WHITE PAPER

Unisys ClearPath MCP

Independent Security Assessment

McAfee™

Contents

Unisys ClearPath MCP

Independent Security Assessment

Unisys coordinated with Advanced Cyber Threat Services (ACTS) —part of the McAfee® Professional Services offering—on a multiphase independent product security assessment of the Unisys ClearPath MCP operating system. The scope of this project focused on the ClearPath MCP core security. The engagement consisted of operating system evaluation, default security configuration assessment, and a threat modeling exercise. McAfee ACTS consultants conducted reviews and attempted exploitation during each phase of the assessment.

This document provides a detailed security review of the MCP operating system. The McAfee ACTS group recognizes that the MCP product line was designed for a high level of security, and the core operating system was designed following best practices for authorization, resource management, and reliability.

MCP Overview

The Unisys MCP operating system is a general-purpose operating system designed to provide a robust and secure platform for a wide variety of customer-specific requirements. Consequently, security requirements for an MCP system deployment are highly specific to each customer application and security requirements.

The MCP core operating system provides, manages, and monitors resources including memory, processor, and file access. These resources are allocated to user and system processes based on permission and priority to facilitate a multifunctional operating environment. Monitored resource usage is stored in a central log for system analysis by Administrators, and MCP supports multiple user roles and permissions. User accounts may be assigned levels of access based on requirements on the host. In addition to the security built into the MCP platform, Unisys provides and maintains extensive documentation on security features, and PCI best practice guide for secure deployment of the solution and the various components therein.

Testing Methodology and Findings

McAfee ACTS consultants utilized multiple testing methodologies that focused on a specific component of the architecture. Testing was conducted against MCP version 19.0, with an emphasis on manual testing using McAfee ACTS proprietary testing methodologies and industry experience testing non-commodity platforms.

Operating System Assessment

Multiple interviews were conducted with developers and engineers, as well as a review of the MCP default configuration, update methods, and a review of MCP core operating architecture and system services. This top-down approach used in assessing MCP included a review of default settings, user interaction, and the running environment. Strong emphasis was placed on testing the allocation of operating system resources such as disk space, memory, and processor cycles. These resources were vetted for vulnerability to direct or indirect attacks which would allow an attacker to gain unauthorized access to the system, escalate privileges, or deny service. This involved an extensive review of system architecture as well as creating custom software for testing the host system. Application and configurations not integrated into to the core operating system were outside the scope of this assessment. These included, but were not limited to, the following: network services, compilers, file editors, databases, and third-party applications.

Threat Modeling

The threat-modeling process began with a high-level architecture discussion with the MCP solution architects in order to understand the overall platform's

functionality, security requirements, and deployment environment. McAfee ACTS consultants then worked with the development team to understand the implementation of the requirements within the live environment. From these initial meetings and a thorough review of the documentation provided by Unisys, McAfee ACTS consultants derived a list of credible threats to the various components which make up the solution. This process exposed the key components that are likely to be the target of an attack, including storage locations for sensitive information, configuration files, data flows, and other significant features that may pose a threat to the security of the platform. The threat model also resulted in a list of potential threat vectors and existing countermeasures.

Areas of Analysis

McAfee Advanced Cyber Threat Services consultants focused on multiple areas for the purposes of analyzing the security of the overall solution. The table below breaks these focus areas down into high-level topics and provides guidance and recommendations based on McAfee Advanced Cyber Threat Services consultants' observations during this engagement.

Analysis Topic	Best Practice	Evaluation	Recommendation
Memory Management	Resources must be constantly monitored for ownership, authorization, and availability. Resources assigned to one process should not be available to another process unless explicitly required.	The MCP architecture defines a memory abstraction layer for memory access. This layer creates a separation between user-directed requests for memory access and the actual action performed upon system memory. By establishing protocols, rules, and restrictions that must be followed by user-level execution, the system software can ensure safe behavior. Multiple facets of the MCP operating system create interwoven security controls in prevention of malicious exploitation of memory. MCP implements a safe memory program execution environment, which prevents intentional or unintentional memory corruptions. All programs are written in high-level languages in which access to data segments are automatically bounds-checked through various restrictions built into the core MCP operating system. Programmers work with memory descriptors, or references, and never use direct memory pointers, as in commodity architectures. This creates a layer of abstraction between the program memory reference and the actual memory address. Memory segments are tagged with metadata by the operating system to describe their intended purpose—for example, stack, data, or code segment. This prevents the execution of data or stack segments as code. Commodity operating systems do not store similar metadata as a part of the memory object, allowing for exploits like buffer overflows. All data received by the system from the network is automatically stored in memory and tagged as a data segment, meaning it cannot be executed. These controls mitigate stack memory attack methods for known vulnerabilities in common network protocols. McAfee ACTS consultants reviewed memory scrubbing implemented in MCP. Before memory is allocated to a new process, the memory is scrubbed by setting all bits to zero. This prevents memory from a previous process from being accessed by a new process. The memory of a running process can optionally be scrubbed upon deallocation of memory when a process ends execution.	The memory management either meets or exceeds industry best practice.

		In addition, memory allocated for SENSITIVEMEMORY objects in a running ALGOL program can also be assigned attributes requiring the operating system to scrub the memory upon deallocation of that object. This allows for the memory to be scrubbed while the process is running each time the object is deallocated.	
Logging and Auditing	Extensive monitoring of the host operating system and applications allows administrators insight into operations which may not be visible to the user. The operating system should be capable of presenting administrators with a log of system activities. Administrators should review logs at regular intervals for security violations and anonymous activity.	MCP provides an auditing and logging subsystem as part of the operating system. There are two primary logs managed by MCP. The SYSTEM/SUMLOG file contains log records for a variety of system-related events as well as security events such as login success/failure events, access control violations, network access violations, attempted resource misuse, and other security related events. The SYSTEM/SECURITYLOG logs security-sensitive information from SSL, IPSec, and SSH that are relevant for diagnostics. Each event is tagged with four (4) result attributes. In addition to the SUCCESS or FAILURE of an event, MCP also assigns the attributes RELEVANT and VIOLATION. The later attributes indicate that an event was security related. A log analyzer tool provides system security administrators the ability to view and filter the SUMLOG to readily identify security related events for detection and forensic purposes. An important function of logging is not merely for historic record, but also for risk mitigation. The logging generated in MCP can be real time exported using Unisys RealTime Monitor. This additional utility can export logs into syslog format to feed into real time monitoring software, such as a SIEM.	No recommendations are necessary for this topic. The system either meets or exceeds industry best practice.
Resource Availability	The core functionality of any operating system is the management of resources. In order for an operating system to function reliably and securely, it must be capable of allocating the appropriate resources for each process. The operating system should attempt to prevent any open process from adversely affecting other processes from resource starvation.	Processes running on MCP use a shared pool of resources. Each MCP installation provides a finite amount of resources which are shared among all running processes. Additional resources can be manually assigned by an Administrator. McAfee ACTS consultants created a custom application to attempt allocation of all available processor cycles, memory, and disk space on an MCP system. An unprivileged user account was used to execute the resource allocation process. Upon execution, other processes were blocked from allocating processing time, disk I/O, and memory. Consultants discovered that as other processes deallocated resources, the custom application would expand and allocate those resources. Processes (including the core MCP) were able to maintain resources allocated prior to the execution of the malicious process. This allowed most core MCP processes to remain running, despite all visible resources being consumed. The MCP core operating system maintains uptime during resource starvation. However, processes requiring additional	McAfee ACTS consultants recommend implementing functionality that limits the resource allocation for a single process by default. This must restrict the default processing, memory, and disk write capabilities of each process.

		or initial resources were unable to continue to function properly. MCP supports manual restrictions on resource allocation, and prioritization of processes. MCP allows processes with a higher priority to receive more frequent processing cycles. A process can be executed with a cap on memory available for that process. If the process attempts to allocate memory beyond the cap the process execution is terminated. Disk allocation can be restricted for user accounts in specific contexts. This method would still allow a process to consume all available disk space accessible to the user. If disk space is full, additional disks can be dynamically added.	
Default Security Configuration	Apply stringent resource restrictions based on user access requirements. Vendors should encourage secure installations of products. Optional security settings should be configured in the default secure state.	MCP supports a wide variety of security configuration options. These options allow administrators to configure a system to comply with standard security best practices, and context specific security policies in an organization. MCP provides several built-in security profiles in the form of CLASS values S0-S2. Each profile creates a more stringent environment than the previous profile on dozens of security settings. The modification of security configuration has the potential to cause interruption for running MCP environments. It is the practice of Unisys not to force changes on the operating system that could cause disruption or configuration conflict. A best practice security implementation may not be enabled by default, in the interest of system usability. A robust security support library allows Unisys customers to customize authentication controls to meet their specific requirements. New risks are discovered in common network protocols and services every year. These risks influence ever evolving industry best practices. In response, Unisys deprecates legacy protocols and cryptographic algorithms as defaults on the MCP host. Unisys continues to support legacy protocols in MCP for environments which are unable to migrate to newer standards. For example, this means deprecation of default support for known high risk SSL encryption such as RC4 and DES. Unisys provides MCP with default hardened configuration of supported network protocols. Additional recommended settings are provided in the MCP Best Practice Guide for customization of network services.	McAfee ACTS recommends the development of a standalone Security Technical Implementation Guide (STIG) for the MCP operating system. MCP servers subject to PCI regulations can be configured following the Unisys "MCP Security Payment Card Industry (PCI) Data Security Standard Guidelines." MCP servers subject to additional standards can reference the "MCP Security Overview" for configuration options.
Threat Modeling	Threat modeling is a structured approach for identifying, evaluating, and mitigating risks to system security. The view for threat modeling varies greatly depending on the environment. However, general best practices can be applied to most technologies. These include resource allocation, user authentication, authorization based on roles, secure coding practices, and update management.	McAfee ACTS interacted with key personnel at Unisys, including members of the development team and security department. The team conducted workshops to understand the current architecture and design, and then considered all the threats, countermeasures, and potential vulnerabilities that might exist in the system.	No recommendations are necessary for this topic. The system either meets or exceeds industry best practice.

Account Security	User accounts should be assigned permission based on the principle of "least privilege." This principle dictates that permission be provided for accessing resources only when required. Resources should be restricted to a single owner by default and require manual modification for additional user access privileges. Administrator accounts should be provided only to users with the authority to perform systemwide modifications. Mechanisms should be enforced that prevent user accounts from being used by an unauthorized party. The account username and password combination should be complex enough to thwart attempts at recovery.	All access points into the MCP system are designed to require authentication; there are no entry points where a user can gain unauthenticated access. The MCP operating system recognizes multiple usercode privileges. The privileges include the default privilege (an unprivileged usercode), PU (Privileged User) and SECADMIN (Security Administrator). PU and SECADMIN are commonly assigned to MCP Administrators. User accounts may access Public files and those in their account directory. PU accounts may access Private and user files. PU accounts also have permissions to modify most system settings. SECADMIN accounts have full access to system resources. In addition to the permissions of the Administrator, the SECADMIN privileged account can modify security specific resources and settings. These account types allow administrators to assign accounts with appropriate permissions. These accounts were granted appropriate permissions by default. Additional permissions could be permitted as required. McAfee ACTS consultants observed that the MCP system did not record usernames as case sensitive. All lowercase alphabetical characters were converted to upper case prior to being interpreted and stored by MCP. This method of username string storage greatly decreases the key space for user accounts and might assist an attacker when attempting to brute-force potential usernames to gain access to the system. Default password policies on MCP did not meet recommended standards, and most password policies were either set to the minimum or disabled entirely. The following policies were observed: ▪ Enforce Password History = 0 ▪ Minimum Password Age = 0 ▪ Minimum Password Length = 0 ▪ Password Must Meet Complexity Requirements =Disabled ▪ Account Lockout Duration = 0 minutes ▪ Account Lockout Threshold = 0 ▪ Password Case Sensitive = Disabled MCP was designed to provide a variety of mechanisms for authenticating end users, including usercode (username) and password, Kerberos, NTLMv2, smart cards, and more. A malicious privileged user or attacker who gains access to the MCP USERDATAFILE may be able compromise user passwords using brute-force techniques against weak password hashes.. Access to the USERDATA files is restricted to usercodes assigned administrator level privileges and is not accessible with a standard account. The passwords are for the usercodes are stored in a salted SHA-256 format.	McAfee ACTS consultants recommend requiring that the configuration for new MCP deployments enforce case sensitivity for system usernames, and that a process/update is implemented to enforce the same requirement on existing MCP deployments. MCP provides built in functionality to perform the following: ▪ Password Case Sensitive = Enabled Unisys provides an optional security library to its clients, which can be configured to enforce best practices. The existing FAQ article 4257 provides details on configuration option for the security library from the Security Software Development Kit. The security library is capable of providing more complex password policies: ▪ Enforce Password History = 24 ▪ Minimum Password Age >= 1 ▪ Minimum Password Length >=12 for regular users, >=14 for administrators ▪ Password Must Meet Complexity Requirements = Enabled ▪ Account Lockout Duration >= 30 minutes ▪ Account Lockout Threshold <=3 In the default implementation, AdMiniStRatOr would convert to ADMINISTRATOR when assigned as the username. User names can be case sensitive if placed in double quotes. For example, "AdMiniStRatOr" would maintain the upper and lower case characters. Unisys should store all usernames in quotation to allow case sensitive usernames.

		MCP supports multi-factor authentication for user login. Authentication to terminal can be configured to require a unique PIN in addition to the account password. This unique PIN is sent to the user each time authentication occurs as a One Time Password (OTP). This multi-factor authentication can be assigned on a per user account basis.	
File Access	Files must be evaluated for ownership and permissions prior to access. Files assigned ownership to one process or user should not be accessible to another process or user unless explicitly configured. Access to resources should be permitted based on read, write, and/or execute.	Access restrictions are enforced on all files within the MCP environment. Access permissions on files can be configured to Private and Public as well as read and write. These settings are stored in the header for each file. A Public file can be accessed by all users, while a Private file is restricted to Administrators and system processes. MCP is designed with access control capabilities that extend the POSIX ACL model for discretionary access control with a more finely-grained access control mechanism known as GUARDFILEs. This provides a flexible means for users and system administrators to control which users and programs can access their data files, programs, and databases. Access is based on a variety of criteria, allowing for the creation of an access control model to meet a wide variety of customer requirements. Processes are not permitted to view files without permission. Additional permissions can be assigned custom for specific users, groups, and processes. File permissions are verified at resource access time. The modified permissions do not affect access in conditions when resources are currently loaded by a process. McAfee ACTS consultants leveraged a standard user account to execute a process that opened a Public file for reading and writing. While the user's process maintained access to the file, an Administrator account changed the privilege to take ownership of the file and set it to Private. This permission setting allowed only the Administrator to access the files. After the file had been changed to Private, the running user process was able to write to the Private file. After process termination, additional attempts to access the Private file were denied to the user. Mounting network storage hosted from MCP requires authentication from MCP operating system accounts. This is performed using the SMB protocol. The files displayed on the network drive are only those accessible to the account used to access the drive. No files belonging to other accounts or operating system files would be shown on the attached disk.	Evaluate open access to resources prior to confirming changes to permission in order to avoid unauthorized access after permission changes take effect.

		MCP supports archiving one of more files in a "container" file. Containers can be manually created by a user or automatically when exporting files from an MCP host. By default, these container files are not encoded like other zip, rar, and tar archive formats. However, MCP does support encoding, encrypting, and signing features when creating container files. This allows container files on an MCP host to store encrypted files as well as exporting encrypted files for storage outside of MCP.	
Development Environment Security	Access should be restricted to system development software to authenticated user accounts. Development tools that can bypass system access restrictions should be explicitly allowed only when required. Administrators should be made aware of the potential risks.	MCP provides a robust development environment to allow consumers to develop custom applications. Software supported by MCP is predominantly written in ALGOL 68, COBOL 74, or NEWP (a derivative of ALGOL designed for operating system by Unisys). McAfee ACTS consultants observed that the NEWP compiler was provided by default on larger MCP installations. These compliers are provided by Unisys, but not installed by default; making it possible to install the complier on a "development" MCP host and not a "production" MCP host. The NEWP language supports low-level operating system program development. The ability in NEWP for Administrators to execute "unsafe intrinsics"—built-in operating system functions for low-level access (for example, raw memory access)—was allowed in NEWP. Compiling and executing NEWP software requires an authorized user account. McAfee ACTS consultants observed that the debug analysis tool (included in the default installation) allowed Administrators unlimited visibility into the running system via the live-analysis mode—including the MCP internals and raw memory. Consultants observed it demonstrated by an MCP systems developer as it was used in a typical development environment.	McAfee ACTS recommends restricting access to the NEWP compiler and/or its ability to use unsafe intrinsics (for example, functions that allow raw memory access and low-level system manipulation) for default installations. Consider leveraging existing security implementations to restrict access, as they are already mature production code and included in the design. For example, the file header for the NEWP compiler and any code it generates could contain a flag only accessible and visible to the MCP core system to determine if access is allowed.
Update Management	All software update packages should be provided in a trusted manner. Packages should be transported encrypted over the network from the update server to host(s). All software updates should be verifiable for authenticity and integrity by the host.	MCP files produced by Unisys are the primary software used by the MCP operating system host. McAfee ACTS consultants were provided with two update package container files. The updates were contained in a CON file. The container files may include sourcecode, configuration files, sourcefiles, sample files, libraries, etc. The update files were examined for a better understanding of the software as part of how the system operates. Files are not encrypted and could be read on disk. Files not sent securely could be captured in transit. McAfee ACTS consultants were able to extract and view contents of update packages, as no encryption was implemented. Modifications to the container file wrapper were successfully accepted by MCP using the standard installation method.	While it is not currently a common practice for MCP administrators to install third-party software, McAfee ACTS consultants recommend that the MCP update service perform a check on all containers before installation of any new updates. All update files must be signed by a recognized trusted source and verifiable by the MCP. The updates must then be verified by the MCP to prevent installation in the event of file tampering. Encrypt the package files to mitigate the risk of their contents being read while residing on disk or in transit. Implement a method whereby decryption of packages residing on disk can only be performed by authorized developers and the software that the package updates.

	Modifications to the headers and the files were identified by the MCP using checksums contained in the wrapper.

Conclusion

Unisys ClearPath MCP is designed to provide a secure environment for program execution, which protects against attempts to inject and execute malicious code. MCP access control capabilities extend the POSIX ACL model for discretionary access control to allow users and administrators a more granular means to control which users and processes can access data files, programs, and databases. ClearPath MCP provides a robust auditing and logging mechanism integrated into the operating system. Extensive logging includes a large number of events that are logged as being either security relevant, or security violations, enabling the rapid discovery and forensics of potential attacks. MCP provides a truly integrated technology stack in which all system components, including resource allocation, system monitoring, and account management have all been designed, implemented, and tested to work in unison securely. As with any software platform, administrators and users can greatly affect the overall security. The MCP environment offers a wide variety of security configuration capabilities. Unisys continues to monitor industry trends on risk and best practices in order to provide secure network protocols and services.

MCP provides the capability for consumers to configure a highly secure operating system environment. The MCP developers prioritized the security by design starting over fifty (50) years ago and this practice continues today Security principles such as “deny by default” and “least privilege” have been incorporated into the foundation of MCP from its origins. Administrators can leverage the extensive MCP documentation on configuration options to customize an environment which meets a variety of security best practice standards.

Every version of MCP implement new features. This often includes changes to the MCP core operating system as well as additional user configuration options. The review conducted for this whitepaper was MCP version 19.0. Significant differences between current and legacy MCP versions can found in the version documentation on https://public.support.unisys.com.

Security Resources

In addition to the default MCP installation, multiple software packages can be leveraged for improved security.

- The Security SDK is provided as development tools for creating security features including:
  - Password complexity policies
- Operating Environment Encryption Option package which includes:
  - CRYPTOGRAPHY
  - Encrypted Network Protocols (TLS, SSH, etc.)
  - WRAPENCRYPTED

Reference Material

- “MCP Security Overview and Implementation Guide” (8205 7498-001)
- “MCP Security Payment Card Industry (PCI) Data Security Standard Guidelines” (3850 7315–009) (part of Imp Guide)
- “Security Operations Guide” (8600 0528–210)
- “System Configuration Guide” (8600 0445–310)

Version

- The original testing began in June 2015 with a retest conducted in October 2015 on MCP version 16.0.
- An evaluation of was conducted in October 2020 on MCP version 19.0.

About McAfee Professional Services

McAfee Professional Services delivers strategic guidance and expert assistance to help customers elevate their security programs, maximizing the return on their security investments.

Advanced Cyber Threat Services

Advanced Cyber Threat Services (formerly Foundstone) offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Advanced Cyber Threat Services consultants identify and implement the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

Disclaimer: This document is provided on an "as is" basis and does not imply any kind of guarantee or warranty, including the warranties of merchantability or fitness for a particular use. Your use of the information in the document or any materials linked from this document is at your own risk.