Internet Security Report 2019

By Rayhaan (AS210036)

Topics

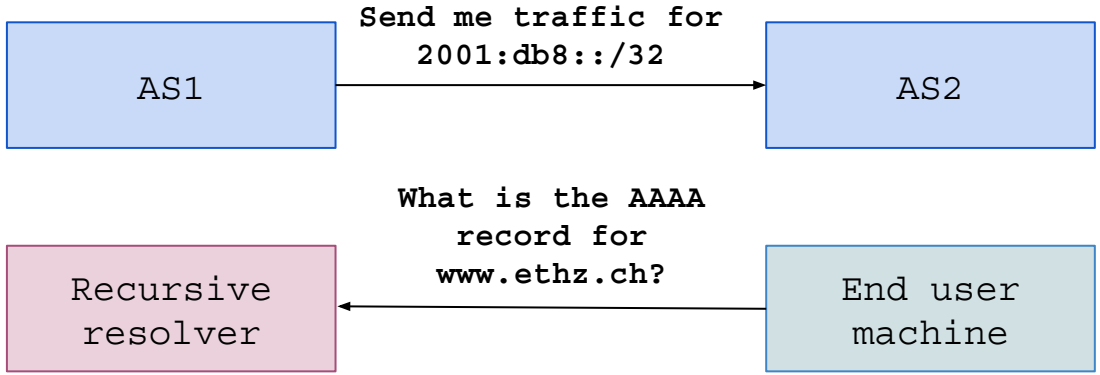
→ Interdomain routing security

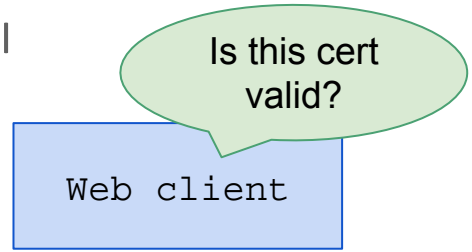
→ RPKI

→ BGPSec

→ Naming Security (DNS)

→ PKI





Why should I care about infrastructure security?

- Current setup is a patchwork of fixes on top of broken infrastructure

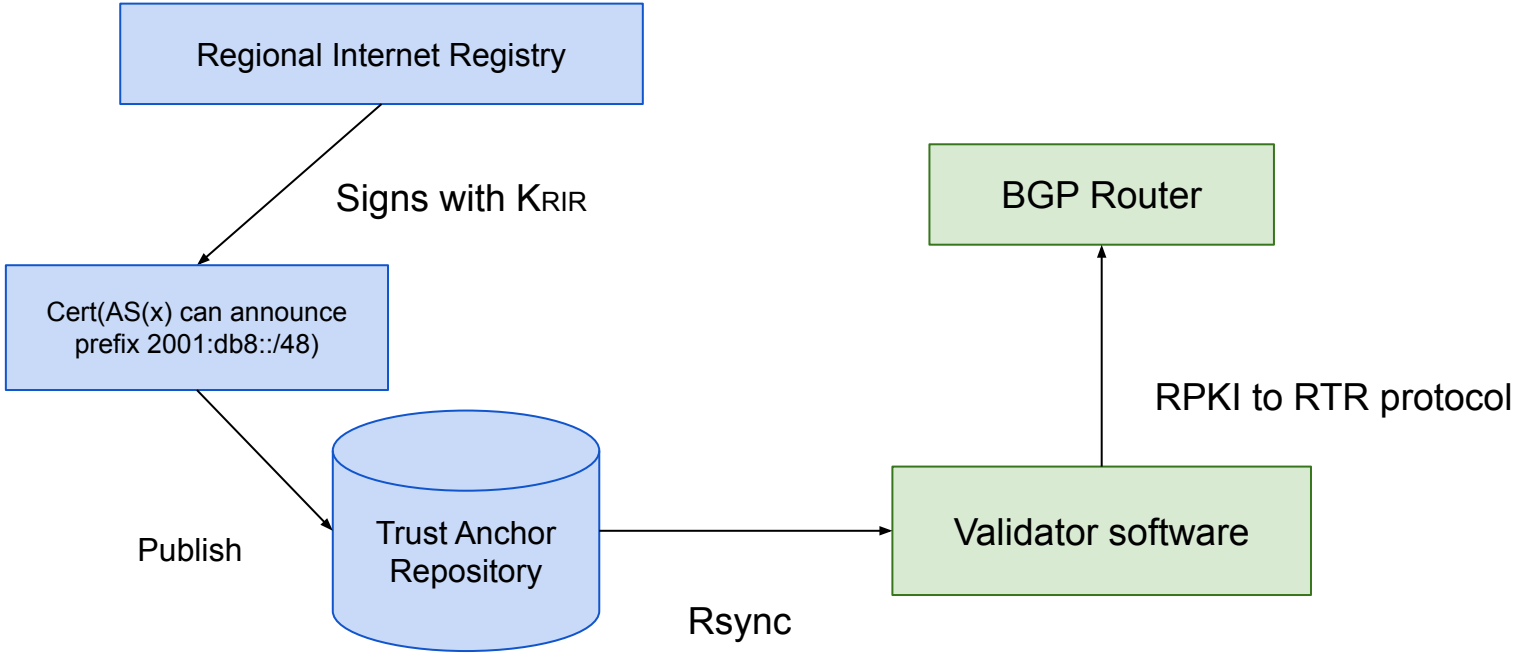
- Is application layer security enough?
  - Does TLS give us everything we want? Non TLS protocols?
  - Do you check the SSH fingerprint when connecting to a new machine, out of band?
  - Information is still leaked by other protocols such as DNS.

Interdomain routing security

Resource Public Key Infrastructure (RPKI)

- Certification of Internet resources by RIRs.
- Proof that a certain AS is authorized by the resource owner to announce those resources.
- Only works to curtail accidental announcements, not malicious ones where the attacker announces a false AS path.

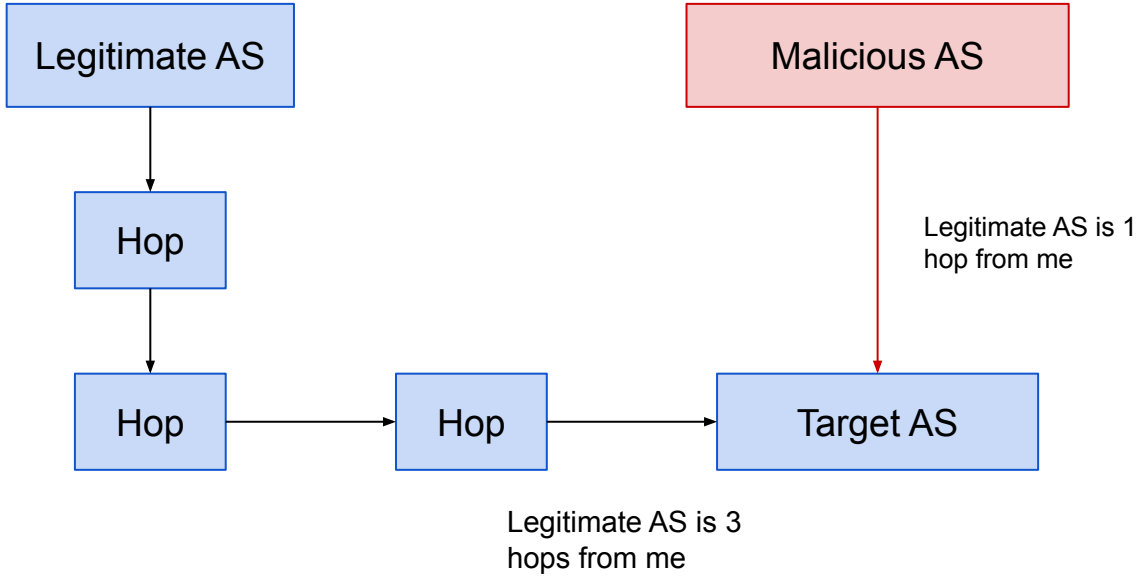
How RPKI is deployed



Properties obtained from RPKI

- Safety from accidental announcements, configuration mistakes which leak prefixes,
- Lays the groundwork for cryptographic verification of routes (via BGPSec, covered later)

RPKI does not itself prevent attacks



BGPSEC

Builds upon RPKI to leverage certificate infrastructure to secure BGP announcements end to end.

Leverages trust anchors and certificates from RPKI to cryptographically verify the path.

M_1 :=

```
Source AS: x
Path: [x]

Signature: [Sig_kx(source AS, Path, Sig: [])]
```

M_2 :=

```
Source AS: x
Path: [x, y]

Signature: [Sig_kx(...), Sig_ky(..., Sig[m1.Signature])]
```

M_3 :=

```
Source AS: x
Path: [x, y, z]

Signature: [Sig_kx(...), Sig_ky(...), Sig_kz(...)]
```

Properties of BGPSEC

+ End to end confidence that the path verified is not forged (modulo key compromise).
+ Same as RPKI: authorization to announce a certain prefix by the designated owner.
- Higher computational overhead at each hop to sign the messages
- Single point of failure / kill switch?

BGPSec kill switch debate

+ Small set of authorities means more resources to protect those assets

+ Simplified interactions for all parties (i.e. no state explosion like TLS with many anchors)

- Single point of failure to take down the internet

- Target for attackers / people wanting to disrupt routing

- What about jurisdiction, can a government of the country an RIR is hosted in request revocation of other peoples prefixes?

BGPSec kill switch debate

Should we move to a more globally stable model BUT accept the risk of a global kill switch

OR

Stay in the current state with no global kill switch BUT no local attack protection.

Public Key Infrastructure

What is wrong with PKI?

- How can we tell if a certificate is the one the website owner really controls and has not been compromised?
  - With many CA's it is relatively easy for an attacker to compromise it and issue a fraudulent certificate?
  - How can a compromised certificate be efficiently revoked?

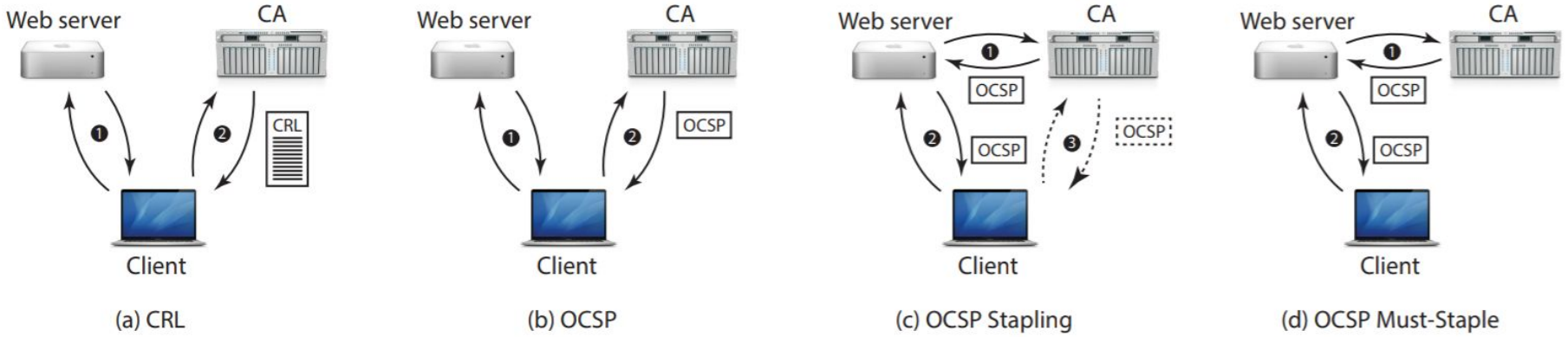
- Privacy issue: A passive eavesdropper can collect domain names being connected to.

Certificate Transparency

- Logs all issued certificates to create a global repository of all valid certificates,
- Website owner can monitor logs to know if fraudulent certificates have been issued,
- Only helps for detection, but better than nothing.

Certificate revocation?

- Online Certificate Status Protocol (OCSP) was intended to check certificate validity, by querying a OCSP server from the client…



OCSP must-staple

Is the Web Ready for OCSP Must-Staple?

Taejoong Chung*
Rochester Institute of Technology

Jay Lok
Northeastern University

Balakrishnan Chandrasekaran
Max Planck Institute for Informatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and
Akamai Technologies

Alan Mislove
Northeastern University

John Rula
Akamai Technologies

Nick Sullivan
Cloudflare

Christo Wilson
Northeastern University

IMC '18, October 31-November 2, 2018, Boston, MA, USA

https://mislove.org/publications/OCSP-IMC.pdf

TLS-SNI

Server Name Indication (SNI) allows a TLS server to know which certificate to serve.

Domain request is sent in plaintext.

TLS-SNI attempts to encrypt this: https://datatracker.ietf.org/doc/draft-ietf-tls-esni/

Put the public key in DNS...

DNS security

DNS over HTTPS / TLS (DoH / DoT)

Plain DNS provides no protection against eavesdropping or modification of request / response contents.

Tunneling DNS over an encrypted transport solves the information leakage problem.

Still not the default for regular users, adoption growing on mobile with Android support.

Blockers for widespread DoH adoption

- Lack of support in end user operating systems,
- Lack of support in ISP issued CPE,
- How to configure DoH resolvers?

DNSSEC

Properties:

- Cryptographic validation of DNS records from the root to leaf nodes

Why are we not there yet:

- Where to perform the validation?
- How to let the user know the result?
- Does the user need to know?

Questions?