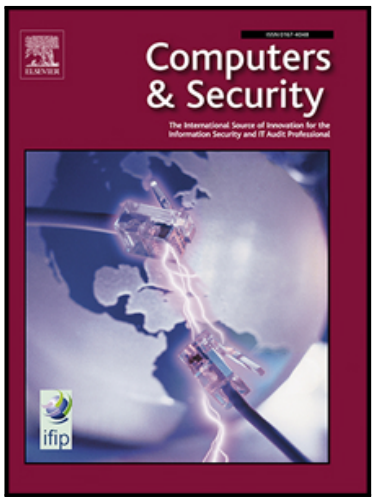
Accepted Manuscript



Another Look at TLS Ecosystems in Networked Devices vs. Web Servers

Nayanamana Samarasinghe, Mohammad Mannan

PII: S0167-4048(18)30691-6
DOI: https://doi.org/10.1016/j.cose.2018.09.001
Reference: COSE 1392

To appear in: *Computers & Security*

Received date: 18 June 2018
Revised date: 11 September 2018
Accepted date: 12 September 2018

Please cite this article as: Nayanamana Samarasinghe, Mohammad Mannan, Another Look at TLS Ecosystems in Networked Devices vs. Web Servers, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.09.001

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Another Look at TLS Ecosystems in Networked Devices vs. Web Servers

Nayanamana Samarasinghe*, Mohammad Mannan

Concordia Institute for Information Systems Engineering, Concordia University, Montreal, Canada

Abstract

High-speed IPv4 scanners, such as ZMap, now enable rapid and timely collection of TLS certificates and other security-sensitive parameters. Such large datasets led to the development of the Censys search interface, facilitating comprehensive analysis of TLS deployments in the wild. Several recent studies analyzed TLS certificates as deployed in web servers. Beyond public web servers, TLS is deployed in many other Internet-connected devices, at home and enterprise environments, cyber physical systems, and at network backbones. In Apr. 2017, we reported the results of a preliminary analysis based on measurement data of TLS deployments in such devices (e.g., routers, modems, NAS, printers, SCADA, and IoT devices in general) collected in Oct. 2016 using Censys. We also compared certificates and TLS connection parameters from a security perspective, as found in common devices against top Alexa sites. Censys has evolved since then and its data volume has increased with the addition of several new device types. In this paper, we perform a similar but more comprehensive measurement study to assess TLS vulnerabilities in devices, and compare our current results with our 2016 findings, showing how such systems have evolved in the last one and half year. Indeed, there are noticeable improvements in the TLS ecosystem for devices, especially in terms of adoption of TLS itself (from 29.4% in 2016 to 73.7% in 2018) and stronger cryptographic primitives. However, we also note the continuity of significant weaknesses in devices for which immediate remediation is warranted (e.g., the use of known private keys, SSLv3, MD5-RSA, and RC4). We have also contacted the top manufacturers of vulnerable devices to convey our findings. Most of them blamed users for not updating their devices with latest firmware images that apparently would mitigate the reported findings.

Keywords: CPS, IoT, SCADA, TLS, certificates, cryptographic primitives

1. Introduction

Beyond user-level computing devices and back-end servers, there are many other Internet-connected devices that serve important roles in everyday IT operations. Such devices include routers, modems, printers, cameras, SCADA (supervisory control and data acquisition) controllers, DVR (digital video recorders), HVAC (heating, ventilating and air conditioning technology), CPS (cyber physical systems), and NAS (network-attached storage) devices. Several past studies have identified critical security issues in these devices, including authentication bypass, hard-coded passwords and keys, misconfiguration, serious flaws in their firmware and web interfaces; example studies include: [1, 2, 3, 4, 5, 6]. The massive DDoS attack on DynDNS as attributed to the Mirai botnet (e.g., [7]), populated by DVRs, IP cameras and other IoT devices, shows the clear danger of security flaws and weaknesses in these devices. Antonakakis et al. [7] argue that the absence of sound security practices in the IoT

*Corresponding author

Email address: n_samara@ciise.concordia.ca (Nayanamana Samarasinghe)

ACCEPTED MANUSCRIPT

Download English Version:

https://daneshyari.com/en/article/11021085

Download Persian Version:

https://daneshyari.com/article/11021085

Daneshyari.com