CONCEPT PAPER

IDENTITY AND ACCESS MANAGEMENT FOR SMART HOME DEVICES

Bill Fisher
National Cybersecurity Center of Excellence

Sudhi Umarji
The MITRE Corporation

DRAFT
June 2016
IoT-NCCoE@nist.gov

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, open, integrated reference designs that are broadly applicable and repeatable. To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

KEYWORDS

authentication; authorization; identity and access management; Internet of Things; IoT; non-person entities; smart home

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

COMMENTS ON NCCOE DOCUMENTS

Individuals and organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: IoT-NCCoE@nist.gov

Comments will be accepted on a rolling basis.

1. CONCEPT

Description

The following concept paper identifies potential project topics for the NCCoE to explore with stakeholders and technology collaborators.

Through research and discussion, the NCCoE has identified several areas of interest within a broader cybersecurity subject; in this case, improved security for connected devices, or the "Internet of Things." Public comments on this concept paper will help the NCCoE understand specific challenges and needs, and may be used to help define a challenge statement, use cases, and/or a project description. Comments will be reviewed on an ongoing basis. Our hope is that stakeholders will help identify models, methodologies, protocols, best practices, or standards from other industries that may be relevant to securing smart home technology.

Areas of Interest

The Internet of Things (IoT) refers to the ability of everyday objects (things) to connect to the internet and to send and receive data. These things include cameras, home automation systems, and industrial control systems. It is estimated that there are already 6.4 billion connected devices, and by 2020, there will be 20 billion[1]. Industry experts agree that in spite of this projected growth, IoT technology is immature and lacks adequate security safeguards.

The NCCoE is seeking comments from the public and industry on the challenges of identification, authentication, and authorization for devices in the IoT space; specifically requirements for authentication and authorization of autonomous non-person entities (NPE) found in smart home devices. Areas of interest include the following:

- models for the lifecycle of IoT and/or smart home devices
- threat vectors and attack surfaces of smart home devices throughout their lifecycle
- using commercially available technology, methods for the identification, authentication, and authorization of smart home devices including:
  - core requirements in addressing these three capabilities
  - implementation challenges
  - potential security weaknesses or gaps
  - mechanisms for NPE-to-NPE, NPE-to-Network, and NPE-to-Cloud authentication

[1] http://www.gartner.com/newsroom/id/3165317

    - mechanisms for binding device, APIs, and user identity with applicable authentication contexts
    - privacy risks to individuals raised by improving smart home device identification and authentication
    - mechanisms that enable improved identification and authentication of smart home devices while maintaining individuals' privacy
- models for handling encryption on constrained devices
- business cases for the identification, authentication, and authorization of smart home devices for which the NCCoE could build a demonstrable solution

Based upon community feedback on these topics, the NCCoE will consider instantiating a project to engage in building an example solution using commercially available technology. Such a solution will demonstrate how the requirements enumerated can be met and document current best practices related to identification, authentication, and authorization of autonomous NPEs within smart homes.

2. Relevant Standards and Guidance

A number of organizations have initiated the development of standards relevant to IoT. Below are a few of the efforts that may be leveraged for this work. If there are other standards or guidance that would be relevant, please submit comments with that information.

- IETF (The Internet Engineering Task Force) - Authentication and Authorization for Constrained Environments (ACE) Working Group: The ACE working group aims to produce a standardized solution for authentication and authorization to enable authorized access in constrained IoT environments (where nodes are limited in CPU, memory and power)
- OASIS (Organization for the Advancement of Structured Information Standards) - OASIS Message Queuing Telemetry Transport (MQTT) Technical Committee (TC): The MQTT TC is developing an open publish/subscribe protocol for telemetry messaging designed to be simple, lightweight, and suited for use in constrained networks and multi-platform environments
- The Thread Group started by Google (NEST), ARM, Haiku Home, NXP, Samsung Electronics, SiliconLabs, and Yale Security currently has over 230 member organizations and has developed the Thread Stack for connecting products in the home. Thread is built on open standards and IPv6 technology with 6LoWPAN as its foundation and leverages a wireless mesh network to connect devices to each other, the internet and cloud services
- The Open Connectivity Foundation (OCF) - A non-profit organization that defines connectivity requirements for interoperability between IoT devices. OCF develops specifications, open source implementations and a certification

program for diverse markets. OCF supports the IoTivity[2] open source effort, which will deliver a reference implementention of OCF specifications

- Object Management Group - Data-Distribution Service (DDS) Platform Special Interest Group: DDS defines a virtual Global Data Space where applications can share information by reading and writing data-objects addressed by means of an application-defined name and a key. DDS features fine and extensive control of quality of service (QoS) parameters, including reliability, bandwidth, delivery deadlines, and resource limits. DDS also supports the construction of local object models on top of the Global Data Space

3. Desired Outcomes

The following are desired outcomes for an NCCoE project:

- collaborate with industry subject matter experts to define and publish requirements for identification, authentication, and authorization of autonomous NPEs in ways that minimize intrusions on individuals' privacy, and to enumerate gaps in technology and standards in meeting those requirements
- publication of an NCCoE practice guide in order provide early implementers of smart home technology with relevant best practices to help maintain the security of the information that individuals and organizations may store or collect in their smart home devices or in supporting applications
- a demonstration, leveraging commercially available smart home technology, of identification, authentication, and authorization methodologies and capabilities. This worked example would help reduce the barriers for participating smart home device manufacturers to adopt more secure and privacy-preserving configurations

Seeking Public Comment

The NCCoE is seeking comments to help us evaluate the feasibility of realizing these outcomes and suggestions on how NCCoE resources may be able to advance the adoption of sound security principles and best practices relating to the identification, authentication, and authorization of autonomous NPEs in smart homes.

Comments may be made public. If you wish for your comments to remain anonymous, please let us know that when you submit feedback. Comments on this publication may be submitted to IoT-NCCoE@nist.gov or online at nccoe.nist.gov.

[2] https://www.iotivity.org/