Case study

Hardware-based DNSSEC Signing – Turning Domain Administrators into Gatekeepers of the Internet

More than 25 years ago, when the Internet was first invented, nobody really thought to include security checkpoints. Fast forward a few years and we've all learned the lesson that anyone with bad intentions and some technical skill can accomplish severe harm to the core on which the Internet is built: the Domain Name System (DNS). DNS is a distributed naming system that associates and navigates information by translating domain names to numerical IP addresses.

The Domain Name System Security Extensions (DNSSEC) is a worldwide initiative to develop a set of add-on specifications to ensure that the information we transmit through the Internet is kept safe and private. DNSSEC technology prevents fraudulent domains, or websites, by creating a unique signature for every domain name. By matching the user with the correct website, attacks can be avoided such as phishing, when user data—such as payment details—are redirected to third party servers via fake websites.

The new gatekeepers of the Internet are the enablers of DNSSEC Signing. Groups of servers all over the Internet store information about domain names in readable open text

to be able to direct user traffic. After applying DNSSEC Signing, the data remains readable but a unique signature has been generated to sit on top of the data to authenticate or reject traffic requests.

In Lithuania, the Kaunas University of Technology is responsible for top-level domain .lt. As an official Administrator of the .lt domain, the University opted for Utimaco's hardware security module (HSM) technology to turn the domain into a DNSSEC protected zone.

Utimaco's FIPS-certified hardware security module (HSM) generates and stores secure digital signatures that are required for authorizing communication commands between the domain, the server, and the user. Each cryptographic signature is generated via true random number generation, www.utimaco.com which enables cryptographic keys that are truly unique and that cannot be accessed by a third party. In comparison, software-based cryptographic keys can be captured in the moment of unlocking – offering attackers the ability to learn the software, exploit vulnerabilities and run attack remotely.

With the help and guidance of Utimaco partner Altacom, the Kaunas University of Technology successfully deployed a hardware-based DNSSEC Signing solution to ensure .lt top-level domain administration principles and procedures are upheld. With Utimaco's HSM, the University is able to generate domain signatures that ensure user privacy and cryptographic keys that can withstand any kind of attack—whether digital attacks via the Internet or physical attacks to the hardware box itself.

About Utimaco

Utimaco is a leading manufacturer of hardware based security solutions that provide the root of trust to keep cryptographic keys safe, secure critical digital infrastructures and protect high value data assets. Only Utimaco delivers a general-purpose hardware security module (HSM) as a customizable platform to easily integrate into existing software solutions, embed business logic and build secure applications. Tens of thousands of enterprise and infrastructure companies rely on Utimaco to guard IP against internal and external threats and protect hundreds of millions of consumers globally.

Visit Utimaco at: https://hsm.utimaco.com/

About KTU

KTU is one the largest technological universities in the Baltics. Known for its linkages with business, leadership in scientific research, flexible interdisciplinary study programmes and unforgettable study experience, KTU is fast forwarding to becoming an internationally acknowledged institution of higher education. Since its establishment in 1922, University has had more than 130,000 graduates.

Visit http://ktu.edu/en for further information.