Crestron® System Architecture

Security Reference Guide

Crestron Electronics, Inc.

Original Instructions
The U.S. English version of this document is the original instructions.
All other languages are a translation of the original instructions.

Contents

Introduction

Crestron® designs systems with a focus on integration with Enterprise IT infrastructure. Crestron prioritizes support for industry standard protocols (SSH and TLS), Active Directory® software, 802.1x, and SNMP. Products are rigorously tested to ensure stability and compatibility within the Enterprise.

The DMPS3 family of products is included on a list of U.S. military-tested and approved devices. These products have undergone network device testing by the Joint Interoperability Test Command (JITC), which is a part of the U.S. Department of Defense that conducts testing on behalf of the U.S. Military. While focused on the needs of the DoD and other federal agencies, the test criteria are applicable to any professionally managed enterprise.

3-Series® processors use a unified platform to provide the same security functions. In addition, Crestron is in the process of evaluating our products against the Common Criteria, which is a set of security standards used for government deployment.

Crestron also regularly reviews the National Vulnerability Database and Common Vulnerabilities and Exposures Database for any applicable security flaws. Crestron ensures that any required patches are given the highest possible priority and provided free of charge.

Development Practices

Crestron identifies operating environment assumptions and applicable risks for created systems. Since the intent is to comply with the Common Criteria, Crestron has incorporated a number of aspects from the collaborative Protection Profile for Network Devices (NDcPP) Version 2.0 into the internally published coding standards and network interoperability guides. Other sources of controls include a number of Security Technical Implementation Guides (STIGs) published by the Defense Information Systems Agency (DISA) including Network Device Management, Network Devices, and Network Infrastructure Policy.

Crestron's Open Source Policy requires senior level approval to ensure extensive security considerations. To allow for vulnerability tracking at the product level, open source libraries are assigned a part number and added to the Bill of Materials of the product(s) that includes the library.

Crestron engineers are required to be familiar with, and conform to, these coding standards. In addition, source code is reviewed to ensure both proper functionality and conformance to security guidelines. Source code is also subjected to scans that use automated tools to review code for common errors and security holes.

A rigorous testing process is in place once the software/firmware is compiled and loaded into systems. Each night, the latest code is built and automatically tested to ensure system stability. Included in these tests are standard network scanning tools to ensure that no unauthorized ports have been opened.

When a system is ready for release, automated and manual tests are run to ensure a robust and secure environment.

Updates are also secured via firmware components that are digitally signed using a 2048-bit long RSA asymmetric key pair with SHA-256 as the hash. The system checks the signature before updating the device. The private key is kept in a secure location with access to a limited number of administrators. During the build, an automated process accesses the key, signs the components, and wipes the key from the build system.

Security Features in the 3-Series Controls Systems

The 3-Series platform was first released in 2011. The following year, the 3-series platform was updated to add security features to the system.

The platform supports a multi-level authentication model for user accounts with different levels of system access. An administrator has the ability to perform configuration steps while other users may be prohibited from making changes to the system. In this case, administrators operate the system as authenticated users.

This authentication model is integrated with Active Directory, allowing AD groups to map to the various access levels without the maintenance of local user accounts.

In addition, devices can be authenticated to access the network itself using 802.1x.

Crestron regularly releases updates for any applicable security flaws found in the National Vulnerability Database or in the Common Vulnerabilities and Exposures Database. These updates are given the highest priority.

Most recently, the security functions were updated to support, and default to, TLS 1.2 with fallback to earlier TLS/SSL versions when configured to do so. Support for audit logging was also enhanced to support an RSYSLOG server over a secure TLS connection.

Guidance documentation regarding the best practices and deployment of secure systems is available via Crestron's security site at security.crestron.com.

Certifications

Many Crestron products have been added to the U.S. Department of Defense Approved Product List (APL). More information about products on the APL can be found on the Defense Information Systems Agency website. Enter **Crestron** into the keywords field and press **Search APL**. Crestron also maintains a detailed list of products for JITC certified products.

DigitalMedia™ System Solutions Security

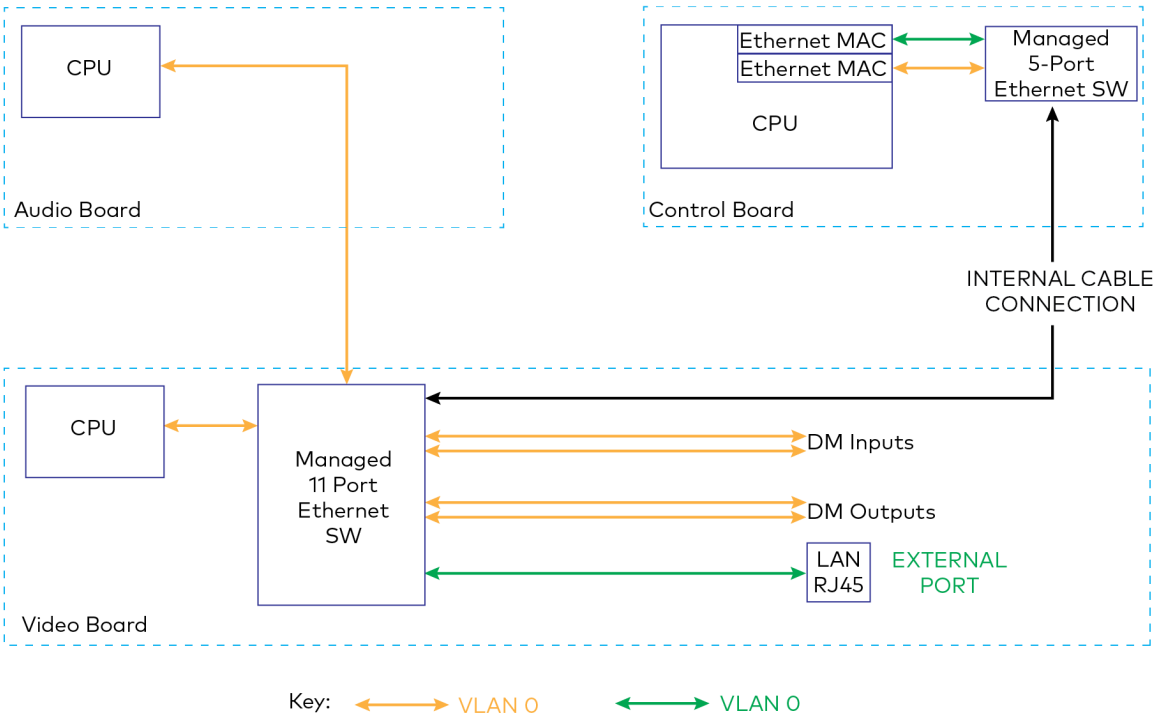
Crestron's popular DigitalMedia Presentation System (DMPS) product line was added to the Approved Product List (APL) on April 13, 2015 as a certified Video Distribution System.

The PRO3, AV3, and CP3N provide the same functionality as the DMPS control board and connect to the video devices in a similar manner. In particular, they contain a network router which, when configured in Isolation Mode, prohibits all traffic to the LAN.

NOTE: For more information on network router rules in Isolation Mode, see the Crestron Control Systems Security Reference Guide (Doc. 8563) at security.crestron.com.

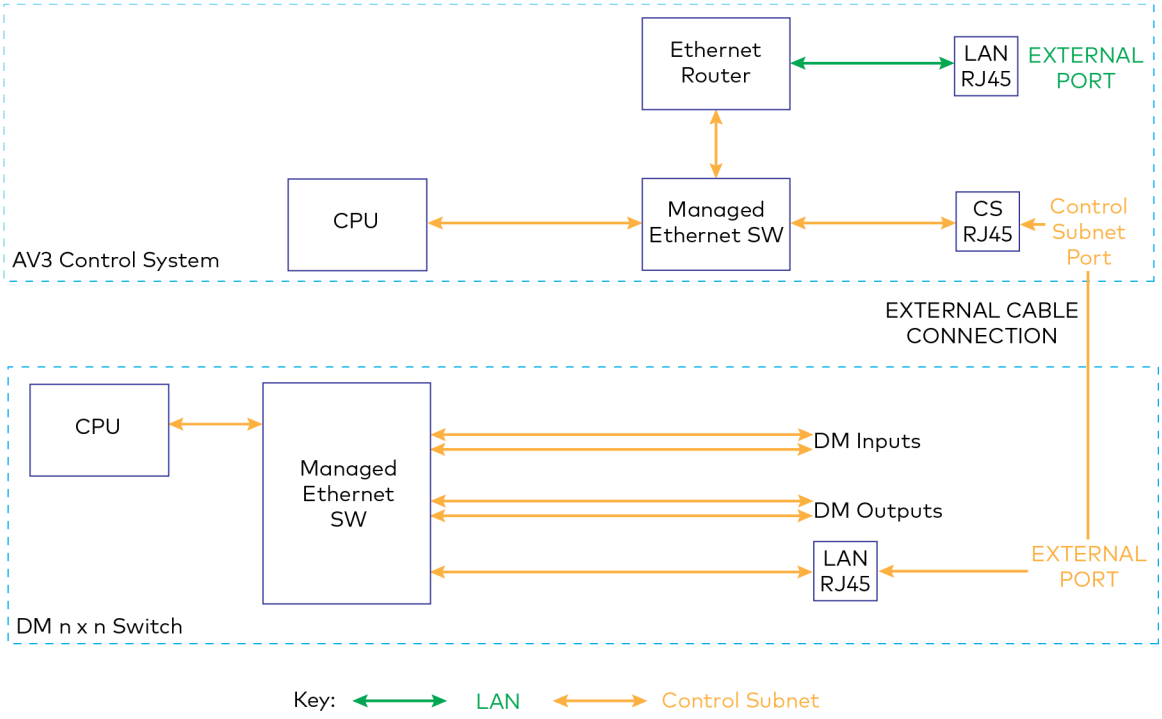
As seen below, the DMPS uses Ethernet® connections for internal communications.

DMPS ETHERNET ARCHITECTURE



By utilizing the AV3 (or PRO3, CP3N) and its Control Subnet function, the same architecture is achieved (including the DM-MD8x8, DM-MD16x16, DM-MD-32x32, DM-MD-64x64, DM-MD-128x128) as the video switching portion. The only difference is that the Ethernet connection is made via an external connection, as seen below.

AV3 with DM SWITCH ETHERNET ARCHITECTURE



Android™ Software Based Device Security

While some Crestron devices are built on Android software, they are fundamentally different devices than the Android devices the reader may be more familiar with.

- Android is used to provide the core operating system and display rendering components.
- There is no access to the Google Play™ store or any method to allow arbitrary 3rd party applications to run on the device.
- None of the Google® applications (with the exception of the browser) are included on the device.
- While the devices do include a browser client, the client is not typically exposed to the end user. When the client is exposed, it is usually set to render a captive URL and no browsing to arbitrary URLs is provided. Browser client exposure is fully within the installer's control.
- Most devices do not support wireless communication, which significantly reduces the number of relevant vulnerabilities. Bluetooth® devices are only used for beaconing support.
- The Crestron TSW touchscreens designated as -NC have no camera, microphone or Bluetooth beacon support.
- The devices support 802.1X authentication.

Crestron's hardening guidelines are available at security.crestron.com.

Crestron Control Subnet

Crestron's CP3N, AV3, and PRO3 feature the Crestron Control Subnet to create a new Ethernet network dedicated to Crestron's Ethernet devices. The Control Subnet's main purpose is to simplify setting up a dedicated Crestron LAN. The Control Subnet has a DHCP and DNS Server and is designed as a fully functional firewall/router. The control system and Crestron tools will open up ports as needed.

By default, the devices on the Control Subnet are able to reach out to the wider LAN, but other traffic inbound into the Control Subnet is limited to Crestron tools.

To further restrict the system, the 3-Series processor supports Isolation Mode. In Isolation Mode, the firewall is configured in such a way that no traffic can traverse from the LAN to the devices on the Control Subnet nor from the Control Subnet to the LAN.

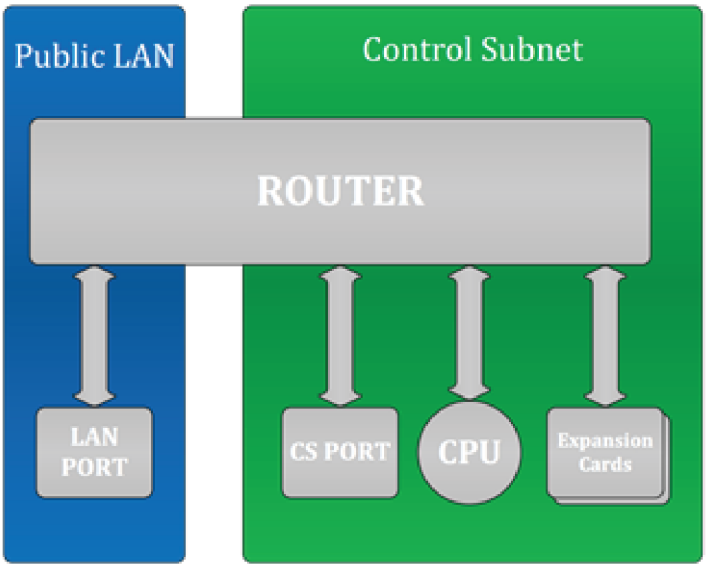
Using this mechanism, a corporate LAN can be protected from devices on the Control Subnet.

Architecture

Even if nothing is plugged into the Control Subnet port on the back of the control system, there are still some devices on the Control Subnet:

- Control System CPU (this is where the AV Programs run)
- Optional Expansions cards (PRO3 and AV3 only)

This design ensures that the Crestron CPU and optional expansion cards are protected from malicious packets on the LAN. The diagram below illustrates how the components work together.



The firewall rules only allow in traffic that the CPU perceives. As a result, a port scan will only show ports that the CPU perceives. Manual port forwarding rules can be set to make custom connections to the devices on the Control Subnet.

Crestron's management utility, Crestron Toolbox™ software, creates custom port forwarding rules in the 64000–64299 range to enable management of the devices on the Control Subnet. These port forwarding rules are created when the tool connects, and they are broken down when either the tool disconnects or the device is rebooted.

NOTE: For more details regarding port forwarding rules, see the Crestron Control Systems Security Reference Guide (Doc. 8563) at crestron.com/manuals.

Security Feature Matrix

	Secure Cresnet® Connection over IP Protocol	SSL/TLS Encryption Suite	Supports RSYSLOG	Requires Signed Firmware Updates
DM Switchers (8x8 through 32x32)	Yes	SSLv3 (Systems may be updated to TLS1.2 using the new CPU3 card)	No	No
DM Switchers (8x8 through 128x128) with 3 Series Processor	Yes	TLS 1.2	Yes	Yes
3-Series (CP3N, PRO3, AV3)	Yes	TLS 1.2	Yes	Yes
3-Series (All other models)	Yes	TLS 1.2	Yes	Yes
DMPS 3-Series	Yes	TLS 1.2	Yes	Yes
DMPS 3-4K series (250, 350)	Yes	TLS 1.2	Yes	Yes
DMPS 3-4K series (All other models)	Yes	TLS 1.2	Yes	Yes
NVX Series	Yes	TLS 1.2	Yes	Yes
DSP Series	Yes	TLS 1.2	Yes	No
AMP series	Yes	TLS 1.2	Yes	No
TSW-x60	Yes	TLS 1.2	Yes	No
TSW-1542	Yes	TLS 1.2	Yes	No
Mercury (Flex M series)	N/A	TLS 1.2	Yes	No
DM-TXRX	Yes	TLS 1.2	No	No
AM-200/300	Yes	TLS 1.2	Yes	No
DGE-100/200	Yes	TLS 1.2	Yes	No
Fusion	Yes	TLS 1.2	No	N/A
UC-Engine	Yes	TLS 1.2	No	Yes
XiO Cloud	N/A	TLS 1.2	N/A	N/A
Flex P series (Phones)	N/A	TLS 1.2	No	Yes

	SSH/SFTP	Can add 3rd party certificate	Isolated LAN	802.1x	Active Directory Authentication.
DM Switchers (8x8 through 32x32)	No	Yes	No	No	No
DM Switchers (8x8 through 128x128) with 3 Series Processor	Yes	Yes	Yes	Yes	Yes
3-Series (CP3N, PRO3, AV3)	Yes	Yes	Yes	Yes	Yes
3-Series (All other models)	Yes	Yes	No	Yes	Yes
DMPS 3-Series	Yes	Yes	No	Yes	Yes
DMPS 3-4K series (250, 350)	Yes	Yes	Yes	Yes	Yes
DMPS 3-4K series (All other models)	Yes	Yes	Yes	Yes	Yes
NVX Series	Yes	Yes	No	Yes	Yes
DSP Series	Yes	Yes	No	Yes	Yes
AMP series	Yes	Yes	No	Yes	Yes
TSW-x60	Yes	Yes	No	Yes	Yes
TSW-1542	Yes	Yes	No	Yes	Yes
Mercury (Flex M series)	Yes	Yes	No	Yes	Yes
DM-TXRX	Yes	Yes	No	Yes	No
AM-200/300	Yes	Yes	No	Yes	Yes
DGE-100/200	Yes	Yes	No	Yes	Yes
Fusion	N/A	On-prem only	N/A	N/A	Yes (Currently on-prem only)
UC-Engine	No (SCTP)	Yes	No	Yes	Yes
XiO Cloud	N/A	No	N/A	N/A	Yes
Flex P series (Phones)	No	Yes (see Admin Guide V9.45-366)	No	Yes (see Admin Guide V9.45-76)	No

This page is intentionally left blank.

Crestron Electronics, Inc.
15 Volvo Drive, Rockleigh, NJ 07647
Tel: 888.CRESTRON
Fax: 201.767.7656
www.crestron.com

Security Reference Guide — 8562A
(2054757)
10/25/19
Specifications subject to
change without notice.