

MUSIC Certification

Certification Level:
MUSIC 2007-1 Foundation Level
Certification Process Version:
MUSIC 2001-1 Foundation

Device Certified:
Honeywell Experion® Process
Knowledge System (PKS) C300
Process Controller
Software Release 3.0

Certification Date:
01-Oct-2007

Certificate Identifier:
MUSIC-Foundation-Aug07-1

Certification Tests Conducted By:
Mu Dynamics, Inc.

Certifying Entity:
Mu Dynamics, Inc.

Executive Summary

MUSIC is the certification program for Industrial Control offered by Mu Dynamics, Inc. The program is based on a regimen of vendor testing with independent verification and certification. The Foundation-level certification requires the use of the Mu-4000 analyzer to test the supported protocols from the following list: ARP, DHCP, ICMPv4, IEEE 802.1p/Q, IPv4, TCP, TFTP and UDP. The Tofino Security Appliance was tested at Byers Security Inc.'s facilities in British Columbia, Canada with the independent verification being provided by Mu Dynamics.

The Honeywell Experion® Process Knowledge System (PKS) C300 Process Controller was tested using a Mu-4000 for security and robustness issues using the complete suite of Foundation-level protocols supported by the C300. No faults were detected during the running of the analysis. The C300 controller was tested both with and without a firewall and no faults were detected in either case. The firewall used in the testing was the Honeywell Control Firewall.

The analyses were run using the attacks available for each protocol on the Mu-4000 analyzer. Mu Dynamics carried out the certification testing at the Honeywell facility.

Analysis Details

- **Device tested:** Honeywell Experion® Process Knowledge System (PKS) C300 Process Controller, Software Release 310
- **Test location:** Honeywell facility, Ft. Washington, PA
- **Analysis completion date:** 27th July 2007
- **Tests conducted by:** Mu Dynamics, Inc.
- **Tests verified by:** Mu Dynamics, Inc.
- **Certification specification:** MUSIC-Foundation 2007-1
- **Filters used in Mu-4000 Attack Vector Set:** None. All attack vectors were run during the testing.
- **Mu-4000 Analysis Mode:** Mutation Analysis (Endpoint-mode)
- **Testbed Description:** Two sets of tests were carried out. In the first set of tests, the Mu-4000 analyzer was directly connected to the C300 Process Controller using a Gigabit Ethernet connection. All attacks were transported using IP version 4. No authentication mechanisms were used in the testing of any of the above protocols. In the second set of tests, the Honeywell Control Firewall was placed in-line between the Mu-4000 analyzer and the C300 Process Controller.



Protocols Tested

In Mu terminology, attacks are hierarchically divided into Protocols, Suites and Variants. A Variant is the lowest level in the hierarchy, and is a collection of attacks using a common method of attack. A Suite is a collection of Variants that generally involves a single message or transaction type. A Protocol consists of a collection of Suites. An Analysis can consist of one or more Protocols.

The following protocols were tested during this analysis:

Protocol	Suites Run	Mu Protocol Version
ARP	All	2.3.3832
DHCP	None ^	n/a
ICMPv4	2 of 3 suites*	2.3.3832
IEEE 802.1p/Q	None‡	n/a
IPv4	All	2.3.3832
TCP	All	2.3.3832
TFTP	None**	n/a
UDP	All	2.3.3832

* Since the C300 did not support ICMP timestamp requests, this suite was omitted in the ICMP testing.
^ The C300 is not a DHCP server.

‡ The C300 does not support this protocol.
** The C300 is not a TFTP server.

About the MUSIC Certification Program

The MUSIC certification is based on the philosophy of vendor-driven testing (either at their own facility or using an approved Mu partner lab) with independent verification, an approach that already works well in many industries. Mu Dynamics provides negative tests designed to expose implementation flaws in implementations of all protocols that are part of the certification. Mu Dynamics' customers who own or rent the Mu-4000 and the relevant protocols that comprise the MUSIC test package may run through the certification tests as part of their development and quality assurance processes and submit authenticated Mu-4000-generated reports to Mu Dynamics or MUSIC consulting partners for verification. They may also engage Mu Security or its consulting partners to perform the testing and verification. The tests themselves are accessible to anyone with access to a Mu-4000 analyzer. Mu Dynamics or its partner labs will archive all analyses in such a manner that they can be reproduced at any time if the certified device is available.

MUSIC Certification consists of a Foundation Level and an Advanced Level. Protocols available for testing and certification at the Foundation Level include ARP, DHCP, ICMPv4, IEEE 802.1p/Q, IPv4, TCP, TFTP and UDP. Customers will need to test all applicable supported protocols on the device under test for the target certification level. Protocols available for testing at the Advanced Level include DNP3, FTP, HTTP, MMS, MODBUS/TCP, Telnet and SNMP. Customers may choose to certify individual protocols for the Advanced Level certifications.

Certification details are posted under the Mu Secure Critical Infrastructure solution page at <http://www.mudynamics.com/solutions/customers/endusers.html#critical> and will include:

- Product Name
- Product Version tested
- Protocols tested
- Unique Test identifier
- Test location
- Date of testing
- Expiration date of certification

Mu Dynamics fully supports the work of ISA SP99 and IEC 61508 in their efforts to define and promulgate security standards within the industrial control systems markets (DCS, MES, SCADA, etc.) and commits to shipping automated test suites corresponding to these evolving security standards as soon as (or before, if possible) they become available, in addition to the MUSIC test suites available today. Complete details on the MUSIC program may be obtained from <http://www.mudynamics.com/music>.

Contact Information

Mu Dynamics – MUSIC Program
Telephone: 1-408-329-6336
Email: music@mudynamics.com



686 W. Maude Avenue
Suite #104
Sunnyvale, CA 94085

Phone 1 866 276 4640
+1 408 329 6330
Fax +1 408 329 6317

www.mudynamics.com
info@mudynamics.com

Analysis performed using Mu Dynamics' analyzer product is consistent with current industry best practices. Vulnerabilities may exist in products in spite of such testing. Mu Dynamics, Inc. and its partner laboratories cannot guarantee that certified products are free of all vulnerabilities. Mu Dynamics and/or its partners also cannot guarantee that testing was carried out on the specific device and version listed unless Mu or the partner lab is the entity listed as carrying out the actual testing. In cases where Mu or a partner lab did not carry out the actual testing, vendors of the products being certified provided a signed affidavit that the testing was actually performed on the device(s) and software version that were submitted for certification. This MUSIC Certification is not an endorsement or warranty of the certified device. Mu Dynamics does not warrant the operation, performance or functionality of the certified device or that the certified device will be suitable for the end user's application or will satisfy the end user's requirements.

Copyright © 2008 Mu Dynamics. All rights reserved. Mu Dynamics, Mu-4000 and the Mu Dynamics logo are trademarks of Mu Dynamics.

PS20070815D