National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Symantec ManHunt
Version 2.11

Report Number: CCEVS-VR-03-0052
Dated: November 25, 2003
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team
Paul Olson
National Security Agency
Ft. Meade, MD

Common Criteria Testing Laboratory

Evaluation Team
Computer Sciences Corporation
132 National Business Parkway
Annapolis Junction, MD 20701

Table of Contents

1. Executive Summary

The evaluation of the Symantec ManHunt, Version 2.11 was performed by the CSC CCTL in the United States and was completed on 17 November 2003. The TOE identified in this Validation Report has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version 2.11) for conformance to the EAL 3 requirements of the Common Criteria for IT Security Evaluation (Version 2.1).

This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced.

The information contained in this Validation Report is not an endorsement of the Symantec ManHunt, Version 2.11 by any agency of the US Government and no warranty of the product is either expressed or implied.

The CSC Lab evaluation team concluded that the Common Criteria requirements for a product Evaluation have been met.

The technical information included in this report was obtained from the Symantec ManHunt Evaluation Technical Report (ETR), Dated October 31, 2003, produced by the CSC Lab.

The TOE is a software-only intrusion-detection system running on a dedicated machine platform. The TOE consists of

- Manhunt software acting as a Console
- Manhunt software acting as Master Node
- one or more Manhunt slave nodes

The product also includes the hardware and underlying operating system, the Handoff Coordinator, Open SSH, and a number of SMON-capable network devices, all of which are part of the IT environment and are excluded from the evaluation.

1.1 Evaluation Details

Dates of Evaluation: April 2003 through October 2003
Evaluated Product: Symantec ManHunt, Version 2.11, Dated October 31, 2003
Developer: Symantec Corporation
CCTL: CSC, Annapolis Junction, MD
Validation Team: Paul Olson, National Security Agency, Ft. Meade, MD
TOE Conformance: Part 2 Extended; Part 3 Conformant

1.2 Interpretations

The following interpretations are considered applicable to this evaluation.

#	TITLE
003	Unique identification of configuration items in the configuration list
004	ACM_SCP.*.1C requirements unclear

#	TITLE
006	Virtual machine description
008	Augmented and Conformant overlap
009	Definition of Counter
013	Multiple SOF claims for multiple domains in a single TOE
016	Objective for ADO_DEL
019	Assurance Iterations
024	COTS product in TOE providing security
025	Level of detail required for hardware descriptions
027	Events and actions
031	(Rev. 1) Obvious vulnerabilties
032	Strength of Function Analysis in ASE_TSS
033	CC use of "Check"
037	ACM on Product or TOE?
038	Use of 'as a minimum' in C&P elements
043	Meaning of "clearly stated" in APE/ASE_OBJ.1
049	Threats met by environment
051	(Rev. 1) Use of documentation without C & P elements.
055	Incorrect Component referenced in Part 2 Annexes, FPT_RCV
056	When can the FPT_RCV dependency on FPT_TST be argued away?
058	Confusion over refinement
064	Apparent higher standard for explicitly stated requirements
065	No component to call out security function management
067	Application notes missing
069	Informal Security Policy Model
074	Duplicate informative text for ATE_COV.2-3 and ATE_DPT.1-3
075	Duplicate informative text for different work units
084	Aspects of objectives in TOE and environment
085	SOF Claims additional to the overall claim
095	SCP Dependency in ACM_CAP
098	Limitation of refinement
103	Association Of Access Control Attributes With Subjects And Objects
104	Association of Information Flow Attributes with Subjects and Objects
111	Settable Failure Limits are Permitted
116	Indistinguishable work units for ADO_DEL
102	Sampling of process expectations unclear
127	(Rev. 1) Work unit not at the right place
128	(Rev. 1) Coverage of the Delivery Procedures
133	(Rev. 1) Consistency analysis in AVA_MSU.2
138	Iteration and narrowing of scope
140	Guidance Includes AGD_ADM, AGD_USR, ADO, and ALC_FLR
141	Some Modifications to the Audit Trail Are Authorized
150	A Completely Evaluated ST is not Required when TOE evaluation starts
151	Security Attributes Include Attributes of Information and Resources
201	"Other properties" in specified by assignment
202	Selecting One or More items in a selection operation and using "None" in an assignment
212	Relationship between FPT_PHP and FMT_MOF
222	Meaning and use of "normative" and "informative"?

1.3 Threats to Security

The TOE is a network monitor wholly under the control of the owning organization and operated only by administrative staff. There are no threats directed at the TOE that the TOE counters. It provides security to the monitored network by identifying and reporting activity that may be malicious in nature.

The following identifies threats to the IT System that may be indicative of vulnerabilities in or misuse of IT resources.

TE.MISUSE	Unauthorized network accesses and activity indicative of misuse such as introductions of Trojan horses and viruses may occur on an IT System connected to the network the TOE monitors.

2. Identification

2.1 TOE and TOE Identification

TOE: Symantec ManHunt, Version 2.11.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 2.1, August 1999, ISO/IEC 15408.

CEM Identification – *Common Evaluation Methodology for Information Technology Security*, Part 1: Introduction and General Model, Version 0.6, January 1997; *Common Methodology for Information Technology Security Evaluation*, Part 2: Evaluation Methodology, Version 2.11, August 1999.

2.2 TOE Overview

Symantec Corporation's ManHunt product is an intrusion detection system (IDS) designed to reduce network security risk from network intrusion and Denial of Service (DoS) attacks. ManHunt is a software product deployed on dedicated hardware that resides in the same location as the switches and other network devices that are carrying the traffic to be monitored. The main components of the ManHunt software are the Sensors, Correlation Analysis Framework, Knowledge Base, and Administration Console, or simply Console. All of the components, with the exception of the Console, reside on the ManHunt host. The Console, which is used to configure and monitor ManHunt, can be optionally located remotely on any Java-enabled system with network access to the ManHunt hosts.

ManHunt is a network infrastructure security software product residing on a Solaris 8 platform deployed on dedicated hardware that resides in the same location as the switches and other network devices that are carrying the traffic to be monitored. ManHunt protects the network and systems under its surveillance by monitoring traffic that pass over the network components with ManHunt sensors looking for nonstandard traffic and then analyzes the anomalies to determine if they present a threat to the components in the network. Should the traffic be determined as potentially threatening, the ManHunt analyzer sends alerts to the ManHunt console or performs predetermined actions (e.g., SNMP alert, Allow Handoff, Trackback).

Sensors allow ManHunt to effectively monitor many ports. The sensors use switch port analyzers (SPAN) to listen to network flows that are directly attached to the sensors by copying all of a particular port's incoming or outgoing traffic to another port. This enables sensors to monitor 100% of the traffic on the ports they are monitoring without slowing down the traffic. The Switch/Router Communication Module sets copy ports on switches so that the sensors

can listen to traffic on the appropriate interfaces. When a sensor detects an attack the information is passed on to FlowChaser.

FlowChaser receives network flow data from Cisco routers and ManHunt sensors, and stores the data in an optimized fashion to accelerate the TrackBack process and provide flow information on attacker and victim hosts. FlowChaser also receives data from the Availability Monitor, which monitors user configured hosts on the network and generates an event when any monitored hosts become unresponsive. FlowChaser collects data on current network connections as reported by ManHunt sensors or configured Cisco routers. Flow-Chaser will also recommend QoS (Quality of Service) measures to take if availability of network resources suddenly falls, so that historical traffic flow is preferred over the change. That is, it will suggest access lists that will allow you to discriminate in favor of "normal" traffic over attack traffic.

The ManHunt Smart Agent (MSA) enables ManHunt to accept event data in real time from external sensors, such as ManTrap, as well as from third-party sensors. The MSA event coordinator receives the event data and sends it to the analysis framework for aggregation and correlation with all other ManHunt events. ManHunt MSAs are considered remote trusted IT products.

ManHunt can hand off and receive data about attacks to/from other ManHunt administrative domains to provide trackback information on the source of an attack.

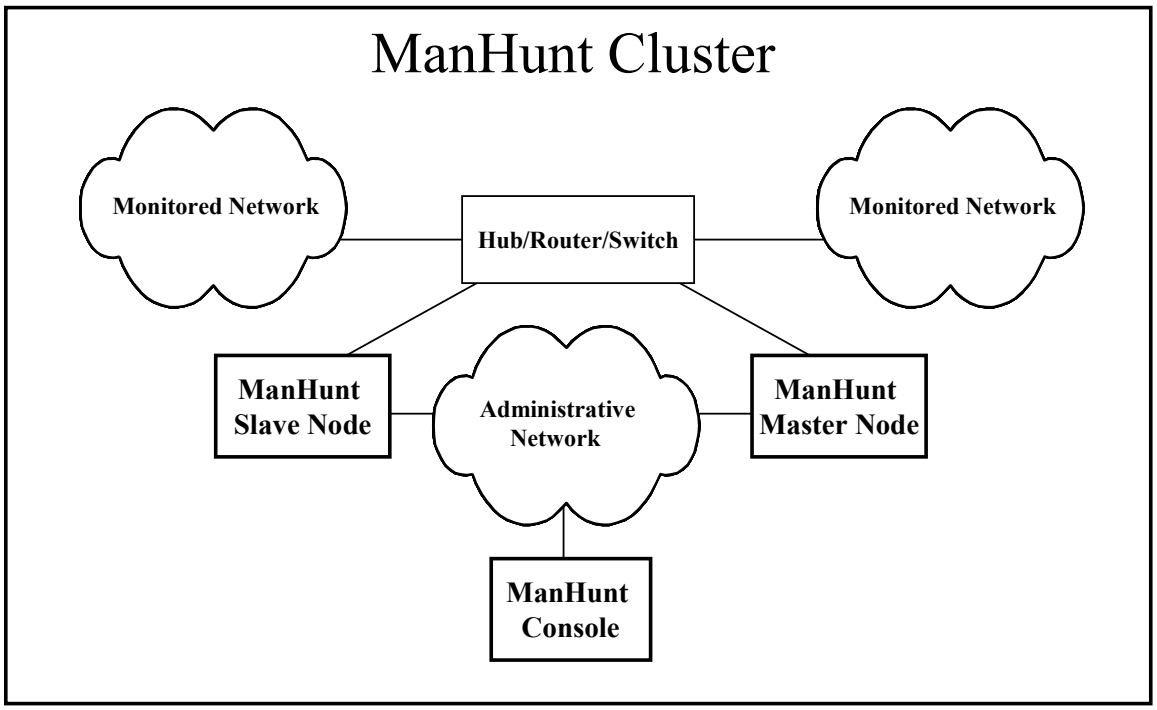
The ManHunt analysis framework aggregates event data on possible attacks from all event sources. The analysis framework also performs statistical correlation analysis on events to identify event patterns that vary significantly from usual network activity and to identify individual events that are highly related, such as a port scan followed closely by an intrusion attempt.

ManHunt uses several databases from which it gathers information about attacks, the network topology, and ManHunt policies, and uses this information, along with data from the sensors, to determine which action(s) to take in response to the attack. For example, it might begin tracking the attack back to its source or hand off the event to another ManHunt. If a policy is set to send an email or SNMP alert, the alerting module does so. The FlowChaser database can be used to quickly determine where an attack is entering the network, and if you supply ManHunt with the appropriate router passwords, the Switch/Router Communication Module can place Access Control Lists (ACLs) on appropriate routers to track flows back to their source.

The QSP proxy is a proprietary protocol that enables secure, encrypted communication between the master node and the administration console, and between ManHunt nodes within the same cluster. From the administration console, the ManHunt system administrator can perform tasks, such as configuring the system, editing the topology and policy databases, monitoring attack incidents in progress, and generating reports. Changes to the configuration, topology or policy databases can be made to a master ManHunt node that will subsequently push the updates to the other ManHunt nodes in the cluster.

The reporting module can automatically generate and send daily email reports on the most frequently occurring event types for the day. For a greater level of detail, the reporting module can also generate graphical reports on demand from the administration console. These reports provide detailed data on the types of events and incidents that occurred and protocols exploited during the specified time period.

> Within a network, multiple ManHunt nodes can work together as a ManHunt cluster and share event data. A ManHunt cluster can comprise up to 100 ManHunt nodes across multiple network segments within multiple network locations. Each cluster will have a master node (and possibly a backup master node) and slave nodes
>
> The evaluated TOE consists of the ManHunt Version 2.11 Software configured on the Solaris 8 platform residing on the following dedicated hardware as part of a distributed high-speed switched network with access to the Internet.



2.3 IT Security Environment

3. Assumptions

The Operational Assumptions defined for the TOE:

A.AUTHORIZED	Only authorized TOE *Users* and *Console Administrators* will have accounts on those platforms on which the TOE executes.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. (The processing resources of the TOE include the Sensors and monitored IT product, the MSA and monitored IT product, the ManHunt Node(s), and ManHunt Console)
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

A.PFORM_SPT	The TOE environment must provide reliable platform functions including: correct hardware operation and functionality including providing system time; correct platform software operation and functionality.
A.ACC_CONTR	The operating systems upon which the Console and Node runs will be configured to restrict modification to TOE executables and configuration files to only the *Console Administrator*.
A.NOEVIL	Authorized *Use*rs and *Console Administrators* are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4. Policies

The operational security policies defined for the TOE:

P.ANALYZ	Analytical processes and information to derive conclusions about intrusions (past, present, or future) must be applied to IDS data and response actions taken as prescribed by local site policy.
P.INTGTY	Data collected and produced by the TOE shall be protected from modification.
P.ADMIN	Management functions of the TOE shall be restricted to the Authorized Administrator(s).
P.ACCACT	Human users of the TOE shall be accountable for their actions.
P.MONITOR	The network will be monitored and reports on network activities will be made in accordance with local site policy.

5. Architectural Information

5.1 Monitoring of IT resources

Sensors take information from each of the monitored switches and classify events as either legitimate or "suspicious (anomalous)". Suspicious (anomalous) events are passed up to the Analysis Framework, where related events are grouped as incidents and evaluated "in context" to determine their severity.

FlowChaser receives network flow data from Cisco routers and ManHunt sensors, and stores the data in an optimized fashion to accelerate the TrackBack process and provide flow information on attacker and victim hosts. FlowChaser also receives data from the Availability Monitor, which monitors user configured hosts on the network and generates an event when any monitored hosts become unresponsive. FlowChaser collects data on current

network connections as reported by ManHunt sensors or configured Cisco routers. Flow-Chaser will also recommend QoS (Quality of Service) measures to take if availability of network resources suddenly falls, so that historical traffic flow is preferred over the change. That is, it will suggest access lists that will allow you to discriminate in favor of "normal" traffic over attack traffic.

The ManHunt Smart Agent (MSA) enables ManHunt to accept event data in real time from external sensors, such as ManTrap, as well as from third-party sensors. The MSA event coordinator receives the event data and sends it to the analysis framework for aggregation and correlation with all other ManHunt events. ManHunt MSAs are considered remote trusted IT products.

5.2 Analysis of Events

ManHunt is designed with an analysis layer, Analysis Framework, operating above the sensors, which adds additional information to the raw sensor data and presents a more complete picture of security-related activities on the network.

ManHunt responds to intrusion detection in a number of ways from simple notification of the administrator to providing automated responses to protect systems. ManHunt classifies IDS attacks into two categories: Intrusion Attempts and Denial of Service (DoS) Attacks. An intrusion attempt is a much simpler attack to deal with because once it has been identified the connection can be terminated. A DoS attack does not require a connection to be made and the attack consists of very large volumes of data. ManHunt has a variety of administrator configurable automated responses and multiple responses may be configured for one incident.

ManHunt uses a separate interface for notification that can be located on an administrative network to increase the likelihood the notification can be sent successfully by lessening the chance of deliberate compromise. While session termination is a response option for ManHunt to stop an attack, nothing is learned of the attacker. When possible, ManHunt employs other response options. ManHunt's Trackback function is designed to automatically track a data stream to the entry point into the administered network.

The TrackBack function is designed to automatically track a data stream to its source within the cluster, or, if the source is outside the cluster, to its entry point into the cluster. The Trackback process can continue beyond the administrative domain through communication with an upstream peer network. ManHunt is designed to both send and receive tracking information across administrative boundaries if policies have been configured to do so. ManHunt hosts may register with each other when communication between them is desired and ManHunt will only respond to a message from a registered and authenticated ManHunt.

5.3 Administration and TOE Self-Protection

ManHunt recognizes two types of administrative roles: *Console Administrator* (available from Administration Console) and *User* (also available from Administration Console). The *Console Administrator* can make changes to the topology tree, response policies, and configuration parameters, mark incidents and add incident annotations from the administrative console. The *User*'s privileges are limited to viewing incident data, marking incidents and adding incident annotations.

ManHunt uses QSP proxy, a proprietary protocol that enables secure, encrypted communication between the ManHunt master node and the Administration Console, and between ManHunt nodes within the same cluster.

From the Administration Console, the ManHunt *Console Administrator* can perform tasks, such as configuring the system, editing the topology and policy databases, monitoring attack incidents in progress, and generating reports.

Changes to the configuration, topology, or policy databases can be made to the ManHunt master node, which will subsequently push the updates to the other ManHunt nodes in the cluster

6. Documentation

Symantec ManHunt Evaluation Technical Report, Version 2.11,
Symantec ManHunt Security Target Version 1.24
Symantec ManHunt v2.11 Security Target, Revision 1.24
Recourse Product Version Numbering System, 5/12/02
Recourse Release Engineering Security, 5/12/02
Recourse Engineering Network Security, 5/12/02
Recourse Technologies ManHunt 2.11 Common Criteria Evaluation EAL2 Evidence of ALC_DVS.1 Compliance, 10/03/02
Recourse Technologies ManHunt 2.11 Common Criteria Evaluation EAL2 Evidence of ALC_DVS.1 Compliance, 4/17/2003
Recourse Technologies ManHunt 2.11 Common Criteria Evaluation EAL2 Evidence of ALC_DVS.1 compliance, 12/3/2002
Recourse Technologies Corporate Policy #SEC-1002, Configuration Management Plan
Recourse Technologies Coding Standards
Symantec Corporation, RWC Software Configuration Management Plan
Recourse Technologies Corporate Policy # SEC-1001
Screen Capture of CM System
Screen Capture of CM System
Screen Capture of CM System
Eng_design_doc_listing.txt (open in wordpad for better view)-CI list output from CVS
Recourse Technologies product Security Supplement-Delivery, Installation, and Configuration Procedures.
Fulfillment SOP, last updated: 4/10/02.
ManHunt v.2.11 Installation Guide
ManHunt Design Document Rev 1.2.4
ManHunt Design Documentation Addendum
Recourse ManHunt v.2.11, Administrative Guide
ManHunt v.2.11 User guide
[Separations] Symantec Employee Separation Procedures
ManHunt Functional Test Specification: Re-evaluated with version dated 9/22/2003 2.11
ManHunt Test Coverage and Depth Analysis, Last Updated September 11, 2003
ManHunt Strength of Function Analysis Version 1.0 updated 9/4/2003
ManHunt Version 2.11 Vulnerability Analysis Revision 1.0, dated 9/15/2003
CSC Common Criteria Testing Laboratory Penetration Testing Plan and Report: Symantec ManHunt Intrusion Detection System Version 2.11
CSC Common Criteria Testing Laboratory Site Visit Report: Symantec ManHunt Version 2.11 EAL3 Evaluation

7. Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the EAL 3 section of the CC and the CEM.

The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of the EAL 3 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes in the draft ETR sections for an evaluation activity (e.g., ASE) that recorded the Evaluation Team's evaluation results which the Team provided to the developer. The Evaluation Team also communicated with the developer by telephone, electronic mail, and meetings. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. No constraints or assumptions were identified in performing this evaluation.

Chapter 5, Conclusions, in the Evaluation Team's ETR, states:

> The evaluation team assigns an overall pass verdict for satisfying the evaluation team action elements defined for EAL 3.

8. Validation Comments/Recommendations

As a clarification, the validator notes that the encryption program used on inter-node traffic is not evaluated. It is for the customer to determine whether is it strong enough for their uses.

The validation team recommends the U. S. Government Symantec ManHunt, Version 2.11 receive an EAL 3 Certificate.

7. Abbreviations

Abbreviations	Long Form
ASE	Advanced Encryption Standard
ATM	Asynchronous Transfer Method
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme
CEM	Common Evaluation Methodology
CM	Configuration Management
DoD	Department of Defense
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IP	Internet Protocol
IPSEC ESP	Internet Protocol Security Encapsulating Security Payload
IT	Information Technology
I&A	Identification and Authentication
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	Network Time Protocol
OR	Observation Report
PC	Personal Computer
PKI	Public Key Infrastructure
TOE	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SOF	Strength of Function
ST	Security Target
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSE	TOE Security Environment
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy
TSS	TOE Summary Specification
VPN	Virtual Private Network

8. Bibliography

The evaluation and validation methodology was drawn from the following:

[CC_PART1] Common Criteria for Information Technology Security Evaluation-Part 1: Introduction and general model, dated August 1999, version 2.1.

[CC_PART2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, dated August 1999, version 2.1.

[CC_PART2A] Common Criteria for Information Technology Security Evaluation Part 2: Annexes, dated August 1999, version 2.1.

[CC_PART3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, dated August 1999, version 2.1.

[CEM_PART 1] Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model, dated 1 November 1997, version 0.6.

[CEM_PART2] Common Evaluation Methodology for Information Technology Security – Part 2: Evaluation Methodology, dated August 1999, Version 2.11.

[CCEVS_PUB1] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Organization, Management and Concept of Operations, Scheme Publication #1, Version 2.0 May 1999.

[CCEVS_PUB2] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Validation Body Standard Operating Procedures, Scheme Publication #2, Version 1.5, May 2000.

[CCEVS_PUB3] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Technical Oversight and Validation Procedures, Scheme Publication #3, Version 0.5, February 2001

[CCEVS_PUB 4] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to CCEVS ATOEroved Common Criteria Testing Laboratories, Scheme

Publication #4, Version 1, March 20, 2001

[CCEVS_PUB 5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, Guidance to Sponsors of IT Security Evaluations, Scheme Publication #5, Version 2.11, August 2000.