When BGP Security Meets Content Deployment: Measuring and Analysing RPKI-Protection of Websites

Matthias Wählisch
Freie Universität Berlin
waehlisch@ieee.org

Robert Schmidt
Freie Universität Berlin
rs.schmidt@fu-berlin.de

Thomas C. Schmidt
HAW Hamburg
t.schmidt@ieee.org

Olaf Maennel
Loughborough University
olaf@maennel.net

Steve Uhlig
Queen Mary, U. of London
steve@eecs.qmul.ac.uk

ABSTRACT
Web content delivery is one of the most important services on the Internet. A secure access to websites is typically granted via SSL. However, traffic hijacking on the network layer may break this security model and makes additional protective mechanisms necessary. This paper presents a first quantitative analysis of the protection of web servers by RPKI, a recently deployed Resource Public Key Infrastructure to prevent hijacking in the Internet backbone. We introduce an initial methodology that accounts for distributed content deployment and shall enable the content owners to estimate and improve the security of the web ecosystem. For a current snapshot, we find that less popular websites are more likely to be secured than the prominent sites. Popular websites significantly rely on CDNs, which did not start to secure their IP prefixes. Whenever CDN-content is protected by RPKI, it is located in third party ISP networks. This hesitant deployment is the likely cause why popular content experiences reduced security.

Categories and Subject Descriptors
C.2.2 [Computer-Communication Networks]: Network Protocols—Routing Protocols

Keywords
BGP, RPKI, secure inter-domain routing, deployment, web content, CDN

1. INTRODUCTION
Websites often disappear, when BGP misconfiguration (or prefix hijacking) occur [1,3]. In the worst case, traffic hijacking is used to implement forged SSL certificates. Even though such incidents have not been clearly documented [4] and the SSL vulnerability can be mitigated by DANE [5], twisting BGP reduces service availability of the Web ecosystem—this has been experienced multiple times.

The relevance of websites in social and business critical operations challenges a comprehensive security provisioning. In particular, the network operators of popular sites should be given protective mechanisms at hand. The Resource Public Key Infrastructure (RPKI) is a new framework that enables BGP routers to perform prefix origin validation, and when active prevents incidents such as the YouTube hijack. On the same time, the web is a complex ecosystem with multiple players. The content owner has only limited influence on the delivery infrastructure. This is foremost valid for popular sites as their deployment is usually outsourced to CDNs, which distribute content into many autonomous systems. We know from IPv6 deployment that such companies are slower adaptors of new Internet technologies than smaller ISPs or webhosters. In our case, this leads to less protected popular content but better protected unpopular content.

In this paper, we conduct a first quantitative analysis of the deployment of securing web servers by RPKI. We map the IP addresses of 1M Alexa domains to IP prefixes and evaluate if these prefixes are part of the RPKI infrastructure. Our findings can be summarized as follows:

1. Less popular websites are commonly better secured than websites with many visitors.

2. CDNs tend to ignore RPKI, whereas ISPs and webhosters started RPKI deployment.

3. CDN content that is not placed in CDN networks benefits from these earlier adopters.

4. CDN deployment policies are the likely cause for a reduced security level at prominent websites.

The remainder of this paper is structured as follows. Section 2 details the problem space and our measurement methodology. Section 3 discusses our findings, and Section 4 briefly surveys related work. Section 5 concludes with an outlook.
2. X-RAYING RPKI & WEB DEPLOYMENT

2.1 Why the Web Ecosystem Challenges
Network Security Measurements

Vulnerability of BGP The Border Gateway Protocol (BGP) [6] governs the inter-domain routing of the Internet. BGP exchanges announcements of the service to reach IP prefixes between Autonomous Systems (ASes). An AS represents a set of prefixes that it originates. ASes are identified by unique Autonomous System Numbers (ASNs). Larger ISPs service multiple IP prefixes as well as several ASes [7].

Prefix information are carried in unprotected update messages—BGP is based on mutual trust. A BGP speaker may announce any IP prefix and receiving peers cannot validate the origin of the prefix. The injection of incorrect BGP data into the Internet backbone by intention or by misconfiguration is easy by design. Some heuristic prediction methods, e.g., [8,9] have been developed for discovering illegitimate announcements but tend to fail in cases of multiple origin ASes (MOAs) or require active probing. To overcome the attack model of prefix hijacking, a cryptographically strong certification system is required that attests the ownership of ASNs and prefixes as well as the legitimate origination of an IP prefix by an AS.

Secure Prefix Origin Validation The Resource Public Key Infrastructure (RPKI) [10] is a PKI framework dedicated to securing the Internet routing infrastructure. It includes certificates that prove the ownership of Internet number resources (ASNs and IP prefixes). Certification of resources follows the hierarchy of Internet resource allocation. The IANA issues certificates for RIRs (e.g., RIPE), RIRs for LIRs (e.g., ISPs), and LIRs for end users [11]. All certificates are included in a distributed, openly accessible repository.

Resource certificates attest that its holder is legitimate to use the described resources. The Internet routing decouples the ownership of resources and their deployment. A prefix owner may ask an ISP to route its prefix, for example. Further on, a resource certificate does not bind the mapping of an IP prefix to an origin AS. This is implemented by Route Origin Authorization (ROA) objects. A ROA authorizes an autonomous system to originate one or multiple prefixes. It is signed with the private key of an RPKI certificate which cryptographically confirms that the signer is the legitimate holder of these prefixes.

Using ROA data, an RPKI-enabled router is able to verify the BGP updates it receives. The prefix information within the BGP update might be valid (i.e., the origin AS is allowed to announce this prefix), invalid (i.e., the origin AS is incorrect or the announced prefix is too specific), or not found (i.e., the announced prefix is not covered by the RPKI). Rejecting an invalid route helps to successfully suppress an incorrectly announced prefix, which finally secures network layer reachability of services assigned with an IP address of this prefix.

It is worth noting that invalid routes might also appear due to misbehaving RPKI authorities [12] or misconfiguration [13] of the RPKI. In this paper, we do not consider why a BGP route is invalid as we are primarily interested in the RPKI-coverage of the web server infrastructure.

Web Ecosystem The web ecosystem basically consists of the following components. The end user requests a web page from the content infrastructure, which is delivered via the underlying network. The web page belongs to a specific domain name (e.g., www.google.com). To successfully reach the content infrastructure two steps are necessary: (a) a valid mapping of the domain name to a host address and (b) the correct routing of the host’s prefix within the BGP. DNSSEC [14] ensures valid name to address mapping. This paper focuses on the routing layer.

In the simplest case, a web page is hosted on a single web server situated in a single autonomous system. The prefix owner then needs to create a single RPKI entry for the prefix-AS pair, which hosts the domain. However, highly popular content (i.e., web pages with many visitors) is often distributed among several web servers to increase availability and performance. With the advent of Content Delivery Networks (CDN), these web servers are not only reachable via different IP prefixes but also placed in different ASes. To fully secure the web server infrastructure of the domain, all prefix-AS pairs need to be included into the RPKI. It is worth noting that content provided by CDNs is not necessarily located in the AS of the CDN, in which case the CDN has no control over the authorization of this AS. We will show that end users benefit from diverse deployment, since CDNs—in contrast to larger ISPs—do not protect their IP prefixes so far.

In addition to asking where content is located in the network, the question about relevance is of concern. The Alexa list [15] ranks websites according to their popularity in terms of estimated visitors. Unfortunately, Alexa aggregates all sub-domain names to the second level. google.com for example is merged into maps.google.com. In this example, the two domains obviously offer different content and it may be reasonable to assume a distinct hosting.

On the contrary, it is also common to use different domain names for the same content, most prominently adding the prefix www to the second level domain name. Usually, one of the names redirects to the other. The redirection is not necessarily based on DNS canonical names, but also on HTTP redirects [16]. In such cases, the initial HTTP GET request on a w/o www domain may point to a different infrastructure, even though the
content is finally provisioned by the same servers that host the www domain (or vice versa). Our analysis focuses on RPKI protection and thus needs to consider the first contact point where misconfiguration may become effective. The distinction between www and w/o www domain may be of lesser importance for measurements that only care about actual content location.

We summarize our discussion with a concrete example of the complexity of the current web ecosystem and its implications for RPKI measurements. (cf. Fig-ure 1). When a web client requests http://audi.com from a host at Berlin IXP, the domain is resolved to 143.164.100.143. The corresponding IP prefix is originated by AS 12331 (Audi). The web server sends an HTTP redirect to 62.156.238.22, which is operated by AS 3320 (DTAG). In contrast, resolving www.audi.com directly leads to 62.156.238.22 via several canonical DNS names. The web server behind 62.156.238.22 is operated by Akamai. From a deployment perspective this illustrates that a CDN has only limited influence in achieving full RPKI protection for a domain name. From a methodology perspective it clarifies that both domain names should be analyzed.

2.2 Methodology

Our measurement study proceeds in four steps: (1) selection of websites, (2) mapping domain names to IP addresses, (3) mapping these IP addresses to IP prefixes routed in the Internet and their origin ASes, (4) validating the BGP information against RPKI. We now describe our methodology, which is meant to be simple and widely reproducible, in detail.

1 Selecting Domain Names Domain names in our measurement are taken from the Alexa list, which encompasses 1M entries. Alexa domain names are commonly applied in measurement studies (e.g., [17–20]), as there is no global directory or other striking alternatives. Using them eases reproducibility. In addition, the Alexa list provides indications of the domain popularity.

2 Mapping Domains to IP Addresses The distributed nature of DNS may lead to answers that vary between locations. Requesting the address record of the same domain name from different resolvers may return different IP addresses. This has become even more prevalent in the context of web hosting, where CDNs introduce location-specific DNS replies. In this paper, we decided against launching a data collection campaign or using multiple open recursive DNS servers to request the same name from different vantage points. We restrict our analysis to data from public DNS servers (e.g., GoogleDNS) as they allow for timely and continuous measurements.

Several projects use Open Recursive DNS servers (ORDNS). However, most of these hosts are very instable and do not provide reliable answers, because the majority of the entries refer to CPE devices (e.g., [21]). Our tests showed that the same set of hosts can work well for a short time, but go off-line or return errors a few days later. Based on this observation, we exclude those compilations as they do not allow to reasonably reproduce our measurements. In contrast, DNS Looking Glasses and the Google DNS as well as Open DNS are free and stable global DNS resolution services operated for the public. In Section 3 we show that our RPKI results remain independent of the DNS server selection. Analyzing the effects of many vantage points will be part of our future work.

We collect all A, AAAA, and CNAME records for the Alexa domain names [15], including the names appended with the prefix www. We exclude all invalid DNS answers, i.e., all special-purpose IPv4 and IPv6 addresses reserved by the IANA.

To briefly analyze the overlap between www and w/o www domains, we quantify the amount of equal prefixes per domain. Figure 2 shows that for the first 100k domains more than 76% of the IP prefixes equal for both
names, for the remaining domains more than 94% of the names refer to the same prefix. To accelerate continuous DNS measurements, it is sufficient to resolve only one type of name.

(3) Mapping IP Addresses to Prefixes and ASNs
We combine dumps of the active tables of the RIPE RIS route servers. For each IP address of a domain name, we extract all covering prefixes and derive the origin AS from the AS path (i.e., the right most ASN in the AS path). Note that entries with an AS_SET are excluded from our study as this leads to an ambiguity of the attribute, why the function is deprecated with the deployment of RPKI [22].

(4) RPKI Validation
For the validation of the BGP data, we follow the necessary steps to perform origin validation at BGP routers. ROA data of all trust anchors (APNIC, AfriNIC, ARIN, LACNIC, and RIPE) are collected and validated. Only cryptographically correct ROAs are further used to check the IP prefixes obtained from the BGP table dumps.

To summarize (cf., Figure 3), for each domain name in the Alexa list that can be resolved from our DNS vantagepoint, we create a list of IP prefixes and origin ASes visible within RIPE RIS and assign an RPKI validation state based on the currently deployed set of ROAs. We will make the data publicly available as there are no reasons for privacy or ethical concerns.

Our approach does not measure the protection of embedded web content (e.g., photos that are located under a different domain compared to the landing page). Security incidents in the past [1, 3] showed that routing failures usually affect complete web pages instead of content pieces, which justifies our current focus.

3. RESULTS
After resolving 1M Alexa domains from a host in Berlin via GoogleDNS and excluding 0.07% incorrect DNS answers, we gathered 1,167,086 IP addresses for the www domains and 1,154,170 IP addresses for the w/o www domains. These addresses are mapped to 1,369,030 and 1,334,957 different prefix-AS pairs respectively. 0.01% of the IP addresses are not reachable from our BGP vantage points.

We repeated the DNS measurements over several weeks and also resolved the domain names via Open DNS and us01 of the DNS Looking Glass [23]. For these two different DNS resolvers we found very similar results compared to GoogleDNS.

In the following subsections, we first present the core RPKI validation outcome, and second work out reasons for the observed deployment state. For better visibility, we do not present results per domain but apply a binning of 10k domains in all graphs. As a domain name may refer to multiple IP addresses, which belong to different IP prefixes and ASes, several RPKI states may exist per domain. To represent heterogeneous RPKI deployment, we assign corresponding probabilities to domain names (e.g., 3/5 RPKI coverage of foo.bar).

3.1 Basic RPKI Insights: Infrastructure of less popular sites is more secured
On average, 6% of the web server prefixes are covered by the RPKI (either correctly or incorrectly announced in the BGP) and 94% are not secured (cf., Figure 4(a)). Roughly 0.09% of the prefixes are invalid according to the RPKI prefix origin validation. This observation is
in qualitative agreement with the general RPKI deployment. Note that the current invalid BGP announcements do not necessarily indicate hijacking but rather misconfiguration [13]. The amount of invalids is evenly distributed among all web domains.

Looking into RPKI protection in more detail shows that the portion of RPKI coverage correlates with the popularity of websites Figure 4(b). Domains with a low rank (i.e., popular sites) are less likely secured than domains with a high rank. Among the first 100k domains (e.g., google.com), for only \( \approx 4.0\% \) of the web server prefixes an origin validation can be performed. In contrast, for the last 100k domains \( \approx 5.5\% \) are secured. We admit that the absolute numbers are small, but a clear trend is visible and may reflect the deployment strategy of different stakeholders, which we now try to clarify.

### 3.2 CDN-Content benefits from security by third party ISPs

Popular websites are mainly hosted by CDNs like Akamai, whereas less prominent sites are placed on web servers from a common webhosting service, or on self-maintained servers connected via some third party ISPs like DTAG or Sprint. Following this, we conjecture that CDNs are more hesitant in deploying RPKI for their IP prefixes. To study this interrelation, we inspect the RPKI repository and search for attestation objects that belong to the ASes of well-known CDNs (i.e., Akamai, Amazon, Cloudflare, Cotendo, Edgescan, Highwinds, Instant, Internap, Limelight, Mirrorimage, Netdna, Simplecdn, and Yottaa). It is worth noting that the results of this approach do not depend on DNS measurements and thus do not include a bias which might result from our DNS measurement point. This approach does not consider the case where CDNs own provider independent (PI) address space, which is assigned to ASes of third party ISPs. However, to the best of our knowledge this kind of deployment is not implemented.

For the 199 ASes of the considered CDNs, we only found four entries in the RPKI. These four prefixes are owned by Internap and tied to three origin ASes. Considering the large number of CDN operators, as well as Internap operating at least 41 ASes, this is a very low coverage. On the one hand, we conclude that CDNs tend to not actively participate in the creation of RPKI attestation objects, which is in contrast to webhosters or common ISPs. On the other hand, the results do not show that all CDN-content is only accessible via unprotected prefixes.

CDN content is not exclusively located within CDN network infrastructure, but also placed in third party ISP networks, and thus inherits RPKI deployment there. To quantify this collateral effect, we conduct a very basic classification of CDN domains. Often CDNs use CNAME chains (Canonical Names) to direct DNS requests to their internal end points. We say a domain is served by a CDN, if the IP address of its domain name is indirectly accessed via two or more CNAMEs (e.g., `www.huffingtonpost.com\rightarrow www.huffingtonpost.com\rightarrow edgesuite.net\rightarrow a495.g.akamai.net\rightarrow 212.201.100.136`). We question this rough heuristic by comparing its results with an independent classification provided by HTTPArchive. HTTPArchive classifies the first 300k Alexa domains based on DNS pattern matching of CNAMEs, which is distinct from our test of DNS indirections. Furthermore, the HTTPArchive monitoring agent is located in Redwood City, CA, USA, and thus a geographically separated vantage point.

Figure 5 compares the distributions of CDN-hosted web domains as determined by our classification approach and HTTPArchive. The two almost identically shaped curves clearly indicate that popular websites are more likely to be served by CDNs. Quantitatively, our approach indicates fewer CDNs than HTTPArchive. This is not surprising, since there is CDN deployment without CNAME chains. However, a conservative (under)-estimate of CDN domains sharpens our view on the RPKI-protection of CDN domains: (Over-)enlarging the set of CDN domains will mix deployment cases and diffuse the overall picture.

### 3.3 CDNs likely to cause reduced security of the popular Web

We now focus our analysis on the relation between RPKI-enabled and CDN-served content. We want to examine our earlier conjecture that hesitant deployment at CDNs is the dominant reason for the observed trend that popular sites are less protected. Figure 6 depicts the distribution of RPKI-enabled content under the condition that it is CDN-served. In contrast to the Alexa
domains at large, RPKI deployment is fairly independent of the rank for CDNs. Results fluctuate around an average of ≈ 9 %/per thousand zero. This is almost an order of magnitude lower than the overall RPKI deployment rate, which is plotted for comparison.

Combining the line of arguments, we could show that (a) CDN deployment is strongly enhanced for popular domains, but (b) RPKI deployment on CDN content is low—independent of its popularity. As a result, a high density of CD sites reduces the RPKI-enabled portion of domains. This holds for those ranks of the Alexa list where CDNs are more common: the low ranks of high popularity. Our argumentation is roughly reflected in numbers. The presence of CDNs is enhanced by about 2 % at the lower Alexa ranks, where RPKI deployment is reduced by about the same 2 % In summary, we take this as a strong support of our hypothesis that the observable degradation of routing security for popular websites is caused by the resistance of CDN operators to adopt RPKI.

4. RELATED WORK

The deployment of RPKI started in 2011. Several looking glasses and tools exist [24-28] to inspect the current state of deployment or to do experiments, but up until now only few publications studied the current state of deployment in detail. [13] analyzes the RPKI validation outcome of entire BGP tables trying to better understand invalid BGP announcements. [12] discusses the risk when RPKI authorities misbehave, and [29] explores the general limitations of current secure inter-domain routing protocols. Nevertheless, large ISPs such as Deutsche Telekom and ATT added their IP prefixes to the RPKI, which motivates the relevance of this new protocol framework. The motivation to adapt new Internet protocols is analyzed in [30], with a special focus on secure inter-domain routing in [31,32]. Our work complements these insights by clarifying that CDN-content benefits from early RPKI-adoptin in large ISP networks.

Several measurement studies discovered the content distribution space (e.g., [17,33,35]). We emphasize that the aim of this paper is not to reveal the hosting infrastructure completely but to present a trend analyse of RPKI adoption in the wild and its interplay with the web ecosystem by applying a very basic methodology.

5. CONCLUSION AND OUTLOOK

In this paper, we analyzed the RPKI-protection of websites. We resolved IM domain names from the Alexa ranking (including names appended with the ukv prefix), mapped the IP addresses to IP prefixes and origin ASes visible in the global BGP routing table, and validate each prefix-AS pair against the currently deployed RPKI data.

We found that RPKI security deployment is significantly degraded for the more popular websites, which led us to applying a new, initial methodology for discovering its reasons.

Our findings revealed that CDN hosters are the likely cause for this operational bias. Their enhanced provenience at prominent web domains on the one hand, and their obvious reluctance towards RPKI deployment on the other hand strongly indicate that prominent websites would be better protected against routing attacks without CDNs.

In future work, we will aim to explore why CDNs implement this operational behavior. We will compare RPKI deployment with the adoption of other core protocols such as DNSSEC. Furthermore, we will look in more detail if provider independent address space is actually not used by CDNs in the web ecosystem.

6. REFERENCES


