CA TECHNOLOGIES | Business rewritten by software

# Comments on Promoting Stakeholder Action Against Botnets and Other Automated Threats

*Prepared for:*

## National Telecommunications and Information Administration

Attn:  Evelyn Remaley, Deputy Associate Administrator
National Telecommunications and Information Administration
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230
counter_botnet_RFC@ntia.doc.gov

CA Technologies Point of Contact:
Jamie Brown
Director, Global Government Relations, CA, Inc.
Jamie.Brown@ca.com

# Table of Contents

Introduction: 1

Section 1: Secure Software Development 1

Section 2: API Management 3

Section 3: Identity and Access Management 4

Section 4: Embracing IoT as Part of a Complete Approach 4

Section 5: Security Gaps and Industry/Government Policy Opportunities 5

Conclusion 6

# Introduction

CA Technologies appreciates the opportunity to provide comments in response to the Request for Comment (RFC) issued by the National Telecommunications and Information Administration (NTIA) on June 13, 2017 regarding actions that can be taken to address automated and distributed attacks to the digital ecosystem as part of the activity directed by the President in Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." CA Technologies is a global leader in software solutions enabling customers to plan, develop, manage and secure applications and enterprise environments across distributed, cloud, mobile and mainframe platforms. A majority of the Global Fortune 500, as well as many government agencies around the world, rely on CA to help manage their increasingly dynamic and complex environments.

The RFC requests information on both attack mitigation and endpoint prevention. In this response, CA Technologies highlights the role software can play in both preventing and mitigating automated, distributed attacks. In addition, the response discusses industry best practices, identifies gaps that can be addressed, and provides policy recommendations.

# Section 1: Secure Software Development

Applications are increasingly integrated into our commercial and infrastructure processes to improve efficiencies. But this makes them a prime target for hackers. The global economy, critical infrastructure and government operations have increased their dependence on software.

The recent WannaCry and Petya ransomware attacks culminated in hundreds of hospitals, retail outlets and critical infrastructure being breached. They impacted commerce as well as patient care and innovation, demonstrating how an attack in the digital world can have an alarming and lasting impact on the physical world.

While the importance of software has increased, the way software is developed and deployed has continued to evolve. In addition to the importance applications play in our economy, contemporary application development methodologies like DevOps (combining development and operations practices) are increasing the speed and precision with which software is produced and deployed. The ability to create software that can resist modern forms of attack and exploits will be crucial to our ability to protect not just applications, but the social, economic and political processes that depend on that software.

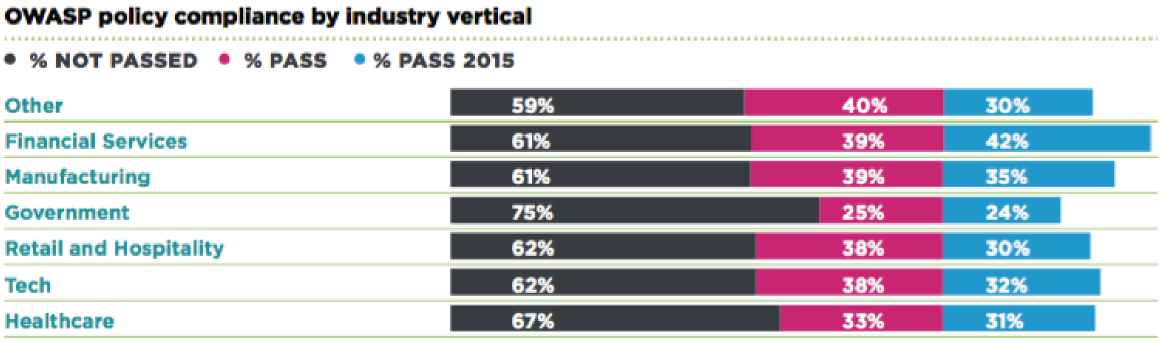
CA Technologies recently acquired Veracode, a leading provider of application security solutions and services.

Data from Veracode's 2016 State of Software Security (SOSS) Report[1] demonstrate the pervasive risk of software security. For example, the frequent use of software components speeds up development, but also increases risk. In the past, vulnerabilities were isolated to the single application in which they resided, requiring hackers to create an exploit that targeted only one application. Today, the widespread use of components means a vulnerability in a single component can reach thousands of applications – so a hacker must only create one virus or program to

[1] https://www.veracode.com/sites/default/files/Resources/Reports/state-of-software-security-volume-7-veracode-report.pdf

breach thousands of applications and potentially millions of companies. Examination by Veracode of a critical vulnerability in a single component found that the component and thus the vulnerability was present in more than 80,000 applications. These applications were then used by thousands of companies – all of them now exposed to hackers.

It isn’t only components increasing risk. The SOSS Report also found that applications in industries including healthcare, tech and government institutions as well as financial institutions are not complying with commonly accepted security guidelines, as outlined by OWASP (Open Web Application Security Project).[2] The graph below shows the pass rates of applications tested for vulnerabilities broken out by industry.



Much software remains insecure in part because many development teams view security as a separate function from software quality. Many organizations fail to integrate security methods into their development lifecycle.

Organizations that follow best practices make security an element of quality, conducting security testing and performing other secure development practices throughout the development lifecycle.

CA Technologies utilizes a secure software development lifecycle process to minimize vulnerabilities in its software. As part of this process, CA utilizes a mix of education, threat modeling, architectural risk assessment, code scanning and analysis, penetration testing, and continuous tracking of known vulnerabilities and attack vectors.

CA is a board member of SAFECode (the Software Assurance Forum for Excellence in Code)[3], which is dedicated to increasing trust in information and communications technology products and services through the advancement of effective software assurance methods.  SAFECode develops software assurance guidance publications available for free to the public, outlining software development best practices for developers and organizations.  For instance, the SAFECode publication, “Fundamental Practices for Secure Software Development, 2nd Edition,”[4] is designed to help others in the industry initiate or improve their own software security programs and to encourage the industry-wide adoption of fundamental secure development methods. Another SAFECode publication, “Principles for

[2] https://www.owasp.org/index.php/Main_Page
[3] https://safecode.org/
[4] https://www.safecode.org/wp-content/uploads/2014/09/SAFECode_Dev_Practices0211.pdf

Software Assurance Assessment,"[5] helps software customers assess the software assurance practices of their suppliers.

SAFECode members have endorsed the following principles for promoting effective software security development practices:

- Software development is an organizational commitment and a holistic process;
- There is no one-size-fits-all approach to software assurance;
- Despite differences, common secure development practices shared across the industry have proven both practical and effective;
- Providing more transparency in software assurance processes and practices helps customers and other key stakeholders manage risk effectively;
- Contributing information about members' own security processes and practices supports SAFECode efforts to advance software assurance and positively impacts the security and reliability of the technology ecosystem; and
- Software assurance training should become a required part of any software engineering training program.[6]

## Section 2: API Management

Application Programming Interfaces (APIs) manage the connections between applications, data and devices. Broadly speaking, APIs make it possible for organizations to open their backend data and functionality for reuse in new application services. Organizations and governments that leverage open APIs can realize significant data-driven value creation.  However, these APIs also represent significant attack vectors for malicious actors.  Therefore, API security and management are key components of IoT and application security.

This need for strong security can conflict with a basic goal of API design—a well-designed API makes it easy for developers to create apps that provide seamless access to enterprise resources. Strong security is likely to impact this ease of access.  Deploying security in a centralized API architecture (rather than in the API implementation) through an API Gateway will help mitigate this impact, as will enabling the use of flexible access management technologies like OAuth[7] and OpenID Connect.[8]

Automated client registration and secure channel creation requires no specific implementation of security protocols by the app developer, but results in an end-to-end protocol and data-level security posture.  API management solutions can be configured to provide end-to-end security between the client and secure data (including dynamic secure data storage on mobile clients), as well as protecting against many web-based threats and OWASP vulnerabilities.

[5] https://www.safecode.org/publication/SAFECode_Principles_for_Software_Assurance_Assessment.pdf
[6] https://safecode.org/safecode-principles/
[7] https://oauth.net/
[8] http://openid.net/connect/

## Section 3: Identity and Access Management

Identities constitute the new security perimeter and are the single unifying control point across all apps, devices, data and users.  Identity and access management software authenticates individuals and services and governs the actions they are permitted to take.  API management software authenticates devices and data and is fundamental to securing the IoT.  API management software also secures and protects the APIs themselves from threats, and ensures authorized access to the APIs by the approved apps and individuals.

The 2017 Verizon Data Breach Investigation Report[9] shows that 81 percent of all hacking-related breaches are caused by compromised password credentials.  Adversaries gain access to credentials through phishing attacks and other methods, and continuously seek ways to heighten their privileges within an organization.  Attackers who gain access to credentials of privileged users can perpetrate extremely harmful attacks against organizations that lack access management controls to mitigate the breadth and depth of these attacks.

Privileged Access Management solutions provide the visibility, monitoring and control needed for those users and accounts that have the 'keys to the kingdom.' One of the most important areas of IT risk relates to privileged users. Whether inadvertent or malicious, improper actions by privileged users can have disastrous effects on IT operations and the overall security and privacy of organizational assets and information. Therefore, it is essential that administrators be allowed to perform only those actions that are essential for their role—enabling "least privileged access" for reduced risk. This visibility provides insight on activity and works to prevent or flag anything unusual that indicates security risk.  Further, organizations can leverage threat analytics to continuously assess risk and detect malicious activity though analysis of contextual and behavioral factors, such as geolocation and unusual administrative activities.

## Section 4: Embracing IoT as Part of a Complete Approach

Automated, distributed attacks will become an increasing challenge as the number, diversity and criticality of intelligent devices continue to increase. While the Internet of Things poses specific challenges for security, it's important to understand that these devices are part of a more complex system encompassing smart devices, mobile applications and back-end web services, often connected to multiple third-party providers who add value or unique services. As such, protecting IoT devices is best thought of as an extension of security practices for our 'existing' digital infrastructures. In fact, we can expect that not only will IoT devices continue to be co-opted and used as part of larger automated attacks, but that attacks on our existing digital infrastructures will increasingly be carried out with intelligent devices as the primary vector of access into our most critical digital systems. In this regard, the three domains of security discussed above gain increasing importance:

- Secure Software: IoT devices will remain difficult to patch or upgrade with any degree of consistency, meaning the quality and security of the software that runs them should be ensured from 'first ship'. Since it is difficult to patch or upgrade many IoT devices, it is important to implement 'secure by default' settings,

[9] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

and for the devices to only include the components, features and protocols required to perform the tasks for which they are designed. Further, any IoT patch mechanism must have robust security to ensure it isn't hijacked by a malicious user, and used as a botnet. Finally, the back-end websites and mobile apps that support and run these intelligent devices must be resistant to exploits to ensure that the devices themselves are not compromised.

- Identity Management: As intelligent devices gain more capability and connectivity, especially through application of machine learning and similar techniques, it will become increasingly difficult to distinguish devices from human or connected systems. Thus, the ability to ensure controlled access to devices and through these devices to other systems becomes more essential; identities online will increasingly be machines, not people, and the ability to ensure trusted access to and by those machines must be part of any security strategy.
- API Management: These devices gain much of their value through their connected nature and the ability of companies to build ecosystems around their devices as Amazon is doing with its Alexa personal assistants. These ecosystems depend on powerful APIs to expose a dizzying array of functionality that third party companies can use to add new services and value to existing ecosystems such as Alexa. The security and robustness of those APIs must be maintained as they are a powerful tool for exploit if they are insecurely designed or deployed.

# Section 5: Security Gaps and Industry/Government Policy Opportunities

A key gap in effective information security, including security to prevent and mitigate distributed and automated attacks, are the competing incentives for rushing a new product or solution to market and for incorporating security into the development of software and devices. As a result, too many organizations fail to incorporate the security development best practices outlined earlier in this response.

The Department of Commerce can play a key role in promoting industry best practices for secure software and hardware development. SAFECode can serve as a key resource to the Department of Commerce in promoting these best practices. Industry stakeholders can develop their own software assurance processes, consistent with the SAFECode principles outlined above. However, industry should be expected to commit to following these practices.

Currently, there are ongoing standards development efforts to enable independent verification of software security assurance best practices, such as the emerging ISO/IEC 27034 standard.[10] However, these efforts generally apply to larger development organizations. CA Technologies recommends that NIST work with industry and other stakeholders to develop best practices for organizations that develop applications and devices with limited functionality. These practices can be applied by small and startup organizations that are looking to break into the market, and can include different levels of security controls and practices based on the functionality of the applications and devices they develop as well as the degree of risk they pose to broader networks and systems.

[10] http://www.iso27001security.com/html/27034.html

Public private partnerships, and stakeholder driven processes remain a strong means of developing effective best practices and approaches. CA believes the Federal government should continue to support the multi-stakeholder process, driven by the NTIA, on IoT Security Upgradability and Patching.[11] The NIST Cyber-Physical Systems Working Group[12] has also played a key role in developing IoT security guidance.

In addition, the IT Sector Coordinating Council, of which CA Technologies is an Executive Committee member, is working with the Department of Homeland Security, the General Services Administration, and the Department of Commerce to develop IoT security procurement guidance for Federal agency acquisition of IoT devices and services.

CA Technologies recommends that any government or policy guidance focused on prevention and mitigation of automated and distributed attacks recognize the wider information security ecosystem, including identity, application and transaction security. Along these lines, the guidance should incorporate authentication and access management best practices, including authentication of devices and access management for privileged users. The NIST Trusted Identities Group and the National Cybersecurity Center of Excellence can play key roles in this space.

On the regulatory side, there is significant risk that global governments and US Federal regulatory agencies will develop multiple, distinct and overlapping compliance regimes around security to prevent automated, distributed attacks, particularly with respect to IoT. This policy fragmentation can force organizations to dedicate scarce resources towards multiple compliance exercises and away from innovation and development, or can provide a disincentive to compete in certain markets, limiting competition.

The Department of Commerce can help lead inter-agency IoT security policy alignment initiatives, and can also work with global government partners to promote policy alignment, tied to international, consensus standards, where possible. The NIST Cybersecurity Framework development process serves as an excellent model for this work.

# Conclusion

Automated and distributed attacks have increased significantly in recent years, both in terms of scope and destructive capabilities. While there are a range of technologies and solutions available to combat these threats, prevention remains the best way to limit their damage. Software hygiene and secure software and hardware development practices are paramount in addressing this challenge. However, mitigation of IoT-based attacks remains critical as well. API security and authentication and access management are key components to improving the security of the broader IoT ecosystem.

Industry forums such as SAFECode, and public private partnerships including NIST and NTIA multi-stakeholder processes, can provide actionable guidance and best practices to further reduce the impacts of these threats.

Deploying state of the art technologies, and promoting the use of these best practices, especially among smaller organizations, will strengthen our resiliency against automated and distributed attacks. CA Technologies welcomes

[11] https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security
[12] https://www.nist.gov/el/cyber-physical-systems

the opportunity to partner with the Federal Government and other industry partners to address this challenge, and to enable continued growth of the digital economy.