



NCSIP Position Paper

The Internet of Things (IoT) – Safety, Security and Opportunity

Prepared on behalf of NCSIP with input from Committee Members by

Robert Samuel/Nova Scotia

2018-01-15

INTRODUCTION

The term Internet of Things (IoT) is used to describe a network of physical devices that are capable of sensing, communicating and exchanging data. IoT devices capture, analyse and either make decisions on our behalf (e.g. self-parking cars and lane departure assist) or provide us with information to make decisions (e.g. blind spot warning systems) based on data and have further interconnected the physical and digital worlds. IoT devices are everywhere including aircraft, cars, medical equipment, industrial control systems, traffic lights, security cameras, smartphones, wireless locks, thermostats, televisions, baby monitors and fitness trackers to name a few.

Unfortunately, IoT devices are often built and implemented with limited or no security as manufacturers look to bring products to market as quickly as possible. As a result, IoT introduces a myriad of new attack vectors and this combination of factors can cause harm to both the end users of IoT devices and third parties that may become victims of unsecured IoT. Some notable examples that have occurred over the past few years include [Mirai, an IoT botnet](#) (robot network) consisting of ~ 500,000 consumer IoT devices such as wireless routers and baby monitors that were unsecured, ultimately infected, controlled by hackers and used to cause a major Internet outage and the identification of potentially life-threatening vulnerabilities in pacemakers, insulin pumps and other medical devices.

NCSIP POSITION

In August 2017, four US senators introduced bipartisan legislation to improve the cybersecurity of Internet-connected devices. Titled “[The Internet of Things \(IoT\) Cybersecurity Improvement Act of 2017](#)”, the bill aims to ensure due care by vendors who supply devices to government to address basic security requirements such as producing devices are patchable, have passwords that can be changed, do not contain known security vulnerabilities, etc.

The number of IoT devices is forecasted to grow to over 20 billion by 2020 and NCSIP believe that a similar approach of legislation and regulation are required to ensure that safety and security are considered throughout the life-cycle of these capabilities and to ensure manufacturers are enticed to develop secure products that can be adequately maintained and secured. As the digital world increasingly converges with the physical world, regulated industries are being transformed (e.g. automotive, transportation, health, etc.) and overarching regulation is needed to ensure security-by-design as devices that were formerly disparate now connect and communicate via the IoT ecosystem.

The same IoT systems that enable vehicles to self-park or to stay between the lines on a road can also be vulnerable to attack and manipulated with false information. This has been repeatedly demonstrated over the past several years, including in 2016 when a team of [researchers successfully implemented remote control on Tesla Model S](#) in both Parking and Driving Mode and in 2017 when the Department of Homeland Security’s Cybersecurity Division revealed that their security researchers [remotely hacked a Boeing 757](#). Mirai was not an isolated incident



and a new IoT botnet referred to as “[IoTroop / Reaper](#)” has been identified and continues to self-propagate across the world via vulnerabilities in unsecured IoT devices.

These examples highlight the reality that IoT and systems of systems connectivity that are implemented without adequate security controls can result in catastrophic consequences including the loss of life and reiterate that safety and security must be mandatory considerations and requirements moving forward. As more physical devices become connected to the Internet, cybersecurity has become just as important as traditional safety features such as seatbelts and airbags.

As noted within the United States Government Accountability Office Technology Assessment, without proper safeguards, these systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain and manipulate sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The threat is substantial and increasing for many reasons, including the ease with which intruders can obtain and use hacking tools and technologies.¹

RECOMMENDATION

NCSIP members agree that the IoT ecosystem requires overarching government oversight as it spans multiple sectors, industries, and consumers yet imposes cybersecurity challenges, privacy implications and safety concerns.

We recommend the following actions be considered:

- Understand the threat that IoT devices pose to organizations due to the sharp increase in adoption and attacks compared with the low or non-existent security controls in place
- Pursue legislation and/or regulation to ensure that safety and security are considered throughout the life-cycle of IoT capabilities and to ensure manufacturers are enticed to develop secure products that can be adequately maintained throughout their life cycle;
- Update procurement processes to treat traditional devices that now come embedded IoT connectivity (e.g. appliances, televisions, security cameras, locks) as computers to ensure rigor around the procurement, implementation, operations and management of IoT;
- Ensure cybersecurity teams are engaged early, in advance of procurement of any Internet or IoT enabled devices, to ensure basic security requirements can be met and to perform supply chain integrity checks;
- Segment and isolate IoT devices based upon their business purpose and function (e.g. establishing a dedicated virtual LAN for security cameras, etc.);
- Implement standards to ensure that IoT devices are implemented securely (e.g. changing default passwords, disabling unneeded features and functionality, etc.);
- Establish and participate in IoT initiatives such as research and development, spectrum use and economic opportunities that will result in exponential IoT growth; and
- Review the [US Government Accountability Office – IoT Technical Assessment](#) for a detailed breakdown of IoT.

NCSIP requests PSCIOC’s assistance to implement these recommendations.

¹ <http://www.gao.gov/assets/690/684590.pdf>