Characterizing Hosting and Security Practices for Public-Facing LDAP Servers

Gustavo Luvizotto Cesar*, Gurur Öndarö†, Jonas Kaspereit†,
Fabian Ising‡, Sebastian Schinzel†‡, Mattijs Jonker*, Ralph Holz*¶
*University of Twente, email: {g.luvizottocesar, m.jonker}@utwente.nl
†Münster University of Applied Sciences, ‡Fraunhofer SIT and National Research Center for Applied Cybersecurity ATHENE
email: {gurur.ondaro, j.kaspereit, f.ising, schinzel}@fh-muenster.de
¶University of Münster, email: ralph.holz@uni-muenster.de

***Abstract*—The Lightweight Directory Access Protocol (LDAP) is widely used to make structured data available for standardized lookup, which may sometimes include personal information or authentication credentials. Previous work, including ours, found security issues such as public LDAP servers leaking sensitive information without prior authentication and server configurations with poor communication security. However, prior work did not investigate whether, or to what extent, the identified problems are linked to hosting and management setups. In this paper, we address this gap and explore the organizations hosting public-facing LDAP servers. We identify the network segments more likely to host LDAP instances, the products and operating systems used, and examine the management practices related to Public Key Infrastructure (PKI) setups for LDAP. In contrast to studies on Web and email, which have revealed strong centralization tendencies in deployment, we show that the LDAP ecosystem is diverse, with a wide range of different hosting networks. In this study, we identify 69.1k LDAP instances—6.5× more than prior work—and map these to the respective LDAP products. We find that 5.8% of the servers use a product that is end-of-life or runs on a deprecated OS. We identify servers using problematic X.509 certificates, *e.g.,* those associated with publicly known private keys. From our observations, we give recommendations for network operators to improve their security posture.**

***Index Terms*—LDAP; network security; hosting, and management practices.**

I. Introduction

The Lightweight Directory Access Protocol (LDAP) is a well-known protocol to access directory servers. The protocol is used by various applications, including Microsoft's Active Directory (AD). It serves as a way for LDAP clients to query a backend—*e.g.,* for Single Sign-On (SSO) or to enable email clients to fetch receiver addresses or the corresponding S/MIME certificates [1]. Due to their content and widespread use of LDAP servers in organizations, it is often intended for internal use and are not reachable from the public Internet. However, there are many legitimate cases of public-facing servers, such as the aforementioned support for (secure) email.

In recent work, we investigated the security posture of the *general* LDAP server population on the Internet [2] with a focus on unauthorized access to sensitive data and some aspects of communication security, leaving an analysis of *LDAP hosting* to future work.

In this paper, we return to the topic with a focus on the *management and hosting of LDAP across hosting providers*. Our main contributions are: a) improved LDAP measurements, which enable us to b) detect more LDAP products at large scale; c) analyze the types of hosting and network segments where LDAP is found; d) analyze the PKI practices in the LDAP ecosystem. We make our code and data publicly available under a permissive license[1].

We extend our previous tooling to improve the identification of LDAP servers by a factor of 6.5, identifying many previously unknown instances in the process. Unlike prior work, we extend our measurement and analysis to Global Catalog (GC) instances, achieving a more comprehensive view of the ecosystem. Our product detection can help operators assess the exposure of their networks by identifying outdated instances that an attacker could exploit. To characterize the diverse hosting practices, we drill down to the level of the hosters' network blocks to identify and describe the network segments they use for LDAP. We use a Pareto-inspired approach to determine the hosting behavior in segments in terms of LDAP server software and underlying operating system.

Against this background, we then investigate management practices such as the use of strong communication security and the setup of PKI, including attempts to deploy private PKIs.

We find that 4.3k servers run a deprecated LDAP product. Unlike the centralization observed in other ecosystems such as Web hosting [3], DNS [4], and email [5], we observed several hosters of LDAP servers. We report on servers using X.509 certificates with a private key that is publicly known, posing serious risks to operators and users of these servers. Our findings enable us to provide recommendations for LDAP operators on how to configure their systems more securely, as well as guidance for hosting operators who wish to identify poorly maintained LDAP deployments within their network segments or develop mitigation strategies.

II. Background and Related Work

Background. LDAP is a client-server protocol to facilitate transfer and access of data stored in directory services such as

[1] github.com/internettransparency/ldap-sequel

OpenLDAP or Active Directory (AD). We use the generic term *LDAP servers* to refer to all servers that speak the protocol and distinguish by directory service as needed. Connectionless LDAP over UDP is restricted to a small set of queries; hence we do not investigate it. LDAP typically runs over TCP on port 389 (clear text with optional StartTLS) or 636 (implicit Transport Layer Security (TLS)), while ports 3268 (clear text/StartTLS) and 3269 (implicit TLS) are reserved for the GC service in Microsoft's AD. The GC is an AD role to manage and access copies of data items across a multitude of LDAP servers [6]. LDAP stores data in a tree-like hierarchy. The special Root DSA-Specific Entry (DSE) data entry stores information about the server's functionality in form of attributes and it can help identify the LDAP product. LDAP may use TLS, where a cipher suite is agreed upon and a chain of X.509 certificates is sent to a client. RFC-9325 gives best-practice recommendations.

A certificate chain must be anchored at a trusted root, requiring the LDAP client to be configured with the required root certificate(s). The so-called end-host (or leaf) certificate provides a cryptographic binding of an identifier—typically the domain name of the LDAP server—to a corresponding public key. On the Web, public Certificate Authoritys (CAs) issue certificates under CA/Browser Forum rules (*e.g.,* verification of domain ownership), and root stores are managed by OS (*e.g.,* Windows, macOS, and Linux) and browser vendors (*e.g.,* Firefox). For LDAP, no comparable body or standardization efforts exist. In many cases (*e.g.,* Linux, Windows), the root store that the LDAP client relies on is the same as for the Web. In refined setups, the LDAP server administrator may supply it directly, even using a private CA to issue their own certificates. In this case, the administrators must also deploy the root certificate to their LDAP clients using tools like AD Certificate Services or scripts. In such a *private PKI*, one should issue intermediate certificates from the root certificate, which in turn are used to issue a leaf certificate. This setup is important as it allows the private key for the root certificate to be kept in a secure location. An alternative, semi-private PKI setup is also possible: an operator could request a sub-CA certificate from a public CA, *i.e.,* an intermediate certificate, from which they then issue their own certificates. This setup must be tightly controlled so leaf certificates are only ever issued for domains under control of the administrator [7].

A discouraged practice is to deploy so-called self-signed certificates, where the key used to sign a certificate is also the certified key. In such a case, the client must be pre-configured to accept only this certificate—or users told to ignore the warnings their LDAP client would show. The setup is only suitable if the LDAP server serves a minimal set of users. It also constitutes a security risk as the private key remains online in memory. As certificates are available for free and can be relatively easily deployed with the ACME protocol, there is little justification to use self-signed certificates any more.

Related Work. Empirical studies on the LDAP ecosystem are scarce. In Table I, we show how our paper is positioned with respect to prior work. The first work we are aware of is from 2016, when Rapid7's Project Sonar published a blog post [8] on the presence of LDAP servers on the Internet. The blog post did not cover TLS, certificates, or hosting. While the methodology was not precisely described, the company released the *recog* tool, which uses Root DSE entries to identify the version of an LDAP server. For our work, we improved *recog* to enhance the software's recognition capabilities. We shared our extensions with the original authors.

TABLE I
COMPARISON WITH RELATED WORK. [2] COVER PORTS 389 AND 636.

	Contributions & key insights						
	Hosting and network operation of LDAP	Use of PKI and compromised certs.	Misconfigurations and sensitive information	Recommendations for operators	Data set	Open-source	Ports 389, 636, 3268, 3269
Rapid7 (2016) [8]	○	○	○	●	○	●	●
Kaspereit (2024) [2]	○	○	●	○	○	○	◑
This work	●	●	○	●	●	●	●

The second prior work is our own. In 2024, we introduced *LanDscAPe*, a tool for large-scale LDAP security analysis that revealed widespread misconfigurations, leaked passwords, and insecure TLS setups [2], and investigated weaknesses in public-facing LDAP servers, focusing on data leaks and misconfigurations. Here, we expand the scope of our prior work and examine the hosting and deployment practices of LDAP servers. We provide details on the LDAP versions, including the product lifecycle, and explore the security practices of LDAP servers, including PKI and key management. Our hosting analysis depicts the distribution of LDAP servers across different networks. This enables us to investigate whether the LDAP ecosystem follows others (like the Web) in terms of centralization. Our analysis includes servers running GC

Other kinds of studies have focused on LDAP attacks. We do not show these works in Table I as they study LDAP from a very different perspective and do not measure or characterize the deployment of public-facing servers. For example, Bulusu *et al.* classified injection attacks and proposed various mitigation techniques [9]. Srinivasa *et al.* used honeypots to investigate anomalous LDAP traffic such as LDAP injection, suspicious searches, remote code execution, and brute-force attempts [10]. When configured over UDP, LDAP can be misused for Distributed Denial-of-Service (DDoS) attacks, amplifying traffic by a factor of 56–70, according to Akamai [11]. Other works also consider the dangers of in-band upgrades to TLS, which include Person-in-the-middle and downgrade attacks [12], [13].

Prior work focusing on other protocols, Web protocols [3], DNS [4], email [5], or TLS [14] provided evidence for strong Internet centralization. Durumeric *et al.* investigated the HTTPS ecosystem [15], and Holz *et al.* studied protocols for email and chat [16]. In contrast, our hosting analysis finds the LDAP ecosystem more diversified.

III. Methodology

We extend our prior work [2] to scan additional LDAP ports and devise it for improved LDAP product detection. We analyze the hosters of LDAP and the network segments (for different sizes of hosters) where LDAP servers are most likely to be found. Our TLS analysis links to the hosters and products we identify. We hence create a new and complementary view of the LDAP ecosystem. Note that we do not retrieve any sensitive information from the servers. Below, we provide a description of each improvement we made to our tooling.

LDAP scanning and retrieval. To determine servers with open LDAP ports, we use ZMap for all routable prefixes on ports 389, 636, and also 3268 and 3269. The latter two are the ports for GC. To the best of our knowledge, GC ports have only been investigated in the Rapid 7 blog post of 2016 so far. As LDAP over UDP has a restricted use case, and our interest lies in the general use of public LDAP, we scan only with TCP. Our campaign runs from 2024-10-29 to 2024-11-01.

We use a custom LDAP scanner, written in Go, that supports both StartTLS and implicit TLS and carries out a so-called *bind* operation to verify that the remote server speaks LDAP. In contrast to our previous work, we now retrieve the Root DSE and store the raw data, which allows us to connect it to our new identification stage (see below). We craft a LDAP search request which limits the scope to the base entry node of the directory tree. This allows us to still retrieve important server attributes without carrying out an authentication process with actual credentials. The attributes we retrieve include vendor name, product version, supported versions of LDAP, and a number of vendor-specific attributes that allow us to identify LDAP servers that do not identify themselves in other attributes. In particular, it allows us to identify various LDAP products by Microsoft [17].

We extend Rapid7's *recog* tool [18] to analyze the attributes we receive (raw LDAP Root DSE entries). We extend it with 13 improved patterns where one (OpenLDAP) has been merged into Rapid'7s source code and 12 others (AD-related) are available in our repository. Importantly, this now also allows us to identify more LDAP products than prior work and, in many cases, also the operating system. To determine product lifecycle status (*e.g.,* unsupported versions), we contacted the vendors if no public documentation was available.

Networks hosting LDAP servers. We define the size of an Autonomous System (AS) as the number of announced IP addresses from routing information (see **data sources** below), *i.e.,* we aggregate over all its announced prefixes on 2024-10-29. An initial analysis shows that LDAP servers are seemingly distributed over networks and prefixes of all kinds and sizes, with no clear pattern discernible in which network segments or prefixes (of some size) of an AS they are hosted. To understand whether LDAP servers occur more commonly in networks or prefixes of particular sizes, we divide the identified, larger prefixes and networks into slices using the Pareto principle. We take an interval that corresponds to a network of a particular size and divide it into two sub-intervals. The exact position of the dividing line is the power of 2 that is closest to 80% of the interval size. We keep the 20% portion as one slice and then iteratively divide the remainder (80%) again, following the same rule. This results in a list of 20 intervals as shown in Figure 1. The largest slice we consider corresponds to networks that have between 2^{26} and 2^{27} IP addresses. The smallest slice corresponds to networks with up to 2^8 IP addresses, *i.e.,* a /24 prefix, which is also the smallest routeable prefix length on the Internet. As we show in Section IV, this division allows us to derive a clearer characterization of the hosting of LDAP servers across networks of various sizes.

X.509 certificates and cryptography. We use a custom tool written in Go to validate the X.509 certificates of LDAP servers. This proved necessary as existing tools implemented only a subset of our requirements, in particular fast, offline validation with checks for so-called cross-signing between CAs as well as custom inspection of self-signed certificates and intermediate certificates with the *CA* flag set. We use this feature set to investigate possible deployments of private PKIs. We consider the CAs in the major root stores: Apple, Java, Microsoft, Mozilla, Chrome, and Google Trust Services.

We perform a security analysis of the public key attributes of the certificates. We check if the public key length complies with the standards set by the CA/Browser forum, *i.e.,* we hold the certificates to the same standards that one would expect from Web connections. We check if a public key is flagged as insecure by *badkeys* [19], *e.g.,* susceptible to known attacks, and if the corresponding private key is known to the online database *pwnedkeys.com* [20].

Our measurements collect TLS connection data (implicitly and with StartTLS), including cipher suites and protocol versions. We evaluate the use of TLS by LDAP servers according to RFC 9325, correlating this with their hosters and the products we detect.

Data sources. For the IPs we identify as publicly accessible LDAP servers, we determine the corresponding ASes with *pyasn* and RIB data from RouteViews. We identify the network type (Internet Service Provider (ISP), data center/cloud, etc.) and hoster using the *ip2location* database. Note that one AS may have multiple network types, as this mapping is per prefix.

We used the Censys Universal Internet Data Set (CUIDS) from February 2022 to October 2024, with one snapshot per month, to verify the online presence of public-facing LDAP servers over time up to the time of our own measurement campaign. Here, we consider the IPv4 addresses that have LDAP service running on ports 389, 636, 3268, and 3269. Our own scans were necessary as Censys does not support LDAP StartTLS, which restricts our TLS analysis, and also does not include raw Root DSE responses, which we need for our product identification.

Limitations. Our focus is on publicly accessible LDAP servers. Hence, our results do not necessarily generalize to the (possibly much larger) population of LDAP servers in internal networks. We conduct our measurement campaign from a single vantage point in Europe. For geolocation and network type identification, we use the external database *ip2location*,

TABLE II
RESPONSIVE LDAP SERVERS BY PORT.

	Total	(Start)TLS
LDAP/389 only	53.1k	14.4k
LDAPS/636 only	12.1k	14.0k
...both LDAP/389 and LDAPS/636	23.0k	21.2k
Global Catalog/3268 only	21.5k	0.5k
Global Catalog/3269 over TLS only	0.5k	0.5k
...both Global Catalog ports	5.3k	5.3k

which means we share any bias it may have [21].

LDAP servers often do not reveal the vendor or product version, limiting our extended *recog* tool when different versions yield identical Root DSE responses. This is the case for newer versions of Microsoft's Windows Server (2019 and 2022). We are able to address this to some degree, however, if the server uses TLS 1.3, which is only available from Windows Server 2022 onwards [22]. Where another TLS version is used, we cannot distinguish between Windows Server 2019 and 2022. However, we note that both are fairly recent and still supported, unlike quite a few other products we identify in our scans. It is also worth noting that a more intrusive anonymous authentication and attempt to access more sensitive content on the LDAP server may have given us further identifying data—however, we refrain from doing this due to ethical concerns. We face similar issues with Kerio Connect and OpenLDAP, neither of which reveals the exact product version.

Ethics and Responsible Disclosure. We followed best practices for Internet measurements as previously documented [23]. In particular, we operate an abuse email address. We distribute our scans over a 24-hour period to minimize any impact. No sensitive information was collected. Our scan servers also host a Web server explaining our work, and we use appropriate, meaningful DNS PTR records. We received only a handful of requests to be excluded from our scans.

Following established responsible disclosure practices, we initiated a campaign to notify operators of compromised certificates, of which there are 74 from 11 CAs. We used the email addresses listed in the certificate's issuer email attribute for initial contact. We included details such as the serial numbers and a description of our methodology used to identify the weak certificates. As of the time of writing, we have not received any responses. We were unable to find the contact information for six compromised certificates.

IV. RESULTS

Table II shows how many servers were responsive on *at least one* of the ports we scanned. We find that about 93.9k public-facing LDAP servers respond with LDAP messages on at least one port, using either plaintext connections, StartTLS, or implicit TLS. This number is higher than we reported in prior work, as in this paper we broaden the scope to GC ports. Only 74.7k distinct IP addresses also respond to our Root DSE requests. Compared with the 2016 data by Rapid7 [8], we find 4.6×, 2.6×, 4.7×, and 5.1× fewer instances for ports 389, 636, 3268, and 3269, respectively.

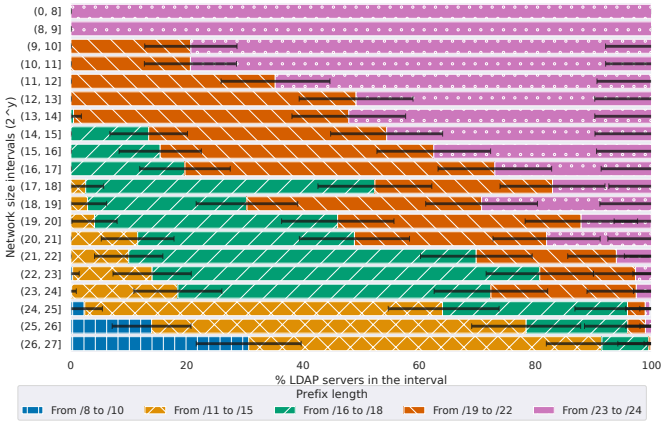

Fig. 1. LDAP servers by prefix length and hoster IP allocation with confidence interval of 95% (horizontal dark bars).

To determine whether the number of public-facing LDAP servers is falling, we carry out an analysis using the CUIDS data. We find an average of 107.5k servers over the previous years. Using linear regression, with high statistical confidence (p-value ≈ 0.0001), the trend is one of a decreasing number of public-facing LDAP servers, converging towards the numbers we identify in this paper. A plausible explanation for this reduction over time is that operators have recognized the problems with unintentionally public-facing LDAP servers and have corrected them.

A. Who hosts LDAP?

Fig. 1 shows the distribution of LDAP servers across network sizes, based on our slicing method (see Section III). Each row groups hosters by IP allocation size within a certain interval, *e.g.,* between 256 (2^8) and 512 (2^9) addresses (second row). Each horizontal bar represents the percentage of LDAP servers located in a routeable (sub-)prefix of a given length inside that allocation size interval.

For instance, nearly 40% of LDAP servers are in either /23 or /24 sub-prefixes, and a similar share is seen between /19 and /22 in hosters with an allocation size of 16k to 32k IPs. This suggests that hosters often place LDAP servers in dedicated network segments—a pattern that aligns with operational practices of service deployment. As the hoster size increases, the sub-prefixes tend to become longer (/16 to /18). The exception appear to be the very large hosters with more than 2^{24} ($\approx 16.7M$) IP addresses, which use longer prefixes.

With our geolocation and BGP data, we identify LDAP servers on 15.3k hosters in 9.4k ASes. The top 10 hosters account for 24% of the total LDAP population, and 2.2k hosters are responsible for 80%. Table III shows the most common hosters. This distribution is *significantly wider across several network operators*, compared to what other studies found for protocols for the Web, DNS, and email [3]–[5].

We find 46.1k (49.1%) LDAP servers in data centers and 37.0k (39.4%) in ISPs, similarly to what was reported in [2] (44.4k and 35.9k respectively).

We identify three categories among the top common hosters. Categories 1 and 2 include data centers and well-known host-

TABLE III
TOP HOSTERS OF LDAP SERVERS, THEIR NETWORK SIZE RANGE, MOST COMMON PREFIX THEY USE, AND USAGE OF AD.

Hoster	All	Network size	Dominant prefix	AD(%)
Category 1	12.6k			
...OVH	4.3k	$(2^{22}, 2^{23}]$	/16	62.5
...Hetzner	3.3k	$(2^{21}, 2^{22}]$	/16	41.0
...Contabo	2.2k	$(2^{18}, 2^{19}]$	/23	76.1
...home.pl S.A.	1.9k	$(2^{17}, 2^{18}]$	/18	2.7
...DigitalOcean	0.9k	$(2^{21}, 2^{22}]$	/20	3.7
Category 2	6.8k			
...Amazon	3.9k	$(2^{25}, 2^{26}]$	/15	47.6
...Microsoft	2.1k	$(2^{25}, 2^{26}]$	/11	89.9
...Aliyun	0.8k	$(2^{23}, 2^{24}]$	/16	35.1
Category 3	3.1k			
...Chunghwa	2.2k	$(2^{23}, 2^{24}]$	/16	29.7
...Comcast	0.9k	$(2^{26}, 2^{27}]$	/9	70.3
Total	93.9k			

ing providers, while Category 3 covers ISPs, responsible for 13%, 7%, and 3% of the LDAP servers we find, respectively. Category 1 is composed of smaller hosting providers (in terms of allocated IPs) than category 2. For each hoster in Table III, we provide the dominant prefix, *i.e.,* the network segment hosting the most LDAP servers. Furthermore, we observe the dominance of AD on the top hosters, except for home.pl and DigitalOcean. DigitalOcean does not offer native support to install Windows Server instances, only by uploading a private image to the VM [24]. We could identify only a small number of the LDAP products on home.pl.

Hosters in the first category have products such as Virtual Private Server (VPS), managed hosting, and/or dedicated hardware solutions, where customers manage their own environment. They also have between 2^{17} and 2^{23} IPs allocated. They host more LDAP servers than those in Category 2, which groups cloud providers offering hosted AD. Category 2 consists of large networks (between 2^{23} and 2^{26} IPs). The third category consists of access providers such as Chunghwa (Taiwan) and Comcast (USA), which are large ISPs that also offer custom business solutions. Neither offers hosted LDAP services accessible via public IP addresses.

B. What LDAP products are in use?

Overview. We verify our changes to the LDAP recognition software with a selected subset of Windows Server (2012, 2019, and 2022) and OpenLDAP instances running in our Universities (in the Netherlands and Germany) to confirm the correctness of our modified tooling. Table IV summarizes the LDAP products we encounter in our scans. We can identify 93% of all servers. The results show a tri-partite division. 47.6% of LDAP servers are AD products, including the Lightweight Directory Service (LDS) running on Windows. 33.5% are instances of OpenLDAP, which is free and open-source software (FOSS), with some running on Apple operating systems. Finally, a group (under 12%) is formed by other vendors, with Kerio Connect leading, followed by 389 Directory Server (FOSS and Fedora-based) and VMWare PSC. The latter is used to provide directory services and SSO functionality in the vSphere virtualization platform. It has been deprecated since 2020.

Our results differ from earlier studies, including our own [2]. We identify 35.9k instances of AD ($\approx$ eight times more), 1.8k instances of 389 Directory Server ($\approx$ 1.3 times more), and just 16 cases of Sun Java System Directory Server (more than 100 times fewer)—the latter is a discontinued LDAP server now known as Oracle Directory Server Enterprise Edition (ODSEE). We do not find ApacheDS (FOSS) or DICOM (a medical software that uses LDAP) instances in our dataset. There are a few reasons that may explain these discrepancies. We take measurements months later, include GC ports (commonly running AD), and use a different product identification methodology compared to our previous work. It is important to note that we identify 69.1k products compared to 10.7k from [2]. In [2], product identification was based on public lists of OIDs and vendor-specific attributes. In contrast, we extended a tool (*recog*) by Rapid7, which uses a comprehensive list of OIDs, attributes, and specific byte sequences from LDAP responses. Our numbers are best comparable to the Rapid7 blog of 2016 due to the use of *recog*. However, we believe that our numbers do not contradict the findings in [2] and are merely due to scanning more ports and having a more comprehensive tool to identify previously unknown deployments at our disposal.

Compared to Rapid7's 2016 work [8], Windows Server 2016 is now much more common (24.6k vs. 224 on port 389). We find 5.1, 3.5, 4.7, and 5.0 times fewer AD servers than Rapid7 on ports 389, 636, 3268, and 3269, respectively. OpenLDAP's absolute number decreased by more than half, while that of 389 Directory Servers has grown by a factor of 4.1. These may indicate a declining number of publicly accessible servers.

Active Directory. Newer Windows AD versions ($\geq$2012) are prevalent (31.9k, 88.9%). The versions from 2016 and later still receive free security updates. Customers of Windows Server 2012 who run instances outside of the Azure cloud can purchase extended support until the end of 2026.

We find that 99% of the AD instances on Windows Server, running on ports 3268 and 3269, have the LDAP attribute set that identifies them as instances of GC. We find only 20 instances of OpenLDAP, Kerio Connect, or 389 Directory Server on ports 3268/3269 with the attribute not set, *i.e.,* they are regular LDAP instances deployed in the GC ports.

Surprisingly, more AD servers use StartTLS–vulnerable to downgrade attacks–than implicit TLS. For versions older than 2012, StartTLS is twice as common; for $\geq$2012, four times. For GC, the gap widens to factors of 10 and 32, respectively.

OpenLDAP. Instances of this second-most-common product generally do not send sufficient data in the LDAP reply for a positive version identification; hence, we cannot break down our results by release year. However, as before for AD, we find that significantly more instances (65.9%) use StartTLS rather than implicit TLS. A possible reason may be an outdated FAQ by OpenLDAP that recommends StartTLS [25].

389 Directory Server. Almost all (1.6k out of 1.8k) servers run versions that have at least one CVE record assigned to

TABLE IV
LDAP PRODUCTS BY CATEGORY. NOTE THAT ROWS DO NOT ADD UP TO THE TOTAL DUE TO OVERLAP BETWEEN CATEGORIES.

Name	All	w/o TLS	w/ TLS	Global Catalog w/o TLS	Global Catalog w/ TLS
Category 1: Active Directory/Windows					
...MS ADC on Windows Server 2016/2019	24.6k	11.9k	7.4k	11.7k	3.4k
...MS ADC on Windows Server 2012 R2	4.9k	2.0k	1.9k	1.9k	1.0k
...MS ADC on Windows Server 2008 R2	2.7k	0.7k	1.6k	0.5k	0.9k
...MS ADC on Windows Server 2022	1.4k	0	1.4k	0	0.7k
...MS ADC on Windows Server 2000	0.8k	0.1k	0.7k	18	7
...MS ADC on Windows Server 2012	0.6k	0.2k	0.2k	0.2k	0.1k
...MS ADC on Windows Server 2008	0.3k	0.1k	0.1k	0.1k	0.1k
...Remainder in this category	0.6k	0.4k	0.2k	0.1k	38
Category 2: OpenLDAP	25.0k	7.6k	17.7k	0	3
Category 3: Less common products					
...Kerio Connect	4.8k	9	4.8k	0	13
...389 Directory Server	1.8k	0.1k	1.7k	0	4
...VMware PSC	1.3k	0.9k	1.2k	0	0
...Remainder in this category	0.4k	0.3k	0.1k	0	0
Category 4: no identification possible	5.6k	3.6k	2.0k	47	29
Total	74.7k	27.9k	40.9k	14.6k	6.3k

them, describing, for example, attacks on availability, information leakage, privilege escalation, forcing the use of a disabled cipher, or reading newly saved passwords in clear text.

VMWare PSC. According to Broadcom, versions 8.x, which account for 32% of the instances we find, have support until 2027, and versions 7.x (38%) until the end of 2025. However, version 6.x, which is still widely used (30%), has not been supported since March 2020.

Correlation to hosting. Fig. 2 shows LDAP products by common hosters. Below, we analyze them based on our categories (see Table III). In category 1, Hetzner's hosting options focus on Linux-based solutions, but the company also provides colocation services that allow customers to run their own servers, including Windows Server. This may explain the presence of many (both old and new) AD versions as well as OpenLDAP. OVH and Contabo offer options for recent versions of Windows Server AD alongside self-managed private servers. DigitalOcean offers several solutions but lacks native support of Windows Server. In contrast, installing OpenLDAP is a straightforward process, which may help explain its dominance. We are unable to identify the products of 97.1% of the LDAP on home.pl—among other reasons, there are too few entries in the Root DSE.

In category 2, unsurprisingly, Microsoft's IP ranges are dominated by AD versions with active support (≥2012). Amazon offers pre-installed virtual machines with various products through its Marketplace, which may help explain the balance of LDAP products we observe. Similar to Amazon, Aliyun offers Windows Server and Linux OSes via its Marketplace; however, we observe more OpenLDAP instances than other products. A plausible explanation for the differences we observe is that Microsoft's bundling of services and cloud infrastructure enables it to migrate its customers to newer versions, which may be more challenging for other hosters. Licensing considerations during upgrades may also play a role.

In category 3, Comcast and Chunghwa have the highest proportion of AD with unsupported versions compared to the other categories. Both are ISPs that allow business customers to run their servers on their networks.

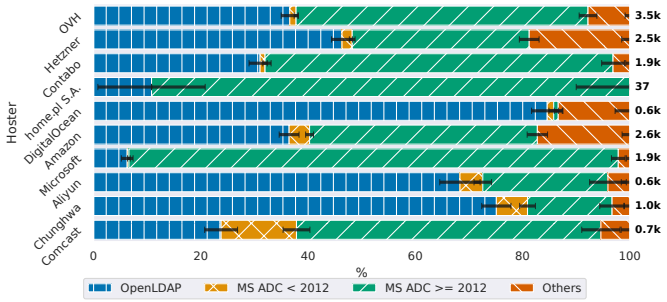

Fig. 2. Most common hosters vs. hosted LDAP products with confidence interval of 95% (horizontal dark bars).

TABLE V
VALIDATION OF CHAINS OF CERTIFICATES ACROSS LDAP PRODUCTS.

	Windows Server				
	All	< 2012	≥ 2012	OpenLDAP	Others
Valid chain	16.7k	0.4k	1.5k	7.8k	3.5k
Signed by unknown CA	15.4k	1.0k	6.1k	3.9k	2.1k
...Self-signed	3.6k	0.3k	1.8k	0.5k	0.4k
Expired/Not yet valid	8.8k	0.9k	2.2k	3.2k	1.3k
No valid leaf certificate	5.8k	32	44	2.3k	0.5k
Total	50.3k	2.6k	11.6k	17.7k	7.8k

We find 4.3k (5.8%) of LDAP servers running software past the end-of-life date. These appear in at least 5% of instances within Aliyun (5.4%, 42), Chunghwa (7.2%, 98), and Comcast (14.7%, 180). In absolute numbers, Comcast and Amazon host most outdated AD versions on Windows Server.

C. How does LDAP use PKI?

We investigate the certificate chains of 50.3k LDAP servers, of which 14.6k are duplicates (with 5k valid chains).

Validity of chains. Table V summarizes the cryptographic validity of the certificate chains (without checking the hostname). There is a significant difference between AD and other LDAP products. Valid chains are found in only 12.5% of recent AD versions and 15.3% of unsupported Windows Server

versions (pre-2012). For AD products, the most common reason is certificates where the root certificate is not in any of the root stores (52.7% for Windows Server $\geq$ 2012, 37.4% for $<$ 2012), with some cases of self-signed certificates (15.5% and 13% respectively). This is followed by expired certificates (18.8% and 33.1%, respectively). We find a higher percentage of valid chains for non-Microsoft products. For OpenLDAP, for instance, we find 44% valid chains; only 22.2% of chains have an unknown root certificate. However, the percentage of expired chains is similar to that of Windows products $\geq$ 2012. Self-signed certificates are rarer on OpenLDAP (2.6%).

The percentages for other LDAP products are generally closer to those for OpenLDAP than to AD. We also find invalid chains where every certificate in the chain has the *CA* attribute set to true, *i.e.,* declares itself to be a root or intermediate certificate. In other words, there is no leaf certificate in the chain. This occurs rarely in AD (76 cases) and is more common in OpenLDAP (13.1%) and other products (6.4%).

We observe that valid chains are more common on hosters from category 1 (see categories in III), with at least 34% of their LDAP servers. The exception is home.pl, with no significant number of instances using TLS. From category 2, Amazon has the most valid chains, which is in contrast to Aliyun and, surprisingly, Microsoft ($<$23%). Invalid chains are prevalent among hosters in category 3 ($>$ 88%), which may be an indication of problems that small organizations face in managing PKI. Compared to our findings, prior studies reported 30–40% valid chains for HTTPS [15] and TLS-enabled email protocols [16], with notably fewer self-signed certificates for the latter, while chat protocols also showed few valid chains ($\leq$30%).

Certificate management practices. These findings raise the question of whether specific certificate management practices are in use. As there are no standards or documented best practices, it is not trivial to verify the existence of in-house CAs. We hence inspect the *subject* fields of 200 randomly selected root certificates of chains that LDAP servers offer.

In our sample, 168 certificates contained placeholder values (*e.g.,* "CN=TurnKey OpenLDAP" and "O=Default Company Ltd") in the subject, or the subject consisted of gibberish or placeholder content, *i.e.,* the subject names indicate a non-existing domain name. In the remaining 32 certificates, we find the names of real companies from different sectors, *e.g.,* pharma, ICT, and civil construction. In 5 cases, we see an indication that the certificate is from a company's CA, *i.e.,* contains "CA" in the subject, *e.g.,* "Pingzapper CA". Our manual inspection did not reveal statistically significant evidence for attempts to run a private PKI professionally.

Validity period of certificates. Unlike the Web, where the lifetime of certificates has been consistently reduced (13 months, and 90 days in the case of Let's Encrypt), there are no standards for the lifetimes of X.509 certificates for LDAP.

We analyze the validity period of *valid* chains. Except for just four cases (three certificates issued by a Finnish CA and one by SSL.com), all certificates have lifetimes of no more than 13 months. Certificates with expiry times of $\leq$90 days (short-lived certificates) occur in 8.4k valid chains. Of these, 97.8% are issued by Let's Encrypt. OpenLDAP instances account for 4.5k (68%) servers. Short-lived certificates are much less common for AD (any version) with just 425 (6.4%). The validity period of *invalid* chains varies from one to thousands of years. Similar numbers have been reported for the Web [26] and contribute to our overall finding of a lack of well-managed private PKIs.

Other notable certificate issues. We use *badkeys* [19] and *pwnedkeys.com* [20] to identify 81 certificates with compromised keys. Of these, 71 certificates have a key listed on *badkeys* (the private key is known), where nine are keys affected by the Debian SSL vulnerability (CVE-2008-0166) and 62 certificates share the same hard-coded default 512-bit RSA key known from a specific firmware image (all with the same issuer). The public keys in the remaining 10 certificates have corresponding private keys in pwnedkeys.com and should no longer be used. In total, the 81 affected certificates share 20 unique keys. We find that CAs not in the root stores sign 60 certificates containing a compromised key, 18 are no longer valid, and two have no valid leaf certificates. Only one certificate has a trusted chain and is issued by Sectigo. Further analysis reveals that the certificate is not only used on the LDAP server but also on the website of the associated domain. We reported this issue to the website operator. We find that the compromised certificates are used mainly on Windows servers: 59.3% were deployed on Microsoft AD on Windows Server 2000, 19.8% on OpenLDAP instances. We could not identify the otherating system for the remaining 20.9%.

There are 5.8k (11.6%) certificate chains where all certificates in the chain have the *isCA* flag set, a surprisingly high number. We manually inspect the intermediate certificates of 200 certificates. We find properly formatted entries showing real businesses ("Holitec Computers Ltd" and "max-crc GmbH") as well as indications of private NAS devices ("QNAP Systems, Inc.") and careless entries ("CN=mail").

D. How does LDAP use TLS?

We find 50.3k unique servers that use TLS, 2.1k (4.4%) more compared to [2]. In the following, we analyze the cipher suites that LDAP servers selected in TLS handshakes and correlate this with the common hosters and products.

Support for TLS. We find that many AD instances are not configured to use TLS. Of the nearly 30k instances of recent versions (Table IV, rows 1-2), over half do not enable TLS. The ratio is even worse for GC instances (3:1). Interestingly, the opposite is true for Windows 2022 and also *older* versions, such as Windows 2000 and 2008 R2. AD instances with no TLS usage are mostly found in data centers (52.3%) and ISPs (38.4%), less so in cloud-ready solutions. We find different relations for other LDAP products. OpenLDAP servers with TLS outnumber those without by more than 2:1. Nearly all KerioConnect and 389 Directory Server enable TLS.

We find that only 1.6k LDAP instances (3.3%) use deprecated TLS versions (1.1 and 1.0), 27.2k use TLS 1.2, and 21.5k use TLS 1.3. This aligns with findings for the Web [14].

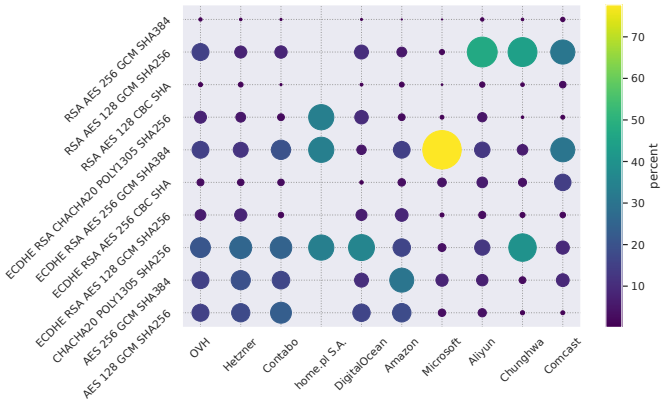

Fig. 3. Percentage of the top 10 cipher suites negotiated with servers on important hosters. The last three entries are TLSv1.3 and use ECDHE for key exchange. These ciphers cover 98% of what servers selected in our data.

Cipher suites. AD instances on Windows Server versions $\geq$ 2012 commonly use Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) as the key exchange mechanism, with TLS 1.2 used in 10.2k cases (87.6%) and TLS 1.3 in 1.4k cases (12.4%). This follows current recommendations [27]. We observe 2.4k cases of newer AD using Cipher Block Chaining (CBC) encryption and the SHA1 algorithm, more than older Windows Server (1k) or OpenLDAP instances (0.5k). SHA1 is in phase-out and CBC does not offer authenticated encryption.

Correlation to hosting. Fig. 3 shows the correlation between common LDAP hosters and cipher suite selection. RSA key exchange is rare in Microsoft's networks, which typically favor secure setups using TLS 1.2, AES at 256 bits in Galois Counter Mode, and a SHA-2 hash function at 384 bit.

We find a diverse set of cipher suites on Hetzner, OVH, Amazon, and Contabo (category 1 in Table III), as expected on VPS-focused providers aimed at self-hosting. The LDAP instances on these hosters use TLS 1.3 with modern ciphers significantly more often. This is in contrast to a study of 2020 [14], which tracked the deployment of TLS 1.3 on the Web. The hosters of our Category 1 are significant actors in the deployment of the new TLS version. From category 2, we observe that Amazon and Microsoft have a clear preference for the RFC-recommended ciphers, while Aliyun has a wider spread, with a few deployments using deprecated ciphers. Hosters in Category 3 use more deprecated ciphers, providing yet another indication that organizations face issues with configuring TLS properly.

V. Discussion and Recommendations

Networks hosting LDAP. The public-facing LDAP ecosystem shows few signs of centralization. There is a wide range of hosters: the top 10 account for only 24% of all instances, and 2.2k hosters account for 80% of LDAP servers. LDAP deployment contrasts with other, more centralized ecosystems such as the Web, email, and DNS. Focusing on the scattered hosting of LDAP, the variety of issues we found among self-managed solutions indicate that the maintenance of such LDAP servers is complex (compared to, *e.g.,* a rollover and upgrade mechanism from a cloud provider). In particular, we find much evidence for outdated software.

Our analysis reveals that LDAP clusters are present in certain subprefixes across networks of varying sizes. The subprefixes where LDAP are found may be shared with different services. From an operator's perspective, it can be advisable to isolate the deployment of LDAP servers to a specific network segment, also using firewalls. This practice can enhance security as it allows operators to prevent unauthorized traffic from accessing critical network segments. In a broader sense, different types of customers of a hosting company or ISP could be in isolated networks.

We recommend network operators use our tools to regularly survey their attack surface and to increase awareness of servers running on known ports, as also advised by Rapid7 [8]. By doing so, they can identify exposed, vulnerable servers and ultimately initiate campaigns to remove their online presence. Additionally, network operators can use our tools to identify LDAP servers and the network segments in which they are operated and isolate them from other critical services or customers. Network operators can also identify where access attempts to LDAP servers in their network originate and block unauthorized clients. We recommend that network operators who self-manage solutions perform regular updates or look for solutions with easy upgrade paths.

Product lifecycle. We identified 69.1k LDAP products, with 4.3k deprecated. The latter servers are (sometimes long) overdue for an upgrade. Our findings indicate that several LDAP servers continue to operate on outdated Windows Server versions, such as 2012 or older, increasing the risk of exposure to known vulnerabilities. Such servers should be migrated to more recent releases, for example, Windows Server 2022, as version 2016 is already under an extended support period. This also highlights the risk to individuals who rely on organizations that run outdated systems. Users may unknowingly rely on an outdated LDAP server where credentials are stored for authentication. Credential theft could occur if such an outdated server is compromised.

Network operators are hence advised to take the task of keeping their networks safe from deprecated services seriously. With our tool set, they can effectively identify deprecated LDAP deployments and even extend it to fit their purpose, such as live monitoring or easy access via a dashboard. Our suggestion is to ensure that old LDAP software is identified, isolate it in a more specific network segment, and initiate communication with the administrator of the LDAP server to patch their software.

Communication security. We analyzed server-side TLS support and the certificates used. LDAP servers are still using cipher suites that are no longer recommended, and there is a low number of valid certificate chains. We identified a small number of compromised certificates as well. The TLS configuration of LDAP servers is a metric that an operator can use to determine the security of their network.

Despite the low number of servers using deprecated TLS versions, a considerable number of them still do not follow

best practices with cipher suites. We recommend that LDAP administrators use a robust certificate management system on public-facing LDAP servers, such as those for the Web. Use of deprecated TLS version, legacy cipher suite, and poor LDAP PKI are also symptoms of old LDAP instances. These metrics help operators to identify unreliable LDAP deployments and ultimately enhance the network security by implementing the measures we have recommended so far.

Finally, network operators can also consider going beyond their infrastructure. Ensuring proper management of their own LDAP servers contributes to the overall security posture of the Internet, but equally important is awareness of poorly maintained deployments in other networks. For example, organizations that rely on external service providers or federated authentication systems may be indirectly affected by outdated or misconfigured LDAP servers outside their administrative domain. Therefore, network operators should be aware that problems in their supply chain may arise.

VI. Conclusions and future work

In this work, we provide a large-scale characterization of hosting and security practices of public-facing LDAP servers. Our findings show a diverse LDAP ecosystem with 15.3k hosting organizations, including many self-managed solutions. This diversity also increases the complexity of maintenance. We find evidence for outdated software, deprecated TLS configurations, and vulnerable certificates, which supports the idea that network operators and LDAP administrators face difficulties in keeping their systems secure. To address these issues, we recommend that network operators adopt systematic monitoring and upgrade strategies, isolate deprecated instances, and follow established best practices for TLS and certificate management. We aim to raise awareness among researchers and network operators about a more secure ecosystem, and we invite the community to extend this research by conducting qualitative or quantitative surveys on server maintenance.

Acknowledgment

We thank the reviewers for their valuable feedback. We thank Benjamin Othmer for his precursory study using Censys data. We acknowledge the support of *IP2Location*, *pwnedkeys.com*, and Censys for providing access to their data. This work was partially funded by the Netherlands Organisation for Scientific Research project CATRIN (NWA.1215.18.003), the research project "North-Rhine Westphalian Experts in Research on Digitalization (NERD II)", sponsored by the state of North Rhine-Westphalia —NERD II 005-2201-0014, 'Cyber Security Incident Response für KMUs (CySIRK)' (13FH101KB1) of the German Federal Ministry of Education and Research (BMBF), and by the National Research Center for Applied Cybersecurity ATHENE.

References

[1] G. Öndarö, J. Kaspereit, S. Umezulike, C. Saatjohann, F. Ising, and S. Schinzel, "S/MINE: Collecting and Analyzing S/MIME Certificates at Scale," in *USENIX*, Aug. 2025.

[2] J. Kaspereit, G. Öndarö, G. L. Cesar, S. Ebbers, F. Ising, C. Saatjohann, M. Jonker, R. Holz, and S. Schinzel, "LanDscAPe: Exploring LDAP weaknesses and data leaks at internet scale," in *USENIX*, Aug. 2024.

[3] T. V. Doan, R. van Rijswijk-Deij, O. Hohlfeld, and V. Bajpai, "An empirical view on consolidation of the web," *ACM Trans. Internet Technol.*, feb 2022.

[4] G. C. M. Moura, C. Gañán, Q. Lone, P. Poursaied, H. Asghari, and M. van Eeten, "How dynamic is the isps address space? towards internet-wide dhcp churn estimation," in *IFIP Networking Conference*, 2015.

[5] E. Liu, G. Akiwate, M. Jonker, A. Mirian, S. Savage, and G. M. Voelker, "Who's got your mail? characterizing mail service provider usage," in *ACM Internet Measurement Conference*, Nov. 2021.

[6] A. Ashcraft, S. Cai, D. Coulter, M. Jacobs, and M. Satran, "Global Catalog - Win32 apps," https://learn.microsoft.com/en-us/windows/win32/ad/global-catalog, Aug. 2020.

[7] CA/Browser Forum, "Latest Baseline Requirements," https://cabforum.org/working-groups/server/baseline-requirements/requirements/, Aug 2025.

[8] T. Sellers, "Project sonar study of ldap on the internet: Rapid7 blog," https://www.rapid7.com/blog/post/2016/11/08/project-sonar-study-of-ldap-on-the-internet/, Nov 2016.

[9] P. Bulusu, H. Shahriar, and H. M. Haddad, "Classification of lightweight directory access protocol query injection attacks and mitigation techniques," in *International Conference on Collaboration Technologies and Systems (CTS)*, 2015.

[10] S. Srinivasa, J. M. Pedersen, and E. Vasilomanolakis, "Deceptive directories and "vulnerable" logs: a honeypot study of the ldap and log4j attack landscape," in *EuroS&PW*, 2022.

[11] Akamai, "What Is a CLDAP Reflection DDoS Attack?" https://www.akamai.com/glossary/what-is-a-cldap-reflection-ddos-attack, accessed 2025-06-17.

[12] D. Poddebniak, F. Ising, H. Böck, and S. Schinzel, "Why TLS is better without STARTTLS: A security analysis of STARTTLS in the email context," in *30th USENIX Security Symposium*, Aug. 2021.

[13] Z. Durumeric, D. Adrian, A. Mirian, J. Kasten, E. Bursztein, N. Lidzborski, K. Thomas, V. Eranti, M. Bailey, and J. A. Halderman, "Neither snow nor rain nor mitm...: An empirical analysis of email delivery security," in *IMC*, 2015.

[14] R. Holz, J. Hiller, J. Amann, A. Razaghpanah, T. Jost, N. Vallina-Rodriguez, and O. Hohlfeld, "Tracking the deployment of tls 1.3 on the web: A story of experimentation and centralization," *Computer communication review*, vol. 50, no. 3, Jul. 2020.

[15] Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman, "Analysis of the https certificate ecosystem," in *ACM IMC*, 2013.

[16] R. Holz, J. Amann, O. Mehani, M. Wachs, and M. Ali Kaafar, "Tls in the wild: An internet-wide analysis of tls-based protocols for electronic communication," in *NDSS*, 2016.

[17] B. Mathers, J. Flores, A. Buck, B. Lamosa, and Alex-Catalin, "Microsoft Entra Connect Sync: Attributes synchronized to Microsoft Entra ID," https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/reference-connect-sync-attributes-synchronized, Jun 2023.

[18] Rapid7, "Recog: A recognition framework," Github rapid7/recog, 2014.

[19] Hanno Böck, "badkeys," https://badkeys.info/, [n. d.].

[20] pwnedkeys.com, "pwnedkeys," https://pwnedkeys.com/, [n. d.].

[21] IP2Location, "IP geolocation capabilities: Myths and facts," Apr. 2024.

[22] A. Ashcraft, T. Clark, J. Krynitsky, M. Howard, T. Shores, V. Vissoultchev, suntsu42, K. Sharkey, and M. Satran, "Protocols in TLS/SSL (Schannel SSP) - Win32 apps," https://learn.microsoft.com/en-us/windows/win32/secauthn/protocols-in-tls-ssl--schannel-ssp-, Jan. 2024.

[23] Z. Durumeric, E. Wustrow, and J. A. Halderman, "ZMap: Fast internet-wide scanning and its security applications," in *USENIX*, Aug. 2013.

[24] DigitalOcean, "Does digitalocean host windows servers?" https://www.digitalocean.com/community/questions/does-digitalocean-host-windows-servers, Aug 2020.

[25] OpenLDAP, "OpenLDAP Faq-O-Matic: Start TLS v. ldaps://," https://www.openldap.org/faq/data/cache/605.html, [n. d.].

[26] R. Holz, L. Braun, N. Kammenhuber, and G. Carle, "The ssl landscape: a thorough analysis of the x.509 pki using active and passive measurements," in *ACM IMC*, 2011.

[27] Y. Sheffer, P. Saint-Andre, and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)," RFC 9325, Nov. 2022.