Chapter 12
DNSSEC vs. DNSCurve: A Side-by-Side Comparison

Marios Anagnostopoulos
University of the Aegean, Greece

Georgios Kambourakis
University of the Aegean, Greece

Elisavet Konstantinou
University of the Aegean, Greece

Stefanos Gritzalis
University of the Aegean, Greece

ABSTRACT

Without a doubt, Domain Name System (DNS) security is a complicated topic of growing concern. In fact, it can be argued that the whole Internet infrastructure depends on the smooth operation of the DNS service. Despite this fact, the original DNS design concentrated on availability, not security, and thus included no authentication. Nowadays, this security gap has been addressed by two cryptographic mechanisms: DNSSEC and DNSCurve. They both utilize public key cryptography and extend the core DNS protocol. Although the second mechanism is still in its infancy while the first is well-standardized, they are both promising and are quite likely to compete with each other in the near future to gain acceptance. This work aims to provide a comprehensive and constructive comparison between the aforementioned security mechanisms. Towards this direction, the authors theoretically cross-evaluate and assess the benefits and the drawbacks of each particular mechanism based on several distinct criteria. This is necessary in order to decide which mechanism is the best fit for each particular deployment.

INTRODUCTION

The Domain Name System (DNS) (Mockapetris, 1987a; Mockapetris, 1987b) is probably the most critical service in the Internet as it translates domain names into the numerical IP address of any network host. One can say that DNS is found virtually everywhere in the Internet. Today, an apparent example where DNS plays a vital role is cloud computing. In fact, cloud computing has been with us for many years. It is the provision of computational resources on demand over a
network which up until now has usually been a corporate local area network. However, the advent of the widespread availability of cheap broadband connections to the Internet is set to change our experience of the cloud. The computational resources accessed do not need to exist on a local area network and may exist on the network of a service provider accessed over an Internet connection. This gives rise to dramatically different business models for the provision of computing resources at the corporate level and to the home. In particular, the maintenance tasks associated with making an application available can be outsourced. The potential implications of this are currently the subject of much discussion within the popular media. For network professionals, more significant is the fact that taking cloud computing outside of the corporate network potentially allows company staff to access applications that are not feasible on the corporate network for reasons of cost or deployment complexity. This has major implications for situational awareness. Network professionals will need to more extensively monitor the use of cloud resources over the Internet by company staff. However, the starting point for all discussions associated with the outsourcing of business critical information services over the Internet is availability. Setting aside issues that may arise with the service provider, if business critical computational resources can only be accessed over the Internet then the availability of Internet connection to those resources is a fundamental consideration. Internet connection depends on the smooth operation of the DNS service. Moreover, since any other popular service, i.e. web, mail, ftp etc relies on smooth DNS operation, its potential vulnerabilities could set at risk the secure usage of any other Internet application that depends on the proper operation of the DNS service. Of course, DNS security is complicated and of widespread concern.

Despite its crucial significance, DNS still suffers from the same vulnerabilities that it had at the beginning of its deployment. Potential attackers aim to exploit the lack of protection mechanisms and corrupt or undermine the integrity of the authoritative responses. For instance, DNS does not provide origin authentication of DNS data leaving the system open to Denial of Service (DoS) attacks. Although the motivation for DNS-oriented attacks varies, the ultimate goal of any aggressor is to provide misleading or bogus data to the end-user. Usually, however, the attackers aim to be gain financially, e.g. by identity theft, or cause DoS. In such an attack incident, called DNS cache poisoning, the attacker tries to deceive the resolvers of the service into accepting and storing forged DNS data in their cache. Consequently, the end-users based on these resolvers are redirected to fake sites instead of what they requested. As already mentioned, the consequences could be identity theft, malware infection, DoS and other similar risks. Eventually, successful cache poisonings could change the way end-users experience the Internet and expose them to a variety of serious threats.

In order to make cache poisoning and other similar attacks very difficult to perform, two long-term security mechanisms are proposed, namely DNS Security Extensions (DNSSEC) and DNS-Curve that utilize public key cryptography and extend the core DNS protocol. The first mechanism was initially proposed in 1997 with RFC 2065 (Eastlake, Kaufman, 1997). Since then, several modifications have been introduced that lead to the current version of the protocol, known also as DNSSEC-bis. This new version is described mainly in RFC 4033 (Arends et al., 2005a), RFC 4034 (Arends et al., 2005b) and RFC 4035 (Arends et al., 2005c). On the other hand, DNSCurve was recently proposed (Bernstein, 2009b; Bernstein, 2009c) by Daniel J. Bernstein and is part of a major project to deploy public key cryptography, and specifically Elliptic Curve Cryptography (ECC), in every Internet packet. The purpose of this effort is to protect the confidentiality and the integrity of all transactions for each protocol used in the Internet. Unfortunately, so far DNSCurve has not
Related Content

An Entropy-Based Architecture for Intrusion Detection in LAN Traffic
www.igi-global.com/chapter/entropy-based-architecture-intrusion-detection/60436?camid=4v1a

A Threat-Response Model of Counter-Terrorism: Implications for Information Security and Infrastructure Risks
www.igi-global.com/article/a-threat-response-model-of-counter-terrorism/106028?camid=4v1a

Mitigation of Identity Theft in the Information Age
www.igi-global.com/chapter/mitigation-identity-theft-information-age/13510?camid=4v1a

Malware Detection and Prevention System Based on Multi-Stage Rules
www.igi-global.com/article/malware-detection-and-prevention-system-based-on-multi-stage-rules/87413?camid=4v1a