Bootstrapping Security Configuration for IoT Devices on Networks with TLS Inspection

Submitted by grigby1 on Fri, 07/03/2020 - 1:27pm

Title	Bootstrapping Security Configuration for IoT Devices on Networks with TLS Inspection
Publication Type	Conference Paper
Year of Publication	2019
Authors	Danilchenko, Victor, Theobald, Matthew, Cohen, Daniel
Conference Name	2019 IEEE Globecom Workshops (GC Wkshps)
Date Published	dec
Publisher	IEEE
ISBN Number	978-1-7281-0960-2
Keywords	authorisation, bootstrapping security configuration, certification, chicken-and-egg problem, computer bootstrapping, computer network security, conventional computing devices, cryptography, deep packet inspection, deep packet inspection proxies, DPI policies, DPI proxy CA, DPI proxy certificate authority certificates, DPI-enabled intranets, enterprise management, IIoT devices, industrial enterprise networks, Inspection, Internet of Things, Internet of Things devices, intranets, manual device configuration, Payloads, performance evaluation, Production facilities, pubcrawl, resilience, Resiliency, Scalability, security bootstrapping, typical IoT devices

Abstract

In the modern security-conscious world, Deep Packet Inspection (DPI) proxies are increasingly often used on industrial and enterprise networks to perform TLS unwrapping on all outbound connections. However, enabling TLS unwrapping requires local devices to have the DPI proxy Certificate Authority certificates installed. While for conventional computing devices this is addressed via enterprise management, it's a difficult problem for Internet of Things ("IoT") devices which are generally not under enterprise management, and may not even be capable of it due to their resource-constrained nature. Thus, for typical IoT devices, being installed on a network with DPI requires either manual device configuration or custom DPI proxy configuration, both of which solutions have significant shortcomings. This poses a serious challenge to the deployment of IoT devices on DPI-enabled intranets. The authors propose a solution to this problem: a method of installing on IoT devices the CA certificates for DPI proxy CAs, as well as other security configuration ("security bootstrapping"). The proposed solution respects the DPI policies, while allowing the commissioning of IoT and IIoT devices without the need for additional manual configuration either at device scope or at network scope. This is accomplished by performing the bootstrap operation over unsecured connection, and downloading certificates using TLS validation at application level. The resulting solution is light-weight and secure, yet does not require validation of the DPI proxy's CA certificates in order to perform the security bootstrapping, thus avoiding the chicken-and-egg problem inherent in using TLS on DPI-enabled intranets.

URL https://ieeexplore.ieee.org/document/9024325
DOI 10.1109/GCWkshps45667.2019.9024325
Citation Key danilchenko_bootstrapping_2019

authorisation bootstrapping security configuration certification chicken-and-egg problem computer bootstrapping computer network security conventional computing devices Cryptography deep packet inspection deep packet inspection proxies DPI policies DPI proxy CA DPI proxy certificate authority certificates DPI-enabled intranets enterprise management IIoT devices industrial enterprise networks Inspection Internet of Things Internet of Things devices intranets manual device configuration Payloads performance evaluation Production facilities pubcrawl resilience Resiliency Scalability security bootstrapping typical IoT devices