Security, Privacy and Identity (SPI) Committee Charter

Introduction

The Internet of Things need interoperable standards from standards development organizations (SDOs) like the IETF and other organizations. This is ongoing: SDOs are today developing new IoT protocols and standards for Internet-Protocol Suite communications, managed network services and interoperation with non IP networks and devices. Ready-to-deploy IoT technology standards are rare, particularly when uniting IoT devices and gateways to cloud and mobile computing.

The SPI committee considers challenges of secure interoperation of authorization, authentication, privacy, integrity and confidentiality services with IP smart objects and object lifecycles. We are ambitious and hope to help improve security and privacy by promoting best practices to the IoT industry.

Problem Statement and Goals

1. Sometimes, an SDO publishes a standard with a large number of deployment options that are TBD. Users of IP smart objects need to determine who can do what across multiple IoT services, platforms and device providers. The SPI committee addresses IoT cross-domain authorization and interoperability challenges by publishing security policy profiles for multiple IoT standards and implementations.

2. Sometimes, SDOs publish standards that lack needed functions. IPSO member companies that move to using message-level signing and encryption, for example, are looking for key management solutions at the message level rather than at the connection level. New key management standards are needed for IoT message signing and encryption. IPSO security and identity will identify interoperable solutions in future plugfests or hackathons.

3. Internet technologies, largely, originated from web infrastructure deployed on very capable smartphone, PC and server platforms. Hence, there often is little attention given to rethinking security for constrained platforms that are the roots-of-trust for the Internet-of-Things. The SPI committee identifies and defines security, privacy and identity best practices for adapting IP smart object technologies to constrained platforms.

4. Sometimes, SDOs presume deployments consisting exclusively of the SDOs specifications ignoring heterogeneity resulting from deployments of competing standards. The broader objective of the IPSO Alliance is to address these challenges; the SPI committee will provide analysis of the security of IPSO work products.

Deliverables

Description	Due Date
IoT roots-of-trust white paper	Q1'17
Cross-domain security policy profiles	Q1'17
Message level signing, encryption and key management white paper	Q1'17
Privacy best practices for IoT white paper	Q1'17
IoT meta-model security, privacy and identity analysis	Q2'17