Analog Devices' Comments on:
Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

Docket No. Docket Number: 170602536-7536-01

Analog Devices (NYSE: ADI) appreciates the opportunity to provide recommendations and supporting comments to the National Telecommunications & Information Administration (NTIA) Request for Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats.

ADI's comments are informed by its experience as 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, including the threats posed by botnets and other automated threats, we are dedicated to working with the NTIA.

As discussed below, ADI recommends that all stakeholders invest in significantly strengthening identity instantiation, identity authentication and identity access management (IAM) as a mechanism for reducing threats from automated distributed attacks such as botnets. To be truly effective in an IOT environment, ADI further recommends that the US Government encourage industry innovation in leap ahead IAM technologies to include hardware intrinsic identity that extends to the farthest reaches of our growing digital networks, the sensors themselves, and keyless authentication methodologies.

Weak Identity and Access Management is an attack vector exploited by botnets and other automated threats

Current IAM methods, based on assigned identities, provide suboptimal protection against unauthorized access that allow an adversary to take over a device and modify its functionality. In the IOT context, many systems use standard default usernames and passwords that are identical for every device and are often not changed by the device owner. These devices generally do not contain identity primitives and cannot be uniquely identified and managed. The vulnerable usernames and passwords combined with the lack of a unique identity, make these IOT devices and easy targets for botnet exploitation. Anyone that can connect to the device can control it. Once connected, an adversary can inject software changes that allows them to spoof the device's data, make the device spoof other device's data, and redefine the

device's functionality.

If both the device and the controlling server had a cryptographically strong identity and utilized mutual authentication, adversaries would be prevented from gaining access and control of such devices.

Current IAM solutions are woefully inadequate to reduce threats from botnets and other automated threats, particularly in 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 2017 Verizon Data Breach Report 81% of hacking-related breaches leveraged either stolen and/or weak passwords. The inefficiency of assigned identities also spreads to other authentication methods.

Current authentication techniques typically use one of three forms of identification to authenticate a user. The three types are:

- Something that is known by a user (e.g., password, pin, or personal data);
- Physical characteristic of the user (Biometrics, such as fingerprint or iris patterns); and
- 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 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.

In addition, key management of existing IAM is complex, costly, and difficult to scale. If we continue to follow today's methods of assigning identity to the device, then every supplier that touches the device components must implement security controls and key management methods. In a typical device, life cycle security controls and key management processes must be implemented at the silicon manufacturer, board assembly manufacturer, device assembly and customer sites. This provides a large attack surface for the adversary and does not scale well into the high volume IoT market.

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, often wireless nature of IOT devices (i.e., without physical boundaries), and volume of connected devices, exacerbate existing vulnerabilities. Moreover, other basic security protections like secure boot and secure upgrade are currently non-existent or not fully implemented and are therefore unable to provide a solid security posture that will span the expected extended lifecycle of IoT devices.

In contrast, a device with identity and a hardware root of trust (and proper secure boot implementation) would provide a strong security posture, with device identity and integrity checks. Since the device can support a cryptographically strong authentication, the device owner or installer does not need an assigned identity such as a static user-name and password. The device itself can authenticate into the system. In addition, the data flowing from the device can include hardware level identity and integrity checks. This means that even if an adversary compromises the higher level software system, they will be unable to gain full control of the device. If the higher level software tries to modify the data, the identity and integrity checks on the modified data will fail, alerting the higher level IAM system that the device has been compromised. In addition, the hardware root of trust can include integrity checks on the software image, allowing it to detect and alert the IAM system of any unauthorized software modification.

IAM solutions that leverage a hardware root of trust with minimal key management are required to eliminate risk from botnets and automated threats, particularly in an emerging IOT environment

Less complex, more robust security frameworks based on a hardware root of trust for IOT devices must be developed. A hardware root of trust creates its security posture by designing secure functions into the hardware elements themselves that is leveraged up the stack. While not a silver bullet, this change in paradigm will allow security to scale into the IoT market and complements advances in big data, analytics, and artificial intelligence. In addition, a hardware root of trust reduces the attack surface and complexities of assigning identity at all the different stages of the device lifecycle. The IoT devices can just leverage the silicon identity into their security posture and eliminate handling and assigning keys.

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.

ADI therefore recommends that the United State Government encourage investment in leap ahead IAM technologies that offer a less complex, more secure, and more scalable approach in order to reduce the impact of botnets and other automated threats. 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.