Team demonstrates that basic mechanism for internet security can be broken

October 5 2022, by Cornelia Reitz

Credit: Pixabay/CC0 Public Domain

The National research center for Cybersecurity ATHENE has found a way to break one of the basic mechanisms used to secure internet traffic. The mechanism, called RPKI, is actually designed to prevent cybercriminals or government attackers from diverting traffic on the internet.

Such redirections are surprisingly common on the internet, for example, for espionage or through misconfigurations. The ATHENE scientist team of Prof. Dr. Haya Shulman showed that attackers can completely bypass the security mechanism without the affected network operators being able to detect this. According to analyses by the ATHENE team, popular implementations of RPKI worldwide were vulnerable by early 2021.

The team informed the manufacturers, and now presented the findings to the international expert public.

Misdirecting bits of internet traffic causes a stir, as happened in March this year when Twitter traffic was partially diverted to Russia. Entire companies or countries can be cut off from the internet or internet traffic can be intercepted or overheard.

From a technical point of view, such attacks are usually based on prefix hijacks. They exploit a fundamental design problem of the internet: The determination of which IP address belongs to which network is not secured. To prevent any network on the internet from claiming IP address blocks they do not legitimately own, the IETF, the organization responsible for the internet, standardized the Resource Public Key Infrastructure, RPKI.

RPKI uses digitally signed certificates to confirm that a specific IP address block actually belongs to the specified network. In the meantime, according to measurements by the ATHENE team, almost 40% of all IP address blocks have an RPKI certificate, and about 27% of all networks verify these certificates.

As the ATHENE team led by Prof. Dr. Haya Shulman discovered, RPKI also has a design flaw: If a network cannot find a certificate for an IP address block, it assumes that none exists. To allow traffic to flow on the internet anyway, this network will simply ignore RPKI for such IP address blocks, i.e., routing decisions will be based purely on unsecured information, as before. The ATHENE team was able to show experimentally that an attacker can create exactly this situation and thus disable RPKI without anyone noticing. In particular, the affected network, whose certificates are ignored, will not notice it either. The attack, called Stalloris by the ATHENE team, requires that the attacker controls a so-called RPKI publication point. This is not a problem for state attackers and organized cybercriminals.

According to the investigations of the ATHENE team, at the beginning of 2021 all popular products used by networks to check RPKI certificates were vulnerable in this way. The team informed manufacturers about the attack.

Now the team has published its findings at two of the top conferences in IT security, the scientific conference Usenix Security 2022 and the industry conference Blackhat U.S. 2022. The work was a collaboration between researchers from ATHENE contributors Goethe University Frankfurt am Main, Fraunhofer SIT and Darmstadt University of Technology.

More information: Attack description: blog.apnic.net/2022/06/15/stal … pki-downgrade-attack

Conference: www.usenix.org/conference/usenixsecurity22

Conference: www.blackhat.com/us-22/

Provided by Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE

Citation: Team demonstrates that basic mechanism for internet security can be broken (2022, October 5) retrieved 13 March 2024 from https://techxplore.com/news/2022-10-team-basic-mechanism-internet-broken.html