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)

space leads to a fragile state of its environment impacted by vulnerabilities in devices. The Reaper [8] IoT botnet appears to be more severe than Mirai, as Reaper is capable of exploiting numerous device vulnerabilities, as opposed to Mirai's rather simple albeit effective exploitations of default credentials; see also [9].

Over the years, manufacturers of networked devices have implemented some security mechanisms, notably, the adoption of SSL/TLS for communicating with other devices. With the help of the ZMap [10] high-speed IPv4 scanner, some recent projects analyzed the TLS ecosystem for web, email and SSH servers, and identified and measured significant security issues in TLS deployments in the wild; see e.g., [11, 12, 13, 14].

Heninger et al. [15] highlighted faulty random number generators in networked devices (see also the recent follow-up work [16]). Chung et al. [17] analyzed over 80 million invalid TLS certificates, and attribute most of them to network devices, including modems/home routers, VPNs, NAS, firewalls, IP cameras and IPTVs. In Oct. 2016, we studied the state of the TLS ecosystem for networked devices [18] and found many devices using cryptographic primitives that are phased out from modern browsers and web servers.

The types and number of devices available in Censys have increased since 2016, with significantly more devices supporting TLS (73.7%) compared to 2016 (29.4%). However, still some devices continue to support weak crypto primitives, while in few device types, the use of such primitives has increased. In this work, we evaluate the progress of securing the TLS ecosystem for devices by performing a similar measurement study in a more comprehensive form and compare the results with our previous study. We extracted certificates of devices and Alexa sites, and process the raw data following the same methodology as in our previous study. There are few new device types added to Censys since 2016. The number of Alexa sites is now restricted to Top-1M in Censys.

We analyze certificates and TLS parameters of 6,319,951 devices (out of 8,570,047), collected from Censys (`http://www.censys.io`) on May 6, 2018. Unsurprisingly, many devices still continue to use cryptographic primitives that are currently being phased out from modern browsers and web servers. The state of the TLS ecosystem doesn't appear to have gained any significant progress. Specifically, we found a significant number of devices using unsafe RSA 512-bit keys (3760 certificates) and 768-bit keys (8338 certificates), slightly lower than our findings in Oct. 2016. The vulnerable/deprecated RC4 stream cipher is still widely used in devices (302,038). A large number of devices (167,900) also use (deprecated) SSLv3. No traces of SSLv2 are found in the snapshot taken in May 2018. We also compare TLS security parameters between devices and Alexa Top-1M sites, which clearly highlights the differences in these two domains. In all security aspects that we consider (SSL/TLS version, signature, encryption and hashing algorithms, and RSA key length), devices on average are more vulnerable than Alexa sites.

Similar to our previous study, we communicated our findings to top manufactures of vulnerable devices. Interestingly, as in our previous study, Cisco appears to have the highest number of vulnerable devices. Furthermore, the information of devices (e.g., model/serial numbers) in Censys with weaker cipher suites is limited, inhibiting us from providing manufacturers concrete identifying information of these devices. We refrained from carrying out intrusive testing to find more specific information of these devices to avoid jeopardizing systems in production. Overall, we hope our results will serve as a catalyst to quick fixing of TLS issues in devices, so that these devices do not remain less secure than the HTTPS/web ecosystem in the long run.

Dataset and code release. Scripts and the steps for analyzing Censys dataset used in our experiments are available at: `https://madiba.encs.concordia.ca/software.html`. The processed Censys dataset can be released upon request for non-commercial use with the consent of Censys maintainers.

Contributions.

- We carried out a measurement study to assess the vulnerabilities in devices based on their TLS certificates and protocol parameters. Our current study is more comprehensive (cf. [18], conducted in Oct. 2016) as new device types and more data relating to devices are added to Censys since 2016. Although the rate of adoption of TLS is remarkable for devices between 2016 and 2018, the use of weak primitives haven't reduced significantly. Ironically, the use of weak primitives has increased in some devices and vice-versa with strong primitives.

- We find an increase of devices with ICS protocols (notably in S7 and Modbus) compared to a study performed by Mirian et al. [19] in 2016. These protocols were originally designed to operate within closed networks without explicit security measures. Although, Mirian et al. found a similar behavior as ours, we report the rate of increase of devices supporting these protocols (except for DNP3) is higher than what they observed in Mar. 2016.

- From our follow-ups with the leading manufacturers of vulnerable devices, apparently, security patches from vendors remain unadopted by many device owners. Beyond adopting secure updates in a timely manner, we also briefly discuss a few countermeasures to improve the security of these devices.

The remainder of this paper is organized as follows. We discuss related work pertaining to TLS deployments in Section 2. We elaborate our methodology and the devices in focus for our study in Section 3. In Section 4, we provide the details of our analysis and results in terms of: the prevalence of weak security practices, and changes (between 2016 and 2018) in the use of weak and strong cryptographic primitives for devices; we also compare the overall results of devices with Alexa-1M HTTPS websites. In Section 5, we present our disclosure procedure and responses from manufacturers of devices with most weaknesses. We list limitations of our experiments and future improvements in Section 6. We suggest a few recommendations to improve the state of device security in Section 7, and finally, conclude in Section 8.

2. Related work

We briefly discuss measurement studies on real-world TLS deployments.

To allow researchers to analyze SSL certificates, the EFF SSL Observatory project [20] offered the first large-scale, open certificate repository containing SSL certificates for the IPv4 address space in 2010. Later, in 2013, Durumeric et al. [11] analyzed the ZMap collected data of web applications (HTTPS) over a period of 14 months to uncover all public certificate authorities (CAs) and the certificates they issued. Censys [21] is a search engine used to query information relating to hosts and networks stored in daily ZMap scans. As an example application for Censys, the prevalence of the unauthenticated Modbus protocol among SCADA systems has been studied. Numerous such systems have been found across the globe. However, non-SCADA devices, specifically, the TLS ecosystem for those devices have not been studied. We extend existing work to understand the TLS ecosystem for networked devices, mostly used at home, enterprise, and industrial environments, and physical/network infrastructures.

Heninger et al. [15] reported in 2012 that RSA/DSA algorithms as used specifically in embedded network devices are vulnerable due to faulty random number generators. They found that 0.75% of TLS certificates share keys, and RSA private keys can be easily calculated for 0.50% of TLS hosts (also reported similar results for RSA/DSA keys as used in the SSH protocol). However, other TLS/certificate parameters were not analyzed in this study.

Pa et al. [6] propose the IoT honeypot (IoTPOT) to analyze malware attacks against devices such as home routers, smart fridges, and other IoT devices. Their honeypot data also shows significant increase in Telnet-based attacks, including DDoS, against IoT devices. Costin et al. [4] devise a platform to find possible reuse of fingerprints of SSL certificates, public/private keys of devices in ZMap datasets; many devices were found with reused keys.

Industrial Control Systems (ICS) are becoming popular facilitating the remote and electronic control of physical equipment and censors. Although these devices with no in-built security are originally designed to work in closed environments, in recent years they are connected to build smart grids. Mirian et al. [19], studied the Internet-connected vulnerable devices, and found an increase of devices supporting BACnet, DNP3, Modbus, Fox and S7.

Shodan.io is a search engine similar to Censys, targeted towards IoT devices (full access requires paid subscriptions). In addition to IPv4 devices, Shodan claimed to have scanned millions of IPv6 addresses, reportedly by exploiting a loophole in the NTP Pool Project [22]. Arnaert et al. [23] highlight challenges in aggregating search results from Shodan and Censys, and propose an ontology to make them more usable and effective for finding vulnerable IoT devices.

There have several large-scale measurement studies of vulnerable IoT/CPS devices in the recent years, including potentially malicious scanning activities. Galluscio et al. [24] used an algorithm with data from the darknet to infer compromised unsolicited IoT devices. They found 11,000 such devices, most of which are embedded into active CPS infrastructures, and can be recruited into botnets. Leveraging a network telescope (consisting of unused, new IP ranges), Fachkha et al. [25] studied the probing of CPS devices supporting 20 common CPS protocols. They analyzed and correlated 50GB darknet data for this purpose (from one-month period), and extracted the probing events after an inferring process. They found more than 9000 such orchestrated events, attributed to unsolicited and malicious campaigns. After cross-matching these events with threat repositories, the authors found Modbus, ICCP, Niagara Fox and DNP3 are the top abused TCP CPS. Torabi et al. [26] performed a similar analysis to infer compromised IoT devices by finding those devices from the Shodan service, and identifying which of them are malicious using a threat repository/malware database. Xu et al. [27] carried out a comprehensive study of vulnerabilities in IP cameras available at `http://www.insecam.org`. In addition to cameras without password protection, the authors found open ports, network traffic rate, live video feeds streamed without owner's knowledge, and outdated/vulnerable software programs. Note that, unlike these studies, we focus on the weaknesses specific to TLS deployment of networked devices.

Benson et al. [28] argue the fragility of the device ecosystem is attributed to unpatchable/insecure devices, insecure default passwords/misconfigurations, and the lack of suitable user interface, regulation, and cooperation between IoT manufacturers, network providers, content providers and end-users. The authors propose a *Security Monitor* to observe the aggregate view of network activity, as the low volume of attack traffic from an individual device is most likely undetectable. In addition, they propose a *Security Manager* to police the behavior of IoT devices at levels of different granularity (e.g., IP and service levels).

To improve the manual annotation process in Censys (the ZTag device tagging module), Feng et al. [29] develop an Acquisitional Rule-based Engine (ARE) capable of discovering and annotating devices automatically. ARE relies on application-layer responses from devices that run an Internet-accessible server, in conjunction with product information collected through web search. However, ARE will miss devices behind a NAT or the ones that cannot be queried from outside (e.g., no web server). Mi et al. [30] scan residential networks behind NAT to discover IP proxy machines including home IoT devices; access to residential machines is purchased from residential proxy providers such as Luminati[1] and Geosurf.[2] This approach is however ethically questionable at best (no consent from the device owners). Also, some proxy providers, such as Luminati disallows scanning the local network.

3. Methodology and device info

We rely on the Censys [21] search engine for our analysis. In this section, we provide a brief overview of Censys, and detail our methodology.

Censys[3] enables querying data from the Internet-wide scan repository, a data repository hosting the periodic scan results as collected by the ZMap scanner [10]. Censys tags the collected data with security-related properties and device types, allowing easy but powerful search queries through its online search interface and REST API. Censys also tags TLS and certificate data of Alexa Top-1M web sites. Tagging is done by annotating the raw scan data with additional metadata, e.g., type and manufacturer for devices, and Alexa ranking for sites. The output from the application scanners is used to identify device-specific metadata. The annotation process involves ZTag (paired with ZMap and ZGrab), allowing researchers to add logic to define metadata for currently untagged devices [21]. Although Censys is now commercialized and a matured product, search capabilities in Censys are still improving (not all device metadata is defined in ZTag, although ZTag can be extended). Thus, TLS/certificate data and tag information for all device types are still not comprehensively reflected in Censys.

Table 1 lists available device types extracted from Censys, divided by their TLS support, for our datasets collected in Oct. 2016 and May 2018. Results discussed here

[1] `https://luminati.io`
[2] `https://www.geosurf.com`
[3] `http://www.scans.io`

Device type	Oct. 2016				May 2018			
	Non-TLS Count	Non-TLS %	TLS Count	TLS %	Non-TLS Count	Non-TLS %	TLS Count	TLS %
Infra. router	237,540	66.8	118,259	33.2	381,379	69.1	170,320	30.9
Modem	158,558	86	25,724	**14**	108,021	2.1	4,959,267	**97.9**
Camera	143,721	95.5	6809	4.5	116,691	92.2	9932	7.8
NAS	71,997	56.5	55,503	43.5	186,222	33.6	368,480	66.4
Home/office router	51,347	66.7	25,667	33.3	211,851	43.9	270,195	56.1
Network	3	0	39,857	100	1,053,091	79.9	265,715	20.1
Printer	10,148	31.3	22,296	68.7	153,147	76.7	46,463	23.3
Scada	24,909	86.8	3773	13.2	23,509	85.9	3860	14.1
CPS	12,820	93.7	868	6.3	11,423	12.3	81,572	87.7
Media	8000	87.9	1102	12.1	3647	2.5	142,293	97.5
Total	719,043	70.6	299,858	**29.4**	2,248,981	26.3	6,318,097	**73.7**

Table 1: Type-wise device distribution

refer to our May 2018 dataset, unless otherwise specified. We further group some device types from Censys for easier presentation as follows: modem (cable/DSL), printer (all printer models, print servers), network (generic network devices, network analyzers), SCADA (scada controller, router, gateway, server, frontend), media (set-top box, digital video recorders, VoIP, cinema), CPS (PLC, HVAC, IPMI, alarm system, environment monitor, fire alarm, industrial control system, water flow controller, light controller, power distribution unit, power monitor, power controller, solar panel). Certain device types (e.g., USB) appear to be small in numbers (9). This may be due to the fact that the tagging process in Censys is not very comprehensive. We do not consider devices that are very low in number or does not fall into our device categorizations (e.g., KVM, TV tuner, USB devices). The devices appear to come from all around the world (78 countries with >1000 devices); the top 10 countries host about 84% of all devices compared to 56% reported in our 2016 study. Top-3 countries hosting these devices in 2018 are USA 43.5%, Mexico 15.8%, Spain 6.3% (in 2016: Germany 17.9%, USA 15.0%, India 4.9%).

For comparison, we chose the Alexa Top-1M sites. Data extracted from Censys is transformed to an intermediary format that requires a resource-intensive post-processing phase. Search queries can be executed on Censys in two ways: a RESTful web API or an SQL interface engine.[4] We used the latter option, as it is more efficient for large-scale search results. After the TLS parameters and certificates are extracted for devices and Alexa-1M sites, we first analyze our selected security parameters and algorithms in devices. We then compare the security parameters from devices with those from Alexa-1M sites, to highlight any important differences between them. Similar to past work (e.g., [11, 31]), we choose the following certificate/TLS parameters: cipher suite (algorithms used for hashing, key encryption, key exchange and authentication, signature), SSL/TLS protocol version, and RSA key length.

4. Analysis and results

On May 6, 2018, we used Censys [21] to extract certificates and TLS parameters from 6,319,951 TLS-supporting devices (out of a total of 8,570,047 devices), and from 735,638 HTTPS sites in Alexa Top-1M. The number of total devices in Censys supporting TLS have increased by 21 fold since our last measurement study. Furthermore, new types of devices have been added to Censys, including: network (switch) and CPS (alarm system, environment monitor, fire alarm, IPMI, power con-

[4] Accessed via Google BigQuery interface: `https://bigquery.cloud.google.com`

troller, solar panel). We also noticed a new type of router: SOHO (Small Office / Home Office) appearing in the latest Censys snapshot, which we categorize as *home/office router*. Only *home routers* were found in our previous dataset. Home routers are normally used for personal use where users prefer accessing the Internet with wifi connections for ease of accessibility. In contrast SOHO routers are intended to support enterprise systems, mostly through wired Ethernet. The count of devices supporting TLS has increased significantly in May 2018 (6,318,097, 73.7%) compared to Oct. 2016 (299,858, 29.4%); the increase of modems is also extraordinary (i.e., from 25,724 to 4,959,267). In contrast, the percentages of some devices (infrastructure router, printer, network) supporting TLS have decreased from that in May 2016. This may be attributed to the variation of the proportion in which devices of different types are added to Censys. In this section, we provide the results of our analysis and compare the use of TLS/certificate parameters.

4.1. Prevalence of weak security practices

For each cryptographic primitive in a device certificate and TLS/SSL protocol banner, we compute the percentage to compare the parameters between devices; see Figures 1–5 for a comparison of the weak cryptographic primitives (for exact data, see Table 2). We also compare average values from devices with Alexa sites (the last two bars). For brevity, we first highlight results for algorithms and parameters that are most vulnerable. We also analyze certificate reuse in both devices and Alexa sites.

Hash functions in message authentication. Some devices still use MD5 although in small fractions. The use of MD5 in home/office routers (60,835, 22.5%) and CPS (14,665, 18%) devices are significant. In Alexa-1M sites, the MD5 usage is negligible as a percentage (1834, 0.2%) compared to our findings in 2016 (6588, 1.1%). Media (141,905, 99.7%) devices and infrastructure routers (152,601, 89.6%) mostly use SHA1; see Figure 1. MD5 is broken for more than a decade now [32]. SHA1 collision attacks are now feasible [33] (see also [34]; being phased out as of writing).

Hash functions in signature schemes. The MD5-RSA signature scheme is mostly used in printers (16,749, 36.1%), while SHA1-RSA is predominant in media (141,882, 99.7%), network (185,607, 69.9%) devices, infrastructure routers (152,601, 29.7%) and modems (3,699,856, 74.6%); see Figure 2. Devices using MD5-RSA are vulnerable to certificate collision attacks, where attackers create certificates that collide with arbitrary prefixes/suffixes [35]. Out of all the modems, the usage of SHA1-RSA is the highest in wireless modems (27,747, 75.2%). Some devices (164,847) use "unknown" algorithms; according to a Censys author (email correspondence), these algorithms are not parseable.

RSA key lengths. The use of factorable 512-bit RSA keys is a serious security issue, enabling efficient FREAK attacks (e.g., via [36]). These keys are mostly observed in infrastructure routers (3111, 1.9%), cameras (434, 4.4%) and Scada (22, 0.6%) devices. We also noticed 512-bit RSA keys in an industrial control system and two solar panels. The industrial control system with the factorable key appears to be located in Spain, and manufactured by *Opto22* [37]. Certificates with 1024-bit RSA keys are deemed to be insecure as of early 2016; see NIST SP 800-131A (at least 2048 bits should be used). However, many devices still use 1024-bit keys (Figure 3); the use of 1024-bit keys is high in infrastructure routers (124,918, 78%) and media (141,771, 99.6%) devices. A few Alexa-1M sites (12,974, 2%) still use 1024-bit RSA keys in certificates.

Encryption algorithms. We check the use of vulnerable ciphers such as RC4 (see e.g., [38], RFC 7465), and 3DES (the Sweet32 attack [39]). Note that the ZGrab application scanner as used with ZMap includes RC4 as a supported cipher (in addition to ciphers included in the Chrome browser), to allow communication with older TLS servers. RC4 is mostly used in infrastructure routers (108,834, 63.9%), while its use is minimum in media (85, 0.1%) devices; see Figure 4. Alexa-1M sites still use RC4 at a smaller scale (4828, 0.66%). The use of 3DES cipher is limited except in CPS (4734, 5.8%) and network (10,392, 3.9%) devices. 3DES is more prevalent in firewalls (8412, 25.8%). The use of ChaCha20-Poly1305 (currently being standardized, RFC 7905) as a replacement of RC4 is still negligible in devices as an average (550, 0.09%) compared to Alexa-1M sites (15,225, 2.07%).

TLS/SSL version. SSLv3 usage (vulnerable to the POODLE attack [40]) is considerable in home/office routers (76,338, 28.3%) and CPS (13,928, 17.1%) devices. TLS

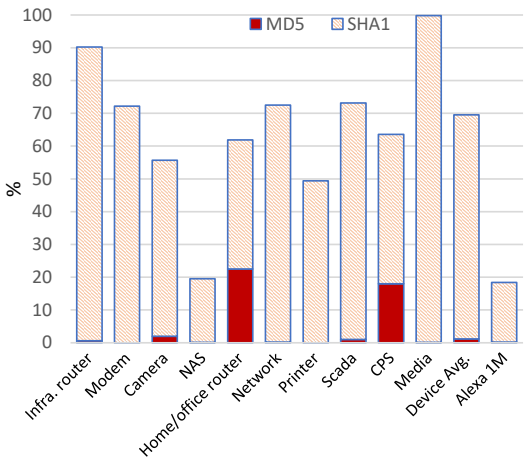

Figure 1: Hashing algorithms

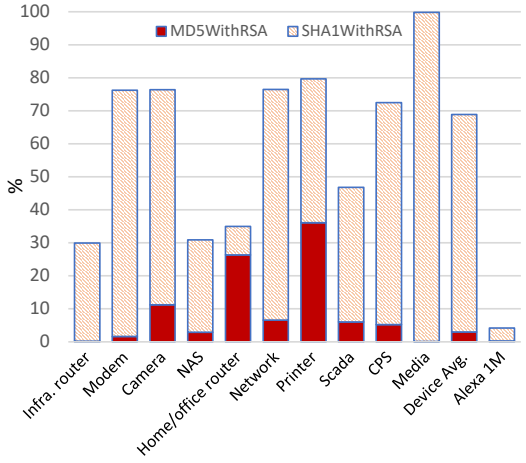

Figure 2: Signature algorithms

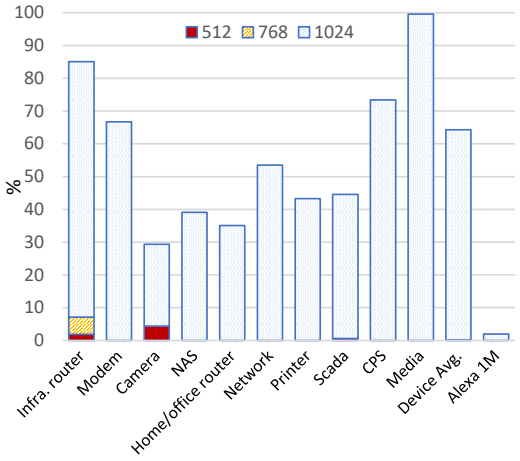

Figure 3: Key lengths (RSA)

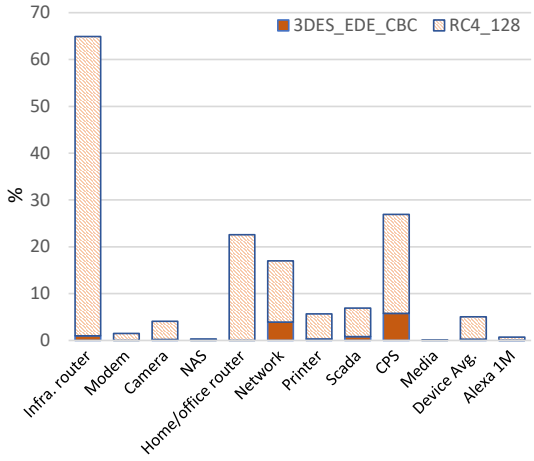

Figure 4: Encryption algorithms

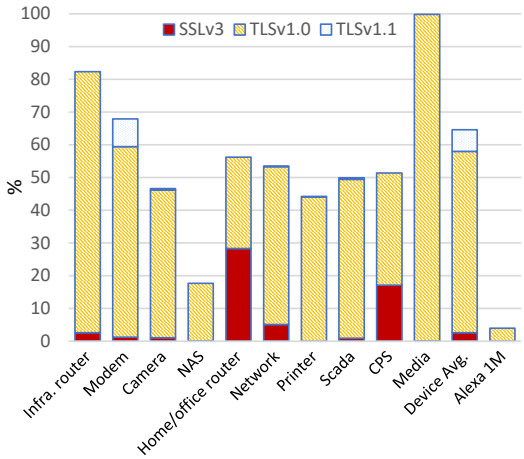

Figure 5: SSL/TLS protocol versions

	Hashing alg.		Signature alg.		RSA keylen			Enc. alg.		Protocol		
	MD5	SHA1	MD5-RSA	SHA1-RSA	512	768	1024	3DES	RC4	SSLv3	TLS 1.0	TLS 1.1
Infra. router	0.6	**89.6**	0.2	**29.7**	**1.9**	**5.2**	**78**	1	**63.9**	2.6	**79.7**	0
Modem	0	72.2	1.6	**74.6**	0	0	66.7	0	1.5	1.2	58.2	8.5
Camera	2	53.7	11.2	65.2	**4.4**	0	25	0.2	3.9	1.1	45	0.5
NAS	0.1	19.4	2.9	28	0	0	39.1	0	0.3	0.1	17.6	0
HO router	**22.5**	39.4	26.3	8.7	0	0	35.1	0	22.6	**28.3**	27.9	0
Network	0.2	72.3	6.6	**69.9**	0	0	53.5	**3.9**	13.1	5.1	48.2	0.2
Printer	0	49.4	**36.1**	43.6	0	0	43.3	0.3	5.4	0	44.1	0.1
Scada	1	72.2	6	40.8	**0.6**	0	44	0.8	6.1	0.9	48.5	0.5
CPS	**18**	45.6	5.2	67.3	0	0	73.4	**5.8**	21.1	**17.1**	34.3	0
Media	0.1	**99.7**	0.1	**99.7**	0	0	**99.6**	0	**0.1**	0.1	**99.7**	0
Device avg.	1.2	68.3	3	65.9	0.1	0.1	64.1	0.27	4.78	2.6	55.4	6.6
Alexa-1M	**0.2**	18.2	0.3	3.9	0	0	**2**	**0.06**	**0.66**	0	**4**	0

Table 2: Percentages of weak cryptographic primitives in devices (as of May 6, 2018); under Enc. alg., 3DES and RC4 represent 3DES-EDE-CBC and RC4-128, respectively. "HO router" in the first column is "home/office router".

1.0 is vulnerable to the BEAST attack [41]. Media (141,861, 99.7%) and infrastructure routers (170,311, 79.7%) have a high use of TLS 1.0. However, in Alexa-1M sites (31, 4%), TLS 1.0 use is low. In our study in Oct. 2016, we found devices supporting SSLv2 (deprecated in 2011, see RFC 6176). Version rollback attacks downgrade SSLv3 to SSLv2 [42]. With the DROWN attack [43], an attacker can even break a strong RSA key, if the server shares the RSA key with an SSLv2 server. Most of these devices were of type NAS (5517) and network (2006). However, none of the current snapshots in ZMap or Censys appear to have devices using SSLv2.

Certificate issuers. Most device certificates are self-signed (68% and 71% in Oct. 2016 and May 2018, respectively), potentially making them vulnerable to man-in-the-middle (MITM) attacks. The remaining certificates are CA-signed; see Table 3 (total CAs: 1335 and 4923 in Oct. 2016 and May 2018, respectively). Some CA organizations are device manufacturers, others are browser trusted. Certificate data in Censys contains a flag indicating the browser trusted status (based on Mozilla NSS). According to the Top-10 issuer organizations data taken from 2016 and 2018 snapshots, a major change is the adoption of free certificates from *Let's Encrypt* (21,006; no certificates from traditional CAs in top 10). We could not find more details of the "Bitbug.net Network Services" certificate issuing organization. The *Issuer DN* field of certificates issued by "hw" contains email addresses from Huawei (e.g., HW@huawei.com). When contacted, Huawei confirmed the issuance of those certificates. Although "trendchip"[5] was acquired by another company in 2010, certificates issued are still in use under its former name. Certificates of both trendchip and Bitbug.net are expired.

Certificate reuse. Some devices often come with the same default certificate, which remains unchanged afterwards. We group certificates according to their SHA256 fingerprints for reuse detection.[6] Many devices reuse certificates, out of which DSL and cable modems are the highest (4,763,389, 75.4%). These devices may be vulnerable to MITM attacks (cf. SSH attacks [44]). Certificates reuse in Alexa sites has reduced slightly (33% of certificates are reused in May 2018 vs. 38% in Oct. 2016, mostly due to CDN, similar to past studies,

[5] `https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=28942714`

[6] Certificates with the same public key may differ in other fields, resulting in different fingerprints. We did not analyze public key reuse in certificates; the dataset we use from ZMap/Censys does not contain actual public key values.

Oct. 2016				May 2018			
Issuer org.	Count	%	Trusted?	Issuer org.	Count	%	Trusted?
Western Digital	6846	0.67	×	Synology Inc.	143,336	2.27	×
Synology Inc.	6461	0.63	×	hw	138,154	2.19	×
ZyXEL	4220	0.41	×	Huawei	125,009	1.98	×
GoDaddy.com	1412	0.14	1213	trendchip	37,161	0.59	×
hw	1101	0.11	×	ZTE Corporation	30,841	0.49	×
TELMEX	1038	0.10	×	Let's Encrypt	22,815	0.36	**21,006**
TAIWAN-CA	818	0.08	818	LANCOM Systems	15,041	0.24	×
COMODO	811	0.08	630	Bitbug.net Network Services	11,376	0.18	×
StartCom Ltd.	628	0.06	399	SANGFOR	9986	0.16	×
GeoTrust Inc.	622	0.06	538	Cisco Systems	9543	0.15	×

Table 3: Top 10 organizations issuing device certificates (the "Trusted?" column represents browser trustworthiness)

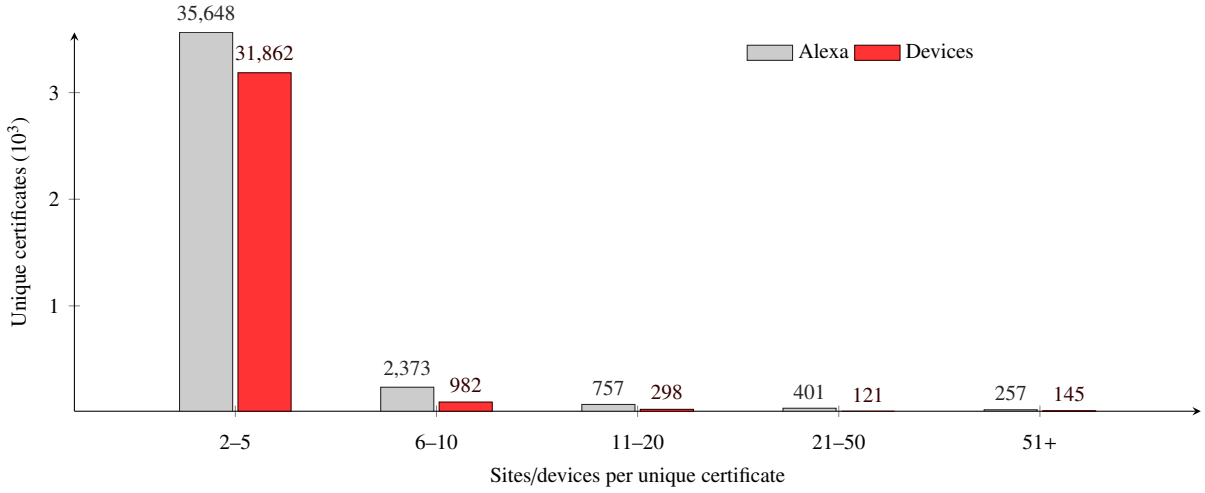

Figure 6: Unique certificates: Alexa-1M (total certs: 735,638) vs. devices (6,319,951) as of May 2018

e.g., [45]); see Figure 6. Certificate reused by groups of 5+ Alexa sites/devices are relatively low.

The Common Name (CN) in most reused certificates contain non-routable IP addresses, e.g., 192.168.1.1 (274,824, 4.35%), generic identification labels, e.g., zxserver (138,135), BMS (1,345,520), or domain names, e.g., *.alarmesomfy.net (14,004).

DH prime number reuse. Many devices supporting Diffie-Hellman (DH) Key Exchange reuse prime numbers. Such reuse can be exploited via the Logjam attack, enabling a MITM attacker to downgrade connections to export grade Diffie-Hellman [14]. Alias et al. [46] reported that a timing side-channel attack is possible with DHKE used in an embedded system which can decrease the key search area, reducing the time to solve the Discrete Log Hard Problem (DLHP). Such an attack can lead to the extraction of private keys from devices. There are (308,139, 4.87%) reused primes in devices, including infrastructure routers (27,187, 0.43%), NAS (5479, 0.54%), modems (97,753, 1.55%), and network (63,443, 1%). In Censys, there are 735,638 Alexa domains supporting TLS, out of which only 3.6% (26,310) support DHKE reused prime numbers. In Oct. 2016, 0.2% of all Alexa sites reused DH prime numbers, while

	Hashing alg.		Signature alg.		RSA keylen			Enc. alg.		Protocol		
	MD5	SHA1	MD5-RSA	SHA1-RSA	512	768	1024	3DES	RC4	SSLv3	TLS 1.0	TLS 1.1
Infra. router	0.4	-9.8	**-54.7**	-10.6	-1.3	-2.2	-5.2	1	-17.6	**-52.4**	35.7	-0.2
Modem	-0.4	**38.8**	0.9	-18.8	-0.1	0	**59.3**	0	-18.4	1	25.8	8.5
Camera	-10	-21.2	-1.3	-6.1	3.3	-0.1	-26.5	-0.2	-17.7	-2.6	-21	-11.6
NAS	-1	-6.1	-7.4	-19.7	-0.2	0	5.2	-0.2	-2.3	-0.7	-4.2	-0.1
HO router	**22.3**	**-32.5**	26	-18.8	0	0	6.9	0	22.3	28.2	2.8	0
Network	-0.1	-17.8	4.8	-25	0	-0.4	-36.5	3.6	6.9	4.2	-36.2	0.1
Printer	0	**-34.8**	**-38.8**	30.2	0	0	-28.2	-0.6	-18.9	0	-34.2	0.2
Scada	-2.7	-11.8	-5.6	-14.6	-1.4	0	-5.1	-1.8	-8.4	-3.2	-19.1	-0.6
CPS	**17.7**	0.9	1.6	-13.7	-0.7	0	**60.5**	-13.9	18.3	16.1	14.6	-19.4
Media	-15.9	**33.5**	-12.2	41.8	-0.3	-0.1	**48.2**	-0.5	-18.9	-15.8	40.1	-0.6
Device avg.	-2.6	**0.9**	-15.3	**7.6**	-1	-1.9	**16.2**	-3.23	-14.5	-6.5	**5.1**	**1.8**
Alexa-1M	-0.9	-13	-0.2	-7.9	0	0	-3.8	-0.2	-1.1	**0**	-11.6	-0.1

Table 4: Changes in weak cryptographic primitives in devices between Oct. 18, 2016 - May 6, 2018; under Enc. alg., 3DES and RC4 represent 3DES-EDE-CBC and RC4-128, respectively.

with Alexa-1M sites, the same reused percentage is 9.9% (50,292). Therefore, it appears that DHKE prime number reuse is significantly high in Alexa-1M sites compared to all of the Alexa sites.

4.2. Changes in the use of weak cryptographic primitives

New devices added to Censys consist of cryptographic primitives at varying proportions. These cryptographic primitives exhibit positive and negative fluctuations at the level of our device groupings, or when taken as an average. Table 4 shows changes in percentages of weak primitives. A negative value represents a reduction of the primitive compared to our previous study and vice-versa. Alexa-1M sites supporting HTTPS have increased in Censys (from 598,888 to 735,638) since 2016. The numbers for device average of SHA1 hashing algorithm (0.9%), SHA1-RSA signature algorithm (7.6%), RSA key lengths of 1024-bit (16.2%), TLS 1.0 (5.1%) and TLS 1.1 (1.8%) have increased.

It is important to note that even when the average of a device category for a weak primitive is reduced, it is still possible to observe an increase of the same primitive for a specific device in the same grouping. For example, the use of MD5 on average has reduced (-2.6%), but its use in home/office router (22.3%) and CPS (17.7%) devices has increased significantly. SHA1 use has increased in modems (38.8%) and media (33.5%) devices, while a sharp drop is noticed in home/office routers (-32.5%) and printers (-34.8%). MD5-RSA use has dropped in infrastructure routers (-54.7%) and printers (-38.8%). The 1024-bit RSA keys increased in modem (59.3%), CPS (60.5%) and media (48.2%) devices. SSLv3 usage has dropped in infrastructure routers (-52.4%). No change is observed for Alexa-1M sites (SSLv3 is not used).

Mirian et al. [19] found devices with ICS (Industrial Control Systems) protocols show vulnerabilities in equipments installed in plants. The number of vulnerable devices for specific ICS protocols (in Mar. 2016) and the percentage increase between Dec. 2015 – Mar. 2016 is shown in columns 2 and 4 of Table 5. All devices supporting ICS protocols are tagged in Censys with the specific protocol name (e.g., BACnet, DNP3, Modbus, Fox, S7), and we use these tags to differentiate when counting devices supporting each protocol. We extracted the number of devices supporting the specific protocols from the May 2018 snapshot in Censys and calculated the percentage change from Oct. 2016. The number of devices using S7 (41.6%) and Modbus (24.9%) protocols have increased significantly. However, devices using DNP3 (1.2%) haven't increased much.

Reusable private keys. It appears that a substantial number of manufacturers include shared private keys into

Protocol	Number of devices (Mar. 2016 [19])	Number of devices (May 2018)	Increase from Dec'15 to Mar'16 [19]	Increase from Mar'16 to May'18
BACnet	16,813	17,178	0.4%	2.1%
DNP3	429	434	2.3%	1.2%
Modbus	23,120	30,771	7.1%	**24.9%**
Fox	26,535	28,261	0.9%	6.1%
S7	2798	4791	18.7%	**41.6%**

Table 5: Changes in vulnerability – an increase in devices supporting vulnerable ICS protocols is apparent with time (specifically for Modbus and S7)

firmware of devices being sold [47]. These keys are mostly used to provide SSH and HTTPS access to devices. It is possible to extract these private keys after buying such devices or from a downloadable firmware. Censys tags these reused private keys, but it is not an exhaustive source to find all devices that are impacted. This is also because not all devices are persistently connected to the Internet. Viehböck et al. [48] published a list of fingerprints of devices with known private keys. Censys identifies these devices with private keys using a non-intrusive approach leveraging the fingerprints of certificates from its Internet-wide scans [49]. If a reused private key is exposed, a large number of devices may become vulnerable to impersonation, man-in-the-middle and passive decryption attacks [49]. Top-10 countries with devices including known private keys are shown in Table 6. Thailand (14.14%), United States (13.09%) and Brazil (10.06%) are the top 3 countries that include known private keys in devices. According to a previous study [49] carried out in 2015, top 3 countries having devices with known private keys are United States (26.27%), Mexico(16.52%) and Brazil (8.10%). While the situation have improved in some countries, in some countries devices with known private keys have increased, e.g., United Kingdom (3.62%), Brazil (1.96%), Colombia (0.04%).

Country	Count	Percentage
Thailand	193,805	14.14%
United States	179,435	13.09%
Brazil	137,803	10.06%
Dominican Republic	132,787	9.69%
Mexico	86,825	6.34%
United Kingdom	80,610	5.88%
Colombia	60,291	4.4%
Spain	59,068	4.31%
Canada	35,254	2.57%
Tunisia	24,298	1.77%

Table 6: Top-10 countries with known private keys included in devices

We summarize the numbers and percentages of devices with reusable keys in Table 7. Modems, home/office routers, network and NAS devices appear to reuse a considerable number of these private keys. According to Table 8, Huawei, DrayTek and Multitech are manufacturing most of these devices. To mitigate this risk, vendors should consider assigning a random private key to each of the devices manufactured. On the other hand, users should change the default passwords and certificates (self-signed) pertaining to devices whenever possible as appropriate. However, this is not always a pragmatic approach due to lack of permissions, controls and knowledge to adopt such security measures by clients.

4.3. Changes in the use of strong cryptographic primitives

The use of strong cryptographic primitives appears to have reduced for certain devices between Oct. 2016 – May 2018; see Table 9. The SHA256 usage in modems (-38.4%), CPS (-18.6%) and media (-17.7%) devices has dropped significantly. The use of SHA256-RSA and SHA512-RSA has significantly reduced in media (-29.7%) and Scada (-8.9%) devices, respectively. Although, the device average of SHA512-RSA has decreased slightly (-0.5%), no change is observed in Alexa-1M sites. Even though, the SHA256-ECDSA use in device grouping under consideration or device average has not reduced, the use of same signature algorithm has reduced slightly in Alexa-1M sites (-0.4%). The device av-

Device grouping	Count	Percentage
Modem	535,530	6.2%
Home/office router	160,892	1.9%
Network	61,375	0.7%
NAS	45,632	0.5%
Camera	253	-
Infra. router	183	-
Media	121	-
Scada	90	-
Printer	85	-
CPS	11	-

Table 7: Devices groupings with a known private key as tagged in Censys

Manufacturer	Count	Percentage
Huawei	503,364	5.9%
DrayTek	151,049	1.8%
Multitech	73,173	0.9%
Ubiquiti Networks	30,030	0.4%
Telrad	27,747	0.3%
Seagate	27,617	0.3%
NetGear	10,809	0.1%
Linksys	9541	0.1%
Adtran	7379	0.1%
Allegro Software	6964	0.1%

Table 8: Top-10 manufactures of devices with a known private key as tagged in Censys

erage for 2048-bit (-13.3%) and 4096-bit (-0.3%) RSA keys has reduced, but the corresponding change in Alexa-1M is an increase (12%, 3.1%). The device average for AES-128-CBC (-2.8%) has reduced, but the stronger AES-256-CBC (17.55%) and AES-128-GCM (1.21%) primitive use have increased. In contrast, in Alexa-1M sites, only the use of AES-128-CBC (-1.8%) and AES-256-CBC (-9.39%) have reduced. The device average of TLS 1.2 protocol is slightly reduced (-2.8%) as opposed to the considerable increase of the same in Alexa-1M sites (11.6%). Also ,TLS 1.2 use in modems (-35.1%) has reduced while it is the opposite for cameras (35.2%).

Overall, apart from encryption algorithms, there is an increase in weak TLS primitives with the growth of devices supporting TLS. It is likely that the legacy devices accumulated over time may not get proper attention to have their firmware upgraded to latest versions to eliminate possible vulnerabilities (due to e.g., lack of oversight [50]).

5. Disclosure

The vulnerable devices we found in our study are manufactured by hundreds of different companies. The Top-5 manufactures of vulnerable devices are show in Table 10. We have contacted the ones with many vulnerable devices, where we could locate contact email addresses of vulnerability management support teams of these manufacturing companies from the web, explaining our findings. We have got responses from Cisco, DrayTek, Synology, Huawei and Ubiquiti Networks. According to Cisco, they allow users to import certificates of their choice, who may be using certificates with weak ciphers due to lack of awareness. As is in our previous study, Cisco appears to be the top manufacturer with vulnerable devices. Interestingly, the devices manufactured by Somfy Systems have the same number (13,897) of ciphersuites with vulnerable MD5, RC4, SSLv3 and RSA1024 cryptographic primitives. All these devices appear to be using the same TLS_RSA_WITH_RC4_128_MD5 cipher suite for negotiation during the SSL/TLS handshake.

As we found, Vigor routers produced by DrayTek are vulnerable. DreyTek informed us that the vulnerable devices are of older units where the owners haven't updated their firmware. Some of these devices support the weak SSLv3 protocol. According to DrayTek: "SSLv3 is, of course, deprecated and users should use TLS1.2 which is supported by all of our current and most recent products". Unfortunately, companies of larger scale will take more time to improve security of devices with their prevailing change management practices, where the focus on stability takes precedence over security. They claim most of their users update the units, but it is challenging to acquire 100% success due to lack of adherence by users in turning off older protocols. In May 2018, more than 800,000 DrayTek routers were found to be exploitable by a DNS reprogramming attack [51], which can eventually hijack web traffic to reveal personal information.

Huawei claims that they deny access to WAN ports by default, but some users appear to have customized their devices by opening the WAN ports, allowing possible

	Hash alg.	Signature alg.			RSA Keylen		Encryption alg.			Protocol
	SHA256	SHA256-RSA	SHA512-RSA	SHA256-ECDSA	2048	4096	AES-128-CBC	AES-256-CBC	AES-128-GCM	TLS 1.2
Infra. router	9.4	-1.2	18.6	1.6	8.8	0.3	1.9	5.4	9.3	16.9
Modem	**-38.4**	18.1	-0.1	0	-58.4	-0.4	-4.7	61.5	-38.5	**-35.1**
Camera	31.2	15.4	0.1	0	32.1	-0.1	-2	-11.3	31.2	**35.2**
NAS	7.1	27.2	-0.1	0	-4.5	-0.3	-2.8	-1.8	7	5
HO router	10.2	-7.1	0	0	-6.8	-0.1	26	-58.5	10.2	-31
Network	17.9	12.4	0.1	7.9	36.6	-0.1	11	-39.4	17.8	31.84
Printer	34.8	8.6	0	0	28.2	0	0.2	-15.5	34.8	38.3
Scada	14.63	19	0.7	0.8	6.9	0.3	-6.7	2.3	14.5	22.9
CPS	**-18.6**	21	**-8.9**	0	-59.3	-0.2	-4.5	18.6	-18.6	-11.3
Media	**-17.7**	**-29.7**	0	0	-46.8	-0.1	-14.3	51.4	-17.7	-23.7
Device avg.	1.3	4.1	**-0.5**	**0.3**	**-13.3**	**-0.3**	**-2.8**	**17.55**	1.21	**-2.8**
Alexa-1M	13.9	8.4	0	**-0.4**	**12**	**3.1**	-1.8	**-9.39**	11.9	**11.6**

Table 9: Changes in strong cryptographic primitives in devices between Oct. 18, 2016 – May 6, 2018

external attacks. They plan to communicate with their customers and have the SSH/HTTPS ports of WAN devices closed, to reduce the risk of devices with known private keys. Dell claims that the reported devices appear to run very old firmware, not properly configured or already out of support. With the latest firmware, they only use TLSv1.0, TLSv1.1 or TLSv1.2 protocols, SHA256 hashing algorithm, longer key lengths (2048 bits), and no RC4 ciphers.

Synology informed us that users may be using outdated settings to host the services provided by their product(s). They were very appreciative of our efforts and plans to publish techniques in enhancing the security of their Data Security Manager (DSM) with different settings to address the problem. Ubiquiti Networks informs us that their airMAX devices used static SSL/TLS certificates until the end of 2015, at which point they fixed the problem by generating a self-signed certificate on the first boot. It appears that users are still using Ubiquiti devices with old firmware.

6. Limitations

Certain statistics as extracted from Censys appear to be unusual. For example, there is only one infrastructure router from certain manufacturers, e.g., Apple, DrayTek and Huawei. We communicated such observations to a Censys author, who attributed them to be possible limitations of the current Censys logic, or device misconfiguration. Data in Censys can be queried using the Google BigQuery SQL interface. This interface allows querying data using standard SQL and facilitates downloading results in CSV and JSON formats that are easy to parse and machine process. However, Google BigQuery is not free after one year of use.

According to a Censys author, it is possible that some devices provide conflicting information on different ports, likely due to port forwarding from specific devices to device types that are tagged incorrectly. This appears to be a known issue due to fingerprinting devices at protocol-level rather than at host-level. Censys plans to work on a more advanced fingerprinting technique to address this problem in the future.

Although Censys allows users to search and analyze all types of connected devices via Google BigQuery, Censys do not have information of devices that cannot be reached via ZMap (e.g., private/non-routable/firewalled addresses, opt-out from ZMap scanning). Furthermore, ZMap do not scan devices in their blacklist [52] or those network prefixes that fall outside in its whitelist. Therefore, to evaluate the completeness of results, correlation with alternative sources may be considered [53, 29]. Newer IoT devices are increasingly adopting IPv6 [54], which also cannot be measured by the IPv4-based ZMap scanner.

Censys requires manual effort in defining annotation rules to tag device meta-data (e.g., type, manufacturer), which is not ideal in discovering new devices at large scale. Therefore, more collective effort is also needed to improve device tagging/annotating in Censys [21].

Manufacturer	MD5	RC4	SSLv3	<RSA1024	Device types
Cisco	1340	126,125	50,268	176,478	Infrastructure router, camera, switch, network, SOHO router, firewall, SCADA controller
DrayTek	60,775	60,877	7293	70,801	SOHO router, camera, infra. router
Synology	242	445	211	81,035	DVR, camera, SOHO router, NAS
Somfy Systems	13,897	13,897	13,897	13,897	Alarm system
Dell	760	2541	22	28,592	IPMI, laser printer

Table 10: Top-5 manufactures with vulnerable devices (in May 2018)

We found thousands of vulnerable devices from many manufacturers, and contacted the top-10 of those with most vulnerable devices via email (using appropriate addresses as found in their websites). This is a manual process and is not scalable. Stock et al. [55] explore several forms of scalable/automated communication channels (e.g., email, domain WHOIS information, phone, social media) for more effective vulnerability notification.

7. Recommendations

Based on our analysis, we suggest a few possible way-out from the current status quo in device security. Note that these recommendations are preliminary, listed here to stimulate future work in solving TLS security issues in non-computer devices.

(1) The obvious one would to enable automatic security updates to devices, instead of relying on proactive user actions. However, for certain devices (especially the ones possibly maintained by professional administrators), care must be taken to avoid unplanned downtimes of production systems. For this purpose, vendors should perform thorough testing before releasing patches to its users [56]. In Mar. 2008, a nuclear plant was accidentally rebooted following a software upgrade [57, 58] causing an unnecessary alarm of a drop of cooling. We strongly suggest that updating should be used as the last resort for fixing a security issue; it is far better to avoid possible security issues in the design than fixing them on-the-go. Also, updates will almost never reach to 100% of all devices. Better understanding the consequences of attacks and designing new attack detection/resilient algorithms to prevent them at the inception is vital [57, 58]. As CPS employ autonomous and real time decision making algorithms, the authors suggest to have automatic recovery built-in during the design phase.

(2) As many devices may not be reachable, or not readily update-able due to operational constraints, unlike desktop/mobile/server computers, we recommend to adopt strong security measures from the beginning, including, the use of latest TLS versions, most secure cipher-suites (given the computational capabilities of a device). We argue against gradual/step-wise increase of security levels (e.g., from RSA-512 to RSA-1024) for devices, as they are difficult to update and may remain operational for years. ICS devices originally developed to operate on isolated environments decades ago, still continue to operate, which are now connected to the public Internet allowing more exposure to possible vulnerabilities [19].

(3) Avoid all known pitfalls in TLS security [59, 60], e.g., the use of fixed private keys, vulnerable or soon-to-be obsolete ciphers (e.g., RC4 and RSA-1024) [61], and self-signed certificates (can be easily avoided by using free certificates from Let's Encrypt).

(4) Although manufacturers may block access to remote management interfaces of devices over SSH/HTTPS, users may still customize to allow remote access to devices. Therefore, it is also prudent for ISPs to ensure remote access to customer-provided equipment (CPE) is disallowed [49].

(5) Allowing insecure device settings (e.g., fixed private key), or protocols (as in many ICS devices) with the

assumption that these devices would remain only in isolated networks must be avoided. Traditionally isolated devices are often being connected to the Internet, e.g., for remote management. Failure to address the vulnerabilities of interconnected devices in smart grids will hinder modernization of such systems [62].

(6) Consider system hardening to tighten system security by shutting down unnecessary applications and ports [63].

8. Concluding remarks

As apparent from several studies on the real-world deployment of web servers (e.g., [31, 11]), TLS can provide tangible security benefit, only when it is configured properly. Partly due to several recent high-profile measurement studies (e.g., [13, 14]), TLS security for user-facing servers is improving. However, we found many networked devices are still using weaker/broken crypto primitives in TLS, compared to Alexa sites. Based on our measurement studies carried out in Oct. 2016 and May 2018, although the number of devices supporting TLS has sharply increased, still a large number of devices supporting weaker cryptographic primitives remain vulnerable. Some manufacturers (e.g., Lenovo, Seagate) appear to have produced a larger number devices with RC4, MD5, SSLv3 and key lengths of 1024-bit (RSA) and below. We also found a considerable number of known private keys in devices, which make them vulnerable. This is more apparent in modems (6.2%) and home/office routers (1.9%). Upon reaching out to them, we were told that the primary reason for the status quo is the inaction of users in applying latest firmware upgrades. However, the reality is such that no action is taken by most manufacturers to mitigate the vulnerabilities of devices where their users are not proactive in applying security patches. Blaming users who haven't updated their devices with security patches, which may sometimes happen due to lack of knowledge, will not solve the issue.

Note that some vulnerabilities may have no effect if the services are accessed within a local network (e.g., inside a private home network), or via a modern browser—e.g., no current browser would accept the RC4 cipher or SSLv2, even if offered by a server. As these devices are varied (unlike regular web servers), actual exploitation of their weaknesses will depend on how they are used/accessed. These seemingly obsolete attack vectors can also be revived in the presence of a vulnerable TLS proxy between a modern browser and the vulnerable server, such as an anti-virus proxy [64].

We hope our findings to raise awareness of this issue and positively influence the manufactures to push appropriate firmware upgrades (possibly with auto-updates).

References

[1] E. Ronen, C. O'Flynn, A. Shamir, A.-O. Weingarten, IoT goes nuclear: Creating a ZigBee chain reaction, Cryptology ePrint Archive, Report 2016/1047. `https://eprint.iacr.org/2016/1047` (2016).

[2] A. Cui, S. J. Stolfo, A quantitative analysis of the insecurity of embedded network devices: Results of a wide-area scan, in: ACSAC'10, Austin, TX, USA, 2010.

[3] A. Cui, M. Costello, S. J. Stolfo, When firmware modifications attack: A case study of embedded exploitation, in: NDSS'13, San Diego, CA, USA, 2013.

[4] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, A large-scale analysis of the security of embedded firmwares, in: USENIX Security'14, 2014.

[5] A. Costin, A. Zarras, A. Francillon, Automated dynamic firmware analysis at scale: A case study on embedded web interfaces, in: ASIACCS'16, 2016.

[6] Y. M. P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, IoTPOT: Analysing the rise of IoT compromises, in: USENIX Security'15, Washington, D.C., USA, 2015.

[7] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou, Understanding the Mirai botnet, in: USENIX Security'17, Vancouver, BC, Canada, 2017.

[8] Wired.com, The Reaper IoT botnet has already infected a million networks, news article (Oct. 20, 2017). https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[9] TechRepublic.com, Mirai variant botnet launches IoT DDoS attacks on financial sector, news article (Apr. 5, 2018). https://www.techrepublic.com/article/mirai-variant-botnet-launches-iot-ddos-attacks-on-financial-sector/.

[10] Z. Durumeric, E. Wustrow, J. A. Halderman, ZMap: Fast internet-wide scanning and its security applications, in: USENIX Security'13, Washington, D.C., USA, 2013.

[11] Z. Durumeric, J. Kasten, M. Bailey, Analysis of the HTTPS certificate ecosystem, in: IMC'13, Barcelona, Spain, 2013.

[12] R. Holz, J. Amann, O. Mehani, M. Wachs, M. A. Kaafar, TLS in the wild: An Internet-wide analysis of TLS-based protocols for electronic communication, in: NDSS'16, San Diego, CA, USA, 2016.

[13] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, V. Paxson, The matter of Heartbleed, in: IMC'14, Vancouver, BC, Canada, 2014.

[14] D. Adrian, K. Bhargavan, Z. Durumeric, P. Gaudry, M. Green, J. A. Halderman, N. Heninger, D. Springall, E. Thomé, L. Valenta, B. VanderSloot, E. Wustrow, S. Zanella-Béguelink, P. Zimmermann, Imperfect forward secrecy: How Diffie-Hellman fails in practice, in: CCS'15, Denver, CO, USA, 2015.

[15] N. Heninger, Z. Durumeric, E. Wustrow, J. Halderman, Mining your Ps and Qs: Detection of widespread weak keys in network devices, in: USENIX Security'12, Bellevue, WA, USA, 2012.

[16] M. Hastings, J. Fried, N. Heninger, Weak keys remain widespread in network devices, in: IMC'16, Santa Monica, CA, USA, 2016.

[17] T. Chung, Y. Liu, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, C. Wilson, Measuring and applying invalid SSL certificates: The silent majority, in: IMC'16, Santa Monica, CA, USA, 2016.

[18] N. Samarasinghe, M. Mannan, Short paper: TLS ecosystems in networked devices vs. web servers, in: Financial Cryptography and Data Security (FC'17), Malta, 2017.

[19] A. Mirian, Z. Ma, D. Adrian, M. Tischer, T. Chuenchujit, T. Yardley, R. Berthier, J. Mason, Z. Durumeric, J. A. Halderman, M. Bailey, An Internet-wide view of ICS devices, in: IEEE PST'16, Auckland, New Zealand, 2016.

[20] Electronic Frontier Foundation, The EFF SSL observatory, https://www.eff.org/observatory (2010).

[21] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, J. Halderman, A search engine backed by Internet-wide scanning, in: CCS'15, Denver, CO, USA, 2015.

[22] ArsTechnica.com, Using IPv6 with Linux? you've likely been visited by Shodan and other scanners, news article (Feb. 1, 2016). http://arstechnica.com/security/2016/02/using-ipv6-with-linux-youve-likely-been-visited-by-shodan-and-other-scanners/.

[23] M. Arnaert, Y. Bertrand, K. Boudaoud, Modeling vulnerable Internet of Things on SHODAN and CENSYS: An ontology for cyber security, in: SECUREWARE'16, Nice, France, 2016.

[24] M. Galluscio, N. Neshenko, E. Bou-Harb, Y. Huang, N. Ghaniy, J. Crichignoz, G. Kaddoumx, A first empirical look on Internet-scale exploitations of IoT devices, in: PIMRC'17, Montreal, QC, Canada, 2017.

[25] C. Fachkha, E. Bou-Harb, A. Keliris, N. Memon, M. Ahamad, Internet-scale probing of CPS: Inference, characterization and orchestration analysis, in: NDSS'17, San Diego, CA, USA, 2017.

[26] S. Torabi, E. Bou-Harb, C. Assi, M. Galluscio, A. Boukhtouta, M. Debbabi, Inferring, characterizing, and investigating Internet-scale malicious IoT device activities: A network telescope perspective, in: DSN'18, Luxembourg, 2018.

[27] H. Xu, F. Xuy, B. Chenz, Internet protocol cameras with no password protection: An empirical investigation, in: PAM'18, Berlin, Germany, 2018.

[28] T. Benson, B. Chandrasekaran, Sounding the bell for improving Internet (of things) security, in: IoT S&P'17, Dallas, TX, USA, 2017.

[29] X. Feng, Q. Li, H. Wang, L. Sun, Acquisitional rule-based engine for discovering Internet-of-Things devices, in: USENIX Security'18, Baltimore, MD, USA, 2018.

[30] X. Mi, Y. Liu, X. Feng, X. Liao, B. Liu, X. Wang, F. Qian, Z. Li, S. Alrwais, L. Sun, Resident Evil: Understanding residential ip proxy as a dark service, in: IEEE S&P19, San Fansisco, CA, USA, 2019.

[31] H. Lee, T. Malkin, E. Nahum, Cryptographic strength of SSL/TLS servers, in: IMC'07, San Diego, CA, USA, 2007.

[32] X. Wang, H. Yu, How to break MD5 and other hash functions, in: Eurocrypt'05, Aarhus, Denmark, 2005.

[33] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full SHA-1, in: Crypto'17, Santa Barbara, CA, USA, 2017.

[34] M. Stevens, P. Karpman, T. Peyrin, Freestart collision for full SHA-1, in: Eurocrypt'16, Vienna, Austria, 2016.

[35] M. Stevens, A. Sotirov, J. Appelbaum, A. Lenstra, D. Molnar, D. Osvik, B. de Weger, Short chosen-prefix collisions for MD5 and the creation of a rogue CA certificate, in: CRYPTO'09, Santa Barbara, CA, USA, 2009.

[36] L. Valenta, S. Cohney, A. Liao, S. Fried, Joshua Bodduluri, N. Heninge, Factoring as a service, in: FC'16, Barbados, 2016.

[37] Opto 22, Opto 22 Products, `http://www.opto22.com/site/products.aspx` (2018).

[38] C. Garman, K. G. Paterson, T. Van der Merwe, Attacks only get better: Password recovery attacks against RC4 in TLS, in: USENIX Security'15, 2015.

[39] K. Bhargavan, G. Leurent, On the practical (in-)security of 64-bit block ciphers: Collision attacks on HTTP over TLS and OpenVPN, in: CCS'16, 2016.

[40] B. Möller, T. Duong, K. Kotowicz, This POODLE bites: Exploiting the SSL 3.0 fallback, techical report (Sept. 2014). `https://www.openssl.org/~bodo/ssl-poodle.pdf`.

[41] T. Duong, J. Rizzo, Here come the ⊕ ninjas, technical report (May 2011).

[42] E. S. Alashwali, K. Rasmussen, Whats in a downgrade? A taxonomy of downgrade attacks in the TLS protocol and application protocols using TLS, in: ATSC'18, Singapore, 2018.

[43] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. Halderman, V. Dukhovni, E. Ḱasper, DROWN: Breaking TLS Using SSLv2, in: USENIX Security'16, Vancouver, BC, Canada, 2016.

[44] CERT, Vulnerability note 566724, `https://www.kb.cert.org/vuls/id/566724` (2015).

[45] N. Vratonjic, J. Freudiger, V. Bindschaedler, J.-P. Hubaux, The inconvenient truth about web certificates, in: WEIS'11, Fairfax, VA, USA, 2011.

[46] Y. F. B. Alias, M. A. M. Isa, H. Hashim, Sieving technique to solve the discrete log hard problem in Diffie-Hellman key exchange, in: ISCAIE'15, Langkawi, Malaysia, 2015.

[47] TheRegister.co.uk, Internet of Sins: Million more devices sharing known private keys for HTTPS, SSH admin, `https://www.theregister.co.uk/2016/09/07/bad_key_security_holes_getting_worse/` (2016).

[48] Viehböck, Stefan and Durumeric, Zakir, Fingerprints for certificates with know private keys, https://github.com/zmap/ztag/blob/master/ztag/annotations/tlskeyknown.py (2016).

[49] SEC-Consult.com, House of keys: Industry-wide HTTPS certificates and SSH key reuse endangers millions of devices worldwide, https://www.sec-consult.com/en/blog/2015/11/house-of-keys-industry-wide-https/.

[50] US-CERT, Alert (ta16-250a) - The increasing threat to network infrastructure devices and recommended mitigations, https://www.us-cert.gov/ncas/alerts/TA16-250A (2016).

[51] TechRepublic.com, More than 800K DrayTek routers vulnerable to DNS reprogramming attack, news article (May 22, 2018). https://www.techrepublic.com/article/more-than-800k-draytek-routers-vulnerable-to-dns-reprogramming-attack/.

[52] ZMap, Blacklisting, https://github.com/zmap/zmap/wiki/Blacklisting (2017).

[53] Shodan, Shodan search engine, https://www.shodan.io/ (2018).

[54] J. Czyz, M. Luckie, M. Allman, M. Bailey, Don't forget to lock the back door! A characterization of IPv6 network security policy, in: NDSS'16, San Diego, CA, USA, 2016.

[55] B. Stock, G. Pellegrino, F. Li, M. Backes, C. Rossow, Didnt you hear me? - Towards more successful web vulnerability notifications, in: NDSS'18, San Diego, CA, USA, 2018.

[56] Australian Government, Department of Defense, Assessing security vulnerabilities and applying patches (Jan. 2018), https://www.asd.gov.au/publications/protect/assessing_security_vulnerabilities_and_patches.htm.

[57] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, S. Sastry, Challenges for securing cyber physical systems, in: Workshop on Future Directions in Cyber-Physical Systems Security'09, Newark, NJ, USA, 2009.

[58] J. Eloff, M. B. Bella, Software failures: An overview, in: Software Failure Investigation, Springer, 2018, pp. 7–24.

[59] SSL Labs, SSL and TLS deployment best practices, https://github.com/ssllabs/research/wiki/SSL-and-TLS-Deployment-Best-Practices (2017).

[60] IEEE Internet initiative, Internet of Things (IoT) security best practices - Feb. 2017, https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf.

[61] Internet Engineering Task Force (IETF), Summarizing known attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS), RFC 7457 (http://buildbot.tools.ietf.org/html/rfc7457) (Feb. 2015).

[62] J. Liu, Y. Xiao, S. Li, W. Liang, C. P. Chen, Cyber security and privacy issues in smart grids, IEEE Communications surveys & tutorials 14 (4) (2012) 981–997.

[63] A. Creery, E. J. Byres, Industrial cybersecurity for power system and SCADA networks, in: IEEE IAS PCIC'05, Denver, CO, USA, 2005.

[64] X. de Carnavalet, M. Mannan, Killed by proxy: Analyzing client-end TLS interception software, in: NDSS'16, San Diego, CA, USA, 2016.