Crestron® Touch Screens

TSW-x52
TSW-x60
DGE-x00
TS-1542x
TST-902

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.

Crestron product development software is licensed to Crestron dealers and Crestron Service Providers (CSPs) under a limited nonexclusive, nontransferable Software Development Tools License Agreement. Crestron product operating system software is licensed to Crestron dealers, CSPs, and end-users under a separate End-User License Agreement. Both of these Agreements can be found on the Crestron website at www.crestron.com/legal/software_license_agreement.

The product warranty can be found at www.crestron.com/warranty.

The specific patents that cover Crestron products are listed at www.crestron.com/legal/patents.

Certain Crestron products contain open source software. For specific information, visit www.crestron.com/opensource.

Revision History

Please send comments and change recommendations to SecurityDocs@crestron.com.

Rev	Date	Notes	Author(s)
A	March 7, 2018	Initial version	JP
B	March 9, 2018	Added DGE and TS touch screens	JP
C	March 12, 2018	Release version	JP
D	May 23, 2018	Added 802.1X Reference	JP
E	January 18, 2019	Added autodiscovery instructions	JD, JP, MR
F	April 7, 2020	Added TST-902 and Ports tables	YP
G	May 8, 2020	Converted to Flare document	BD
H	January 15, 2021	Added TSW-x70 series	YP, IH
J	April 26, 2022	Removed TSW-x70 series (moved to a separate document)	IH

Contents

Overview

This document describes the steps needed to harden a Crestron® touch screen and assumes a basic understanding of security functions and protocols.

> **NOTE:** This security statements and protocols described in this document are applicable only for the touch screen models listed in Devices (on page 3).

Crestron designs systems to integrate with enterprise IT infrastructure. Crestron has prioritized support for Active Directory® credential management, 802.1X, and SNMP, as well as a shift to industry standard protocols including support for SSH and the latest versions of TLS. Products are rigorously tested to ensure stability and compatibility within the enterprise.

The Joint Interoperability Test Command (JITC), which is part of the U.S. Department of Defense, conducts testing for network devices on behalf of the U.S. Military. Security functions are the highest priority, but testing also touches on interoperability and other operational functionality. While focused on the needs of the DoD and other federal agencies, the test criterion are applicable to any professionally managed enterprise.

As a result of JITC testing, the Crestron® touch screens in this document are part of the Crestron video distribution systems that are currently listed on the government's Approved Products List.

> **NOTE:** The listing for TSW-60 series models targets the -NC (no camera) versions of the product line, but the security functionality is otherwise the same.

Conditions of Fielding

Users must reference and follow the Conditions of Fielding (COF) found in the Information Assurance Assessment Report/Cybersecurity Assessment Report (IAAR/CAR). The IAAR/CAR must be requested directly from APCO International® or at aplits.disa.mil.

Devices

This document describes the security aspects of the following Crestron touch screens, which are built on the Android™ OS.

NOTE: For security information regarding TS-70 and TSW-70 series touch screens, refer to the TS-70 and TSW-70 Series Touch Screens Security Reference Guide.

The models listed within this table are covered by this document:

Model	Firmware Version	OS Version	OpenSSL Version
TST-902 TSW-552 TSW-752 TSW-1052	1.003.0020 or higher	Android ICS (4.0.4)	OpenSSL 1.0.1l
TSW-560 TSW-560P TSW-560-NC TSW-760 TSW-760-NC TSW-1060 TSW-1060-NC	2.009.0061	Android Lollipop (5.1.1)	OpenSSL 1.1.1
TS-1542 TS-1542-C DGE-100 DM-DGE-200-C	1.3384.00049 or higher	Android ICS (4.0.4)	OpenSSL 1.0.1l

While Crestron touch screens are built on Android, they are fundamentally different from other Android-based devices:

- There is no access to the Google Play® store or any other method to allow arbitrary third-party applications to run on the device.
- While the devices include a browser client, this is typically not exposed to the end user. When it is exposed, it is usually set to render a captive URL, and no browsing to arbitrary URLs is provided. This is fully within the installer's control.
- The lack of wireless communications significantly reduces the number of relevant vulnerabilities. Bluetooth® connectivity is only used for beaconing support.
- The Crestron TSW-60-NC models have no camera, microphone, or Bluetooth beacon support.
- All listed touch screens (except for the TST-902) support 802.1X authentication.
- TST-902 only supports the following security for Wi-Fi protocols:
  64 & 128-bit WEP, WPA™ & WPA2™-PSK with TKIP & AES.

Security

The encryption libraries in Crestron touch screens are provided via OpenSSL rather than the stock Android encryption methods.

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

In addition, the platform is patched during any regularly scheduled firmware update.

Security Deployment Instructions

To harden any of the devices referenced in this document, use the following commands:

- `authentication on`
- If self-signed certificates are used on a connected control system, issue `ssl noverify`. If CA-signed certificates are used on a connected control system, issue `ssl ca` and load the CA-signed certificate to the touch screen.
- If the touch screen will communicate with a control system that has Authentication turned on, supply the username and password for the control system CIP connection via the `setcsauthentication` command.

> **NOTE:** Authentication credentials must be created on the control system before setting up the IP table entry for the touch screen, otherwise the IP cloud may get blocked on the control system side.

- If SIP/Rava® VoIP support is not needed, disable it with the `sipenable off` command. SIP over TLS is also supported if desired.
- Issue `entersetupseq disable` to disable user access to the device's local configuration screens.
- Issue `hydrogenenable off` to disable a connection to the XiO Cloud® service.

The TSW-60 series also include a web server for configuration, which can be disabled with the `webserver off` command.

Turning on Authentication automatically disables the FTP server, Telnet access, and CTP (legacy Crestron Toolbox™ console). The commands below are provided in case these actions will be taken separately:

- `ftpserver off`
- `telnetport off`
- `ctpconsole disable`

Crestron devices support an autodiscovery feature which allows them to be detected, report basic information, and do some basic configuration remotely. This feature is not protected by authentication and should be disabled for improved security.

Autodiscovery can be shut off by using the `autodiscovery off` command.

Ports and Protocols

Function	Destination Port	From (Sender)	To (Listener)	Notes
NTP	123/UDP	Device	NTP server	Network Time Protocol (NTP)
SSH/SFTP	22/TCP	Admin workstation	Device	Used for configuration, console, and file transfer
HTTPS	443/TCP	Admin or end-user workstation	Device	Secure Web Configuration, for TSW-60 devices only; Disabled with `webserver off`
FTP	21/TCP	Admin or end-user workstation	Device	Disabled with `authentication on`
Telnet	23/TCP	Admin or end-user workstation	Device	Disabled with `authentication on`
CTP console	41795/TCP	Admin or end-user workstation	Device	Disabled with `authentication on`
DHCP	67/UDP	Device	DHCP server	DHCP addressing
DHCP	68/UDP	DHCP server	Device	DHCP addressing
HTTP	80/TCP	End-user workstation	Device	Redirect to Secure Web Configuration on port 443; For TSW-60 devices only
SNMP	161/UDP	Device or SNMP manager	Device or SNMP manager	Available for monitoring; Not required for device functionality
Crestron-CIP	41794/TCP	Device	Control system	Crestron Internet Protocol - to control system; Can be configured in the control system to use secure CIP

Function	Destination Port	From (Sender)	To (Listener)	Notes
Crestron-Secure CIP	41796/TCP	Device	Control system	Crestron Internet Protocol Secure - to control system
Crestron autodiscovery	41794/UDP	Device or Crestron Toolbox	Device	Allows finding Crestron equipment on a LAN; Autodiscovery is disabled with `autodiscovery off`
SIP	5060/TCP/UDP	Device	SIP server	Audio dialer SIP client - can be changed to a different port; May be disabled
SIP-TLS	5061/TCP	Device	SIP server	Audio dialer SIP client - can be changed to a different port; May be disabled
HTTPS	443/TCP	Device	XiO Cloud® Service	For XiO Cloud services, not required for device functionality; A persistent connection is made via AMQP over WebSockets; HTTPS services such as routing lookups and file transfers may be used; Applies only to TSW-60, DGE, and TS-1542 devices.

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 — Doc. 8738J

04/26/22
Specifications subject to
change without notice.