AVIXA RP-C303.01:2018

Recommended Practices for Security in Networked AV Systems

AVIXA
Audiovisual and Integrated Experience Association
avixa.org

AVIXA RP-C303.01:2018

Recommended Practices for Security in Networked AV Systems

ICS Code: 35.030

ABSTRACT

AV systems operating over enterprise networks pose a serious risk for security breaches. AV professionals must understand and mitigate these risks. This *Recommended Practice* provides guidance and current best practices for securing networked AV systems of all sizes. Recognizing that security requirements are highly specific for sole proprietors and/or organizations of all sizes and experience, the steps outlined in this document can be adapted to form a baseline for establishing a robust AV security management program.

ISBN: 978-0-939718-41-2

FOREWORD

The information contained in this *Foreword* is for information purposes and not part of AVIXA RP-C303.01. ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

About AVIXA

AVIXA™ is the Audiovisual and Integrated Experience Association, producer of InfoComm trade shows around the world, co-owner of Integrated Systems Europe, and the international trade association representing the audiovisual industry. Established in 1939, AVIXA has more than 5,400 members, including manufacturers, systems integrators, dealers and distributors, consultants, programmers, rental and staging companies, technology managers, IT professionals, content producers, and multimedia professionals from more than 80 countries. AVIXA members create integrated AV experiences that deliver outcomes. AVIXA is a hub for professional collaboration, information, and community, and the leading resource for AV standards, certification, training, market intelligence and thought leadership.

AVIXA is an ANSI accredited Standards Development Organization (SDO). The work of preparing standards and guidelines is carried out through AVIXA Task Groups and governed by the AVIXA Standards Steering Committee which is governed by the AVIXA Board of Directors.

Suggestions for improvement of this document are welcome. They should be sent to standards@avixa.org.

AVIXA thanks the following contributors:

AVIXA Network Security Task Group

Greg Bronson, CTS-D, Cornell University
Jason Dalton, CTS-I, BAE Systems
Toine Leerentveld, Crestron Electronics, Inc.
Stuart Mitchell, European Centre for Medium-Range Weather Forecasts
John Monitto, CTS, Meyer Sound
Richard Morrison, CTS, AECOM
David Samura, International Criminal Court
Jim Smith, CTS-D, Sound Control Technologies
Pomona Valero, CTS, PITM Consulting

AVIXA extends special thanks to Paul Zielie, CTS-D, CTS-I, Harman, for his contributions to the development of this *Recommended Practice*.

AVIXA Standards Steering Committee

Thomas Mullins, CTS, Affiliated Engineers, Inc.
Ben Boeshans, CTS-D, Idibri
Greg Bronson, CTS-D, DMC-E, Cornell University
Kristian Glahn, EnCollab
John Monitto, CTS, Meyer Sound
Richard Morrison, B.Eng (hons), CPEng, CTS, AECOM
Don Palmer, Administrative Office of the United States Courts
Jim Smith, CTS, Sound Control Technologies
Dick Tollberg, CTS-D, AVI-SPL Chicago
Pomona Valero, CTS, PMP, PITM Consulting

AVIXA Staff

Ann Brigida, CStd, CTS (Senior Director of Standards)
Michelle Streffon Truong, AStd, CTS (Standards Manager)
Loanna Overcash (Standards Developer)
Catalina Vallejos (Standards Resources Coordinator)

TABLE OF CONTENTS

1 INTRODUCTION

Audiovisual (AV) systems are becoming increasingly central to global operations as they offer expanded remote management capabilities for increased oversight, efficiency, and effectiveness. Connecting systems to an enterprise network allows AV professionals to remotely administer management controls and increase the number of systems that can be overseen by a single professional. This capability has become the expected norm in the industry.

As AV systems become more widely connected via enterprise networks, their exposure increases as targets or channels for security breaches. The escalation of these security threats poses a major challenge for AV professionals. To address these security concerns, AV professionals must make securing networked AV systems a top priority – regardless of the size of the system.

Security requirements for individual organizations are highly specific and not one size fits all. Networked AV systems – that is, AV systems that operate over networks – must be aligned with the overall security goals of their organization, regardless of its size, location, or activity. However, the traditional separation of AV and enterprise IT operations within many organizations has left uncertainty about who is responsible for identifying, managing, and ensuring the security configuration of AV systems on the network. This increases security risks and hampers efforts to meet an organization's security needs.

Several essential steps should form the foundation of an effective AV security program:

a) AV professionals must establish a deep understanding of the risks their organizations face. This understanding should be founded on a comprehensive analysis that identifies and prioritizes each risk.

b) Each organization should take a strategic approach to risk management by creating and implementing a risk response and mitigation plan.

c) The mitigation of risk should be supported by proven security measures. For AV systems, these include best practices that contribute to the overall organizational policy.

d) A comprehensive understanding of an organization's stance on security, including its AV systems, should be available to authorized personnel. The careful documentation of systems and security measures creates a base of knowledge that should inform AV programs going forward.

e) Regular testing is imperative to establishing effective security. AV systems should be scanned regularly for common vulnerabilities, as well as subjected to more active penetration testing when practicable.

f) Develop an inventory of networked AV resources for ongoing use to manage updates, patches, and decommissioning (remove from active service).

g) Proactive communication with enterprise counterparts to clearly define areas of responsibility and document responsibilities for each identified part/element under the risk management program.

2 SCOPE

This *Recommended Practice* provides guidance and current best practices for securing networked AV systems of all sizes. Regardless of their size or experience, organizations* that take the steps outlined in this recommended practice can form a baseline for establishing a robust AV security management program.