REQUEST FOR COMMENT RESPONSE

Call for Papers on Cybersecurity Labeling Programs for Consumers: Internet of Things (IoT) Devices and Software

August 17, 2021

I. INTRODUCTION

In response to NIST's call for public papers on cybersecurity labelling programs for consumers, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

Executive Order ("EO") 14028 requires NIST to initiate two labeling efforts regarding Internet-of-Things ("IoT") devices and software development practices. CrowdStrike commends NIST for undertaking these efforts in a deliberate and consultative manner.

Call for papers - scope note

We understand that the IoT initiative is deliberately scoped to focus on better informing consumers and providing more clarity in the consumer marketplace. However, some of our comments reflect and/or acknowledge that IoT devices primarily designed for consumer use frequently end up serving enterprises. For example, throughout the COVID-19 pandemic, many organizations bought and integrated consumer webcams and microphones for remote workers. Traditional physical office spaces also increasingly include smart appliances or smart monitors/TVs. Therefore, we suggest NIST develop a scheme that is straightforward enough to inform individuals yet comprehensive enough to assist decision making within enterprises. As a practical matter, this may simply mean including detail about a few additional enterprise-focused use cases, such as the ability to integrate with third-party security providers.

Q1. Formal and informal processes and practices used to secure the software development process

As CrowdStrike CEO George Kurtz noted in a recent Senate testimony, "[i]n addition to ensuring secure coding practices and adequate code review, organizations must protect their development platforms and code repositories at least as well as their enterprise environment. In practice, this means that beyond the other security concepts" like threat hunting, endpoint detection and response (EDR) technologies aided by AI/ML, and extended detection and response (XDR) solutions, "...organizations must incorporate secure implementation of both hardware and software, conduct architecture reviews, deploy code signing via tamper resistant hardware, engage in ongoing monitoring, and regular testing. Fortunately, the security community has been focusing on these issues, and we commend the National Institute of Standards and Technology (NIST) for their significant and ongoing contributions to this area."[1]

Q2. Technical criteria needed to support validation of consumer software security assertions that reflect a baseline level of secure practices

While we cannot suggest a full set of criteria at this time, we note that some current efforts to this end appear overly constrained to devices themselves. A more comprehensive depiction would include both the device and supporting infrastructure--frequently a cloud environment. Notably, cloud backends may be among the most attractive parts of IoT attack surface to certain types of threat actors. Therefore, cloud security posture is a particularly relevant area of inquiry.

Further, as noted above ("scope") one relevant criteria that may be overlooked with consumer IoT solutions is the ability to support or integrate with third party security providers.

Q3. How different conformity assessment approaches (e.g., vendor attestation, third-party conformity assessment) can be employed in consumer software labeling efforts

In general, we advocate for the use, wherever possible, of real- or near-real time depictions of security posture. Attestations and other compliance-based measures can help establish a floor for the security maturity of a given vendor/provider, and this correlates with stronger security outcomes, including breach detection and remediation. However, point-in-time representations about security have a number of weaknesses, so schemes that support real-time representations are preferred. Ultimately, efforts should incentivize the implementation of methods, interoperability options, and inherent safeguards that strengthen overall security for the lifetime of a given device.

III. CONCLUSION

While IoT security best practices are becoming clearer over time,[2] secure development and implementation practices in the space, as well as transparency measures, still lag behind. Ultimately, IoT adoption rates will increase and attacks will continue to evolve, so now is the appropriate time to strengthen security practices and controls.

The ultimate goal of creating consumer software labeling requirements will require a multifaceted approach, including leveraging the very technologies and security principles highlighted in the EO. In light of recent and ongoing threats, identifying and mitigating software security vulnerabilities is a key part of achieving success.

[1] George Kurtz, Testimony on Cybersecurity and Supply Chain Threats, Senate Select Committee on Intelligence (Feb. 23, 2021), https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary.

[2] What is IoT Security, CrowdStrike Blog, (Mar. 18, 2021), https://www.crowdstrike.com/cybersecurity-101/internet-of-things-iot-security/.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Robert Sheldon
Director, Public Policy & Strategy

Email: policy@crowdstrike.com

***