Security gaps identified in internet protocol IPsec

August 15 2018

Credit: CC0 Public Domain

In collaboration with colleagues from Opole University in Poland, researchers at Horst Görtz Institute for IT Security (HGI) at Ruhr-Universität Bochum (RUB) have demonstrated that the internet protocol IPsec is vulnerable to attacks. The internet key exchange protocol IKEv1, which is part of the protocol family, has vulnerabilities that enable potential attackers to interfere with the communication process and intercept specific information.

The research results are published by Dennis Felsch, Martin Grothe and

Prof Dr. Jörg Schwenk from the Chair for Network and Data Security at RUB, and Adam Czubak and Marcin Szymanek from Opole University on 16 August 2018 at the Usenix Security Symposium, and are available on their blog.

Secure and encrypted communication

As an enhancement of internet protocol (IP), IPsec has been developed to ensure cryptographically secure communication via publicly accessible insecure networks, such as the internet, by using encryption and authentication mechanisms. This type of communication is often used by enterprises whose employees operate from decentralised workplaces—for example, as sales reps or from a home office—and need to access company resources. The protocol can also be used to set up virtual private network (VPNs).

In order to enable an encrypted connection with IPsec, both parties must authenticate and define shared keys that are necessary for communication. Automated key management and authentication, for example, via passwords or digital signatures, can be conducted via the internet Key Exchange protocol IKEv1.

"Even though the protocol is considered obsolete and a newer version, IKEv2, has been long available on the market, we see in real-life applications that IKEv1 is still being implemented in operating systems and still enjoys great popularity, even on newer devices," explains Dennis Felsch. But this protocol has vulnerabilities, as the researchers found during their analysis.

Bleichenbacher's attack successful

In the course of their project, the researchers attacked the encryption-

based logon mode of IPsec by deploying the so-called Bleichenbacher's attack, which was invented in 1998. In this attachl, errors are deliberately incorporated into an encoded message, which is then repeatedly sent to a server. Based on the server's replies to the corrupted message, an attacker can draw progressively better conclusions about the encrypted contents.

"Thus, the attacker approaches the target step by step until he reaches his goal," says Martin Grothe. "It is like a tunnel with two ends. It's enough if one of the two parties is vulnerable. Eventually, the vulnerability permits the attacker to interfere with the communication process, to assume the identity of one of the communication partners, and to actively commit data theft."

Bleichenbacher's attack proved effective against the hardware of four network equipment providers. The affected parties were Clavister, Zyxel, Cisco and Huawei. All four manufacturers have been notified, and have now eliminated the security gaps.

Passwords under scrutiny

In addition to the encryption-base logon mode, the researchers have also been looking into password-based login. "Authentication via passwords is carried out with hash values, which are similar to a fingerprint. During our attack, we demonstrated that both IKEv1 and the current IKEv2 present vulnerabilities and may be easily attacked—especially if the password is weak. Accordingly, a highly complex password provides the best protection if IPsec is deployed in this mode," says Grothe. The vulnerability was also communicated to the Computer Emergency Response Team (CERT), which coordinates the response to IT security incidents. CERT provided assistance to the researchers as they notified the industry about the vulnerability.

The identified Bleichenbacher vulnerability is not a bug per se, but rather an implementation error that can be avoided—it all depends on how manufacturers integrate the protocol in their devices. Moreover, the attacker must enter the network before in order to exploit this vulnerability. Nevertheless, the researchers' successful attack has demonstrated that established protocols such as IPsec still include the Bleichenbacher gap, making them potentially vulnerable to attack.

More information: Dennis Felsch, Martin Grothe, Jörg Schwenk, Adam Czubak, Marcin Szymanek: The dangers of key reuse: practical attacks on IPsec IKE, 2018, Online preview: www.usenix.org/conference/usen … /presentation/felsch

Provided by Ruhr-Universitaet-Bochum