.

Users accessing the system in legitimate ways must not be penalized by the security features of the system. The system should appear to be the same regardless of whether or not security is installed.

Administrators have additional concerns. A security administrator must be offered a straight forward way to map a statement of a security policy to an implementation of that policy, and to ascertain that the mapping is correct. System administrators will need to perform activities like adding new users and resources. Interfaces need to be designed so that these activities can be performed without either compromising the security of the system or inadvertently damaging the system.

As with any product, ‘‘ease of use’’ requires good documentation that is directed to the correct audiences such as end-users, security administrators, and policy makers. OSF must supply such documentation.

2.6. Maintenance of System Attributes

All basic system attributes and general requirements should be maintained whenever the customer enables security features/functionality. The customer should not have to make major tradeoffs between security and other system attributes such as functionality, performance, serviceability, usability, etc.

Very often, in past operating system implementations, security was not considered a required basic system attribute which had to influence the designs and implementations of all the other basic system attributes and requirements. Implementors were ‘‘free’’ to make critical choices while coding the product. This produced a product that forced customers to decide between security or functionality.

When faced with such trade-offs, customers often lack the knowledge to make intelligent decisions because they do not fully understand the effect their choice may have on the overall security of their system.

The OSF strategy should be to make certain its customers are NOT required to make such trade-offs.

2.7. Evaluatable Offerings

A basic requirement for the current OSF/1 system is to be evaluatable under the National Computer Security Center’s Trusted Computer System Evaluation Criteria (TCSEC) at both the C2 and B1 levels of security. As the OSF/1 system is further developed, OSF should ensure that hardware independent portions of the OSF/1 system are, in fact, and remain evaluatable. This implies that OSF must ensure that appropriate security analysis is accomplished for all projects and that the system source, security documentation, system detailed design documentation, and security tests are maintained in an evaluatable state for all releases of OSF/1. This also implies that OSF follow a strict development process (configuration management) to ensure that all changes to the system result in the appropriate changes to the system security deliverables.

OSF should also identify other trusted system evaluation criteria which are applicable to OSF/1. OSF should strive to ensure that the OSF/1 offering is also evaluatable under these criteria, as applicable. For example, OSF should ensure that OSF/1 is evaluatable under the European ITSEC at the F(B2)/E4 and F(B3)/E5 levels. This implies that OSF/1 development process, and the system security design, documentation, implementation, and tests should meet the ITSEC evaluation criteria.

OSF should also identify commercial security evaluation criteria for all OSF offerings. For offerings where applicable evaluation criteria exist, OSF should ensure that those offerings are evaluatable under the criteria at a level consistent with the applicable criteria. Again, this implies that appropriate detailed design, security documentation and security tests are available for all offerings. OSF should also ensure that appropriate development processes are followed for all offerings to ensure that adequate security analysis is accomplished for all projects.

2.8. Exportability

Members require open exportability of all OSF offerings as a prime requirement for successful product sales on an international level. In the past, commercially available, successful, and efficient security technologies have had tight export restriction imposed by governments. A prime example is the United States State Department’s restriction on exporting cryptographic material and operating systems at the B3 level of security and above.

To ensure that members have offerings with effective and exportable security solutions, OSF needs to aggressively take two parallel actions: (1) Provide offerings with existing exportable security technology implemented in a manner which allows for easy upgrading with restricted technologies; and (2) work to change the restrictive export laws on the more effective security technologies.

Recently, cryptography software encryption standards have been proposed by the National Institute of Standards and Technology (NIST). The standards that have been proposed to date provide for data integrity (Secure Hash Standard (SHS)) and for originator authentication (Digital Signature Standard (DSS)). Standards for confidentiality are to be identified in the near future. These and other algorithms do not require approval from the Department of State prior to exporting. Approval for export is through a less encumbered process controlled by the Department of Commerce. These algorithms should be integrated into the OSF offerings in the near-term to provide the security capabilities required by the international market place. Focus should remain on providing exportable B1 level of trust for OSF/1 to provide the access security that will provide some access protection and the cryptographic algorithms and linkage of the cryptographic keys to individuals and processes.

OSF through the influence of the member companies should actively work toward changing the impeding government export regulations to make them more conducive to international business. OSF members will work together with the government to change the export restrictions on these security solutions that promote efficiency and interoperability with existing systems. Changing these export restrictions over the next few years will remove the barriers that currently restrict the open marketing of secure product offerings.

2.9. Security Testing

The addition of new components or changes to existing components within an operating environment whether done to provide new or change existing functions can easily result in the introduction of security flaws into that system. All of OSF's system components should be analyzed and tested for potential security flaws including appropriate penetration analysis. This analysis and testing should be performed for all OSF offerings including those not targeted for formal evaluation.

OSF should require the use of appropriate international security guidelines (including the TCSEC and ITSEC) which are relevant to commercial security requirements. OSF should also develop its own security guidelines tailored to the classes of flaws most likely to be introduced in each of the major components such as the command libraries, the system services, and the kernel.

Suites of test cases should be developed for use in testing for security flaws and interoperability in each of the system components.

A methodology should be developed and made part of the development process which requires the use of the guidelines to perform penetration analysis in the design and coding phases and the test suites in the test phases of the process. To reduce costly redesigns and code rewrites resulting from the discovery of security flaws late in the cycle, the methodology should help ensure that potential flaws are detected and corrected in the early phases of the development process.

3. LONG-TERM PRODUCT IMPLEMENTATION STRATEGY

3.1. Research/Technology Related

Long-term security efforts within OSF should focus on the security implications of new hardware and software on OSF offerings. These efforts should be research oriented and not necessarily related to product specific development efforts.

The OSF security research efforts should leverage other work being done by industry, governments, or the academic community in order to optimize the return on investment.

OSF should ensure that the security research efforts are applicable to future OSF product offerings by defining applicable technology migration path from current offerings to future product offerings.

3.2. Requirements Focused

Long-term security efforts within OSF should focus on expected future commercial market requirements within a 3−5 year period. Care should be taken to avoid addressing only the unique requirements of any particular niche market.

3.3. International Orientation

OSF long-term security efforts should be directed to the international market and not to the unique requirements of any one country or organization.

3.4. Commercial Market Applicability

The objective of long-term security efforts within OSF should be targeted for Commercial Off The Shelf (COTS) product offerings. Care should be taken to stress the ''COMMERCIAL'' aspect of COTS as defined in the industrial and service sectors of the international marketplace.

4. IMPLEMENTATION CONSIDERATIONS

Security services are a mainstay characteristic of all OSF offerings. These services are quickly becoming a ''mandatory'' customer requirement and not a ''desirable''. These same security services are a major interoperability concern when implemented inappropriately and inconsistently on OSF offerings.

It is significantly less expensive to design security services into products from the beginning versus trying to add them on to existing products. For these reasons, the OSF budget for development and research should have at a minimum 15% of the total funding designated to supporting the development and implementation of security services in all offerings. Additionally, this funding should be made a priority item that is specifically identified and justified for each of the project's budget and a mandatory item at all budget reviews.

4.1. Short-Term Strategy

In support of the short-term strategy, OSF funding for security services, approximately 85% should be targeted to the development and implementation of security. These funds will ensure that the security features and capabilities are available and implemented consistently across all OSF product offerings and available through effective and efficient easy to use mechanisms.

4.2. Long-Term Strategy

Of the funding identified for security services, approximately 15% will be focused on achieving the long-term goals of this Global Security Strategy. In addition to these funds, there are frequently opportunities to gain funding from various institutions that sponsor advanced research in the area of communications and computer security. Science and Technology research programs sponsored by agencies such as Defense Advanced Research Project Agency (DARPA). OSF should aggressively pursue these incremental funding opportunities in support of the long-term security strategy. These funds will be in addition to the 15% allocated from the internal funding to ensure the focus of the efforts in support of the long-term OSF security program.

5. EVALUATION STRATEGY

It is a basic development goal that OSF's offerings should meet all applicable criteria for evaluation of trusted systems/products. In addition OSF and its member companies should work to obtain evaluations of the hardware independent portions of OSF offerings under all applicable evaluation criteria.

5.1. Short-Term Strategy

OSF and its member companies should attempt to obtain a C2 and B1 evaluation of the OSF/1 system under the NCSC Trusted Computer System Evaluation Criteria (TCSEC). In addition OSF and its member companies should attempt to obtain an F(B2)/E4 and/or F(B3)/E5 evaluation under the ''harmonized'' European criteria (ITSEC).

As commercial security criteria emerge, OSF should ensure that its offerings are ''evaluatable'' against these commercial criteria at a level of security to meet the requirements of the majority of commercial customers.

For distributed system offerings, DCE and DME, OSF and its member companies should identify applicable trusted product evaluation criteria and actively pursue an evaluation of the offerings under that criteria. The evaluation should be targeted at a level comparable to the TCSEC C2 and B1 levels.

5.2. Long-Term Strategy

As a longer range goal, OSF offerings should provide significantly higher levels of assurance and penetration resistance. As such, evaluation efforts for OSF offerings should be targeted at higher levels of the evaluation criteria.

OSF and its member companies should work to ultimately obtain a B3 evaluation of the hardware independent portions of the OSF/1 system under the TCSEC. Likewise, OSF should work to obtain an F(B3)/E5 evaluation under the ITSEC. As commercial security criteria emerge, OSF should ensure that its offerings are ''evaluatable'' against these commercial critieria a level of security to meet the requirments of the majority of commercial customers.

OSF should provide higher levels of assurance in its distributed system offerings and should work with the member companies to obtain an evaluation of its offerings at a level comparable to the TCSEC B3 criteria.

6. OSF SECURITY STANDARDS STRATEGY

6.1. Short-Term Strategy (Participation)

In the short-term, OSF's role in security standards should be to participate in those security standards efforts that directly impact OSF's current offerings. OSF's goals in participation should be to:

(a) Obtain sufficient technical information to implement the standard in OSF offerings.

(b) Evaluate the progress of the standard to determine when implementation is most appropriate.

(c) To technically influence the standard, if there are significant technical problems in the standard.

OSF should not attempt to actively participate in the drafting of all security-related standards, because OSF lacks sufficient resources to take on such a task. Instead, OSF should coordinate its efforts with member companies to take advantage of their personnel who are involved in the respective standards committees.

In the short-term, the following standards groups are of particular relevance to OSF's security efforts:

(a) POSIX P1003.6 (OSF has been active in this committee.)

(b) X.500 (OSF has not been active in this committee, but it is quite important that OSF become active in the near term, because X.500 is adding security enhancements that are incompatible with much of the security architecture of the rest of DCE. In addition, some of the enhancements seem overly complex and likely to fail ITSEC Ease of Secure Use evaluation.)

(c) TSIG (OSF has not yet been particularly active in this group, but increased activity will be very important if OSF/1 and DCE are to support higher security networking. The particular subgroups of interest are the CIPSO (Commercial IP Security Option), Trusted Sessions, Trusted Admin, and Trusted NFS.)

(d) IETF (The Internet Engineering Task Force is standardizing GSSAPI (a possible DCE 1.1 component) and will be taking technology from TSIG.)

6.2. Long-Term Strategy (Leadership)

In the longer term, OSF has the opportunity to take a leadership role in solving a major problem in security standards — the fact that many of the security standards promulgated so far are mutually incompatible. Each standards committee tends to operate in a vacuum, designing security features that are comparable to security features in other standards, but due to a lack of communications, the features wind up being mutually incompatible. This incompatibility is not just a usability problem, but also represents a potential for security penetration, as the system crackers exploit the incompatibilities. As an example, POSIX, X.500, and ECMA PCTE all define mutually incompatible ACLs. Similarly, PEM, X.400, and X.500 define mutually incompatible security for electronic mail.

Because OSF actually implements the various security standards and must make them work together in DCE, DME, OSF/1, Motif, etc., OSF can provide a unique benefit to the entire computer industry in making sure that all of these security-related standards can actually interoperate in a secure and easy to use manner. OSF should work with NIST, ISO SC27, NSA/NCSC, and DG XIIIF of the European Commission to identify ALL of the security relevant standards and take a leadership role in bringing those standards into a coherent framework.

7. ACKNOWLEDGEMENTS

Charles Blauner and Jim Schindler are the current co-chairs of the Security SIG, and it is in that capacity that they are designated as the ''authors'' of this RFC. In actual fact, however, this document was the joint work of the whole Security SIG (sections were written by different people or groups). Larry Parker (IBM) and Paul Cummings (DEC) were the co-chairs of the SIG when this strategy document was originally produced.

AUTHORS' ADDRESSES

Charles Blauner
Bellcore
444 Hoes Lane
RRC 1J225
Piscataway NJ 08854
USA

Internet email: chazx@ctt.bellcore.com
Telephone: +1-908-699-8395

Jim Schindler
Hewlett-Packard
19091 Pruneridge Avenue
Cupertino CA 95014
USA

Internet email: js@cup.hp.com
Telephone: +1-408-447-4600