CTA Technical Report

Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1

CTA-TR-4

(Formerly CEA-TR-4)

June 2014

ANSI Accredited Standards Developer

Consumer Technology Association™

NOTICE

Consumer Technology Association (CTA)™ Standards, Bulletins and other technical publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards, Bulletins and other technical publications shall not in any respect preclude any member or nonmember of the Consumer Technology Association from manufacturing or selling products not conforming to such Standards, Bulletins or other technical publications, nor shall the existence of such Standards, Bulletins and other technical publications preclude their voluntary use by those other than Consumer Technology Association members, whether the standard is to be used either domestically or internationally.

Standards, Bulletins and other technical publications are adopted by the Consumer Technology Association in accordance with the American National Standards Institute (ANSI) patent policy. By such action, the Consumer Technology Association does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard, Bulletin or other technical publication.

This document does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this document to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

(Formulated under the cognizance of the CTA **R7 Home Networks Committee**.)

Published by
©CONSUMER TECHNOLOGY ASSOCIATION 2015
Technology & Standards Department
www.CTA.tech

CEA Technical Report on Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1

Contents

[This page intentionally left blank.]

CEA Technical Report on Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1

1. Purpose

The existing authentication algorithm described in ANSI/CEA-709.1 is now 25 years old. It uses a short, shared secret (only 48-bits) and a custom algorithm to perform authentication. Compared against today's cryptographic standards it cannot be considered a viable authentication algorithm for new designs. While it *may* be appropriate to implement it for backward compatibility reasons, it must not be considered as a part of an overall security system for ANSI/CEA-709.1 based systems.

This document explains how to add state of the art security to the ANSI/CEA-709.1 application protocol.

This document serves as an accompanying technical document to aid developers in creating secure systems using ANSI/CEA-709.1 by adding encryption and authentication at the application layer. Since ANSI/CEA-852 is a standard for tunneling ANSI/CEA-709.1 messages through an IP network, the changes in this forthcoming technical document, when applied to the tunneled ANSI/CEA-709.1 messages will render the messages secure even when no authentication is used in the ANSI/CEA-852 or ANSI/CEA-852.1 standards.

Architectural details of the proposed solution are provided below. Standardization of these APDU formats will permit interoperability of secure nodes so that a secure system may be created from components sourced from multiple vendors using either or both ANSI/CEA-852 based networks and ANSI/CEA-709.1 based networks.

2. References

[1] ANSI/CEA-709.1 Control Network Protocol Specification http://global.ihs.com

[2] ANSI/CEA-852 Tunneling Device Area Network Protocols Over Internet Protocol Channels http://global.ihs.com

[3] ANSI/CEA-852.1 Enhanced Protocol for Tunneling Component Network Protocols Over Internet Protocol Channels http://global.ihs.com

[4] FIPS 140-2 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[5] Approved Security Functions http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf

[6] Approved Random Number Generators http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf

[7] Approved Key Establishment Techniques http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf

[8] Suite B Cryptography http://www.nsa.gov/ia/programs/suiteb_cryptography/

[9] NISTIR 7628 http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf

[10] “AES Key Wrap Specification”, http://csrc.nist.gov/groups/ST/toolkit/documents/kms/key-wrap.pdf

3. Abbreviations

APDU	Application Protocol Data Unit
NSA	National Security Agency
ECDSA	Elliptic Curve Digital Signature Algorithm
AES-GCM	Advanced Encryption Standard - Galois Counter Mode
ECC	Elliptic Curve Cryptography
NIST	National Institute of Standards and Technology

4. Scope

ANSI/CEA-709.1 is a machine to machine protocol. As such, considerations concerning user management, user access control, user password management, management console logging, physical security of network access points, and physical security of devices and tamper detection of devices are outside the scope of the communication protocol. Nevertheless, these issues must be considered when building any secure system and these and more are discussed in [4] and [9]. System developers are encouraged to review these references and decide what level of security is appropriate to their application.

It is envisioned that some applications will require minimal security – analogous to a computer network sitting behind a firewall where the messages between the machines are sent in the clear. Other applications will require very strong security – for example a network that controls valuable infrastructure that is deployed across a geographic area where each node sits unattended and can be subjected to a variety of attacks.

It is intended that an ANSI/CEA-709.1 network deployed with the enhancements described within this document could be deployed in an environment requiring very strong security provided that the security concerns outside the scope of a communications protocol, e.g. physical security, tamper detection; user management, etc. are also addressed by the system implementer.

5. Requirements within the Scope

Secure Firmware Upgrade. ANSI/CEA-709.1 networks support over the air firmware upgrades. All firmware images must be digitally signed by the image builder and verified on the device prior to activating the downloaded firmware. Any firmware images for which the signature cannot be verified are to be discarded by the device.

Identification and Verification. Nodes must not be permitted to join the network or interact with other nodes without first identifying the node and verifying its origin using strong, public key cryptography. Nodes that do not pass authentication must not be given network addresses or other means that would allow communication on the network with secured nodes.

Authentication/Non-Repudiation. When required by the application, messages must be mutually authenticated by the sender receiver so that both parties know that the message was authentic and the request was received and the response actually came from the intended recipient. The authentication mechanism must also provide affirmation of data integrity such that an attacker cannot modify the contents of the packet in transit without detection.

Confidentiality. When required by the application, messages must be encrypted such that their contents cannot be read by unauthorized parties.

Record/Playback Resistance. Special care must be taken so that an intruder cannot simply record a message that had a desired effect, and re-play it at another time to deceive the recipient that the authorized requestor has sent the message. There are two generally approved techniques to accomplish this: using a timestamp, and using sequence numbers. In either method, the timestamp or the sequence number must be protected from modification by an attacker. Neither technique provides complete protection, but with both techniques an implementer can render the attack window so small as to not be practical for an attacker to mount a successful attack.

Key Management. In a modern cryptosystem there are public/private key pairs used for asymmetric-key cryptography and shared keys used for symmetric-key cryptography. Private keys must never be sent across the network or leave the boundaries of the device. Public keys may be shared in the clear as knowing the public

key does not help an attacker gain access to the private key. Shared keys must be distributed using public key cryptography to be compliant with [4]. Symmetric keys must be established between two nodes using an approved process defined in [7]. It must be possible to revoke keys over the network such that a node may no longer have access to the network. It must be possible for a node to be able to zero out its keys if it detects physical intrusion attempts.

Key Protection. When keying material is stored outside of the device, it must first be encrypted using one of the methods described in [5].

Revocation of Credentials. Nodes that have been compromised, or suspected of having been compromised must be blocked from network access. Potentially, all the nodes in the system must be re-keyed at this point. Nodes that detect tampering on themselves must have the ability to zero out all keying material.

Random Number Generation. Most cryptographic functions rely at one point or another on a random number to create a seed or a Nonce. If an intruder can predict the random number that will be used, then the system may be compromised. For this reason, a random number generator taken from the list in [6] must be used.

6. Architectural Decisions and Rationale

1. Provide security at the application layer rather than at lower layers in the stack.

   In many implementations the application and the application protocol are executed on one processor/memory subsystem, while the lower layers of the protocol are executed on another processor/memory subsystem. A typical example is a PC running the application and the application protocol with a removable USB network adaptor running the lower layers of the protocol. If the encryption is done in the application protocol, then the information that passes between the PC and the USB adaptor is already secured. If, on the other hand, all encryption and decryption is done on the network adaptor, then the connection between the PC and the removable USB network interface becomes a very convenient and accessible attack point.

2. Use NSA Suite B algorithms [8] exclusively.

   The Suite B algorithms are considered to be the strongest security algorithms available for civilian use. Suite B has been heavily promoted by the U.S. government so that virtually all computer systems support Suite B, making interoperability between the new ANSI/CEA-709.1 and these systems easier. Due to its popularity and standardization, the Suite B algorithms have been

subjected to relentless international attacks, further demonstrating their strength. Finally, Suite B is projected to have a long life prior to its eventual deprecation, due to its cryptographic strength.

3. Use ECDSA to sign firmware images.

   ECDSA is a very robust digital signature method, and is included in Suite B.

4. Use AES-GCM for symmetric-key cryptography.

   AES-GCM provides both authentication and encryption in a single, compact and bit efficient manner. AES-GCM is the preferred version of AES supported within Suite B.

5. Use ECC for asymmetric-key cryptography.

   ECC based asymmetric-key cryptography has been shown to provide equivalent strength with shorter keys. This makes it well suited for embedded applications with memory and processing power constraints.

6. Protect keys in external memory using the AES key wrap method described in [10].

   Keying materials must be encrypted if they can be accessed outside of the device. Should an implementation seek FIPS 140-2 certification from NIST [4], this method of key protection is required.

7. Use the sequence number method to implement record/playback resistance.

   The alternative of using time stamps requires tight time synchronization between all the nodes, and a battery backed up time source for rapid restoration of networking functions after a power outage. Many ANSI/CEA-709.1 nodes do not have such a time source. Network protocols that achieve time synchronization do so with the use of additional network bandwidth. This is a significant drawback on slower links.

[This page intentionally left blank.]

Consumer Technology Association Document Improvement Proposal

If in the review or use of this document a potential change is made evident for safety, health or technical reasons, please email your reason/rationale for the recommended change to standards@CE.org.

Consumer Technology Association
Technology & Standards Department
1919 S Eads Street, Arlington, VA 22202
FAX: 703-907-7693 standards@CE.org

Consumer Technology Association™