Analog Devices' Comments
on Fostering the Advancement of the Internet of Things

Docket No. 170105023–7023–01

Analog Devices (NYSE: ADI) is pleased to present the following recommendations and supporting comments to the Department of Commerce (Department) on its recent publication, *Green Paper: Fostering the Advancement of the Internet of Things.* We have also provided a brief overview of our company and our active role in cultivating a secure future for the Internet of Things (IoT) and the associated Identity of Things.

Introduction

ADI commends the Department's focus on the growing importance of technologies that comprise the Internet of Things (“IoT”) and its efforts to seek input from industry partners on both the benefits and challenges of building a secure IoT. This will ensure operational and national security resiliency, enable a new generation of value creation, and support economic, environmental and security objectives.

Analog Devices (ADI) is the world leader in the design and manufacture of analog, mixed-signal, and DSP integrated circuits used in all types of electronic equipment, industrial and commercial products and public and private infrastructure systems. ADI’s technologies enable the interpretation of the world around us by intelligently bridging the physical and digital domains with unmatched technologies that sense, measure and connect. For over 5 decades, ADI’s innovative engineers and dedicated teams have been helping customers and partners know more about their physical worlds, which is central to many of ADI's offerings today and in the future. Because ADI leadership is deeply aware of the threats, challenges, and opportunities of the cyber-physical phase of the digital revolution, we are dedicated to working with the Department.

Recommendations

ADI strongly supports the Department’s efforts support stable, secure, and trustworthy IoT environments. To accomplish that objective, ADI recommends that the Department:

1. Greatly enhance its discussion on the importance of identity instantiation, identity authentication, and identity access management (IAM) as critical aspects of cybersecurity associated with the IoT and IoT devices;
2. Expand the scope of these discussions technically to include the potential for a hardware root of trust that extends to the farthest reaches of our growing digital networks, the sensors themselves; and
3. Encourage and support industry innovation in leap-ahead identity instantiation, identity authentication, and IAM technologies to include hardware intrinsic identity, keyless authentication methodologies, strong encryption,support for anti-tamper detection, and side-channel attack resistance[1].

Supporting Comments

1. ***Identity is a major attack vector for the IoT***

The dynamic environment of the IoT, along with a 10-20 year lifecycle of IoT devices, paints a very different threat landscape than a traditional IT enterprise environment. The shift from content centric architectures to connectivity centric architectures and systems of systems creates an environment where it is no longer possible to define the perimeter (boundaries) or control the connections and data paths. In this ecosystem, traditional security methods are no longer economically viable or effective. We must secure the endpoint intrinsically and avoid assigned identities that are easily compromised and implement architectures that are cost effective and more risk tolerant.

The concept of the "IDENTITY of Things" is emerging with IoT and it is possible to create outcomes based on the trusted data. Having intrinsic identity or hardware based at the endpoints makes this concept of IoT inherently possible.

2. ***Current solutions will not scale and are woefully inadequate to support the emerging IoT environment***

Utilizing traditional IT assigned identity methodologies in an IoT environment results in a sub-optimal security posture and will create an attack vector that is as easily compromised as it is today. According to Verizon's *2016 Data Breach Investigations Report*, 63% of confirmed data breaches involved weak, default, or stolen passwords.

Current authentication techniques typically use one of three forms of identification to

[1] A side channel attack is an attack that uses auxiliary information about a cryptographic system to extract static sensitive information about an entity that can be exploited. For example, both electromagnetic radiation and power consumption by a device performing cryptographic operations have been demonstrated to reveal information about the device's private key. Each time a static value is used by the device, an adversary observing the device learns additional information about the value. Over time, the information leaked about the private key accumulates and the adversary is able to recover the private key.

authenticate a user. The three types are:

1. Something that is known by a user (e.g., password, pin, or personal data)
2. Physical characteristic of the user (Biometrics, such as fingerprint or iris patterns)
3. Something the user physically has (e.g., a PKI identity token or digital certificate).

Attacks capable of exploiting each of these techniques exists; hackers are able to spoof the authentication system into thinking a valid user is present at the remote end instead of the hacker. Passwords are usually the easiest form of authentication to attack. Systems attempting to increase security will typically request larger and more complex passwords of its users. This makes it more difficult for a user to remember. To remember these complex passwords, users may write down their passwords, making it easy to extract their identity. Even systems with enhanced security have been exploited, particularly if they have little resiliency and store all sensitive data in a single location.

Biometric authentication is a powerful method for establishing user identity. Accordingly, Biometrics are becoming more commonplace in the mobility marketspace as sensors become less expensive and smaller, and have improved physical characteristics extraction algorithms. However, the increased use of biometric sensors and some key limitations have also increased the number and types of attacks on them. Most of the current biometric readers can be fooled with just a simple photocopy of a fingerprint, while others have been attacked using gummy bears and gelatin/latex copies of the finger.

Since biometrics authentication is done by comparing biometric data against an ‘enrolled’ digital representation of biometric data, the stored data and even raw digital biometric data are sought after to use with various replay attacks. Eavesdropping adversaries may observe the output of biometric scanners to launch replay attacks, as the origin of biometric scan data is not guaranteed to originate from a valid sensor. Therefore, users are often hesitant to entrust entities with their biometric characteristics. If revealed, revocation is problematic due to the immutable nature of biometrics.

Identity tokens and digital certificates are typically used to authenticate an individual through possession of the token. Theft of the token transfers “identity” to whoever possess the token or certificate.

Accordingly, using traditional IT methodologies of assigned identity introduces significant management complexities, expense, and risk of compromise that is incongruent with IoT models. Assigned identity and its management, (to include secure storage, database management, and policy enforcement) presents a scalability issue across billions of devices communicating wirelessly with each other. The distributed, diverse, and often wireless nature of IoT devices (i.e., without physical boundaries), along with orders of magnitude more connected devices, exacerbates existing vulnerabilities.

In addition, other basic security protections like secure boot and secure upgrade are currently non-existent or not fully implemented to provide a solid security posture that will span the expected extended lifecycle of IoT devices.

3. A hardware root of trust is required for a secure IoT environment

Less complex, more robust security frameworks based on hardware root of trust of IoT devices must be developed. A hardware root of trust creates its security posture by designing secure functions into the hardware elements themselves. While this is not a silver bullet, intrinsic identity at the edge compliments big data, analytics, and artificial intelligence in such a way that a multi layered architecture using identity as a foundational element is needed.

From ADI's perspective, secure identity must extend to the edge of the IoT, at the silicon, where the physical to digital connection occurs. This represents the highest security with the smallest attack surface and has the potential to address many of the performance constraints -- power, processing and memory -- that limit the ability of software based identity solutions to function at the edge. Ideally, these solutions would be keyless and eliminate the costs and complexity associated with asymmetric key management and policy governance and enforcement for billions of devices.

A hardware root of trust approach will also shift the existing cyber economics paradigm. As discussed above, traditional architectures have "break one break all" vulnerabilities that provide the attacker with economic advantage. In architectures using endpoint hardware based identity, the adversary must capture the hardware and can only compromise one point. This not only increases costs to the attacker but makes it much more difficult for them to succeed.

Unless the community evolves towards a new hardware based root of trust for identity, ADI is concerned that the greater potential of IoT will be limited. Accordingly, ADI recommends that the Department encourage industry to invest in leap ahead IAM technologies that offer a less complex, more scalable approach to providing the necessary level of trustworthiness in the data that inform real time, often life-critical, decisions (i.e. autonomous vehicles, medical devices).

Innovative Identity Instantiation, Identity Authentication and IAM technologies is a means to address this problem in a scalable, less complex fashion to provide the necessary:

1. Secure Data Management, protection of privacy and adherence to rules for data exchange;
2. Data Integrity and Authentication maintained at all stages of Collection, Analysis, Exchange and Storage; and

3. Trust in the data that these systems produce so that the full power of these new sources of information, intelligence and impact can be sold, traded or shared as widely as goals demand.

Establishing a capability for end-to-end trust (from sensor to cloud) anchored with identity at the edge provides a basis from which data integrity is derived, data is securely and accurately managed/accessed/stored, and data source attribution is achievable. In addition, establishing a high pedigree intrinsic identity and IAM policy applies broadly throughout the IoT functional stack and spans a myriad of industry verticals and stakeholder interests. Examples include:

1. The technology development of Identity, Identity Authentication, and IAM solutions to enable virtually any connected device to instantiate identity in such a way that enables identity mapping for authorizations, public/private data sharing, and privacy protections, to include:
    a. Device owner identity – with full access to all data, including IP-protected closed data
    b. Infrastructure identity - with real-time polling or subscription-based access to defined content
    c. Marketplace identity(ies) – appropriate for any number of marketplaces that are developed
2. The broad application of Identity, Identity Authentication, and IAM capabilities provide a common construct/architecture to support the agile distribution of management functions to their optimal location to include:
    a. A broad collection of installed and to-be-deployed sensors, and edge nodes
    b. Private customer premises intelligent gateways/ data collectors/aggregators/ servers/ policy managers
    c. Public sector premises intelligent gateways with robust policy management, preprocessing, and selected advanced/ deep processing capabilities – sense-making
    d. A foundation for advanced DRM (Digital Rights Management) support for individual sensor data optimization: core/ primary functions, public/private access, and data exchange.

Conclusion

The true value of the IoT will only be realized through incorporation of the broadest range of infrastructure, analytics and application enablement, and service creation entities. To achieve this, a hardware root of trust identity-enabled architecture is essential. In that spirit, ADI recommends that the Department:

1. Increase its emphasis on identity instantiation, identity authentication and IAM

technologies and address the need for stronger identity at each and every level of the equally complex legacy and 'state-of-the-art' IoT solutions;

2. Expand the scope of these discussions to technically to include the potential for a hardware root of trust that extends to the silicon, where the physical to digital connection occurs; and
3. Encourage and support industry innovation in leap-ahead identity instantiation, identity authentication, and IAM technologies to include hardware intrinsic identity.