WHITE PAPER

Communications Service Providers
Network Security

Understanding the SSL/TLS Adoption of Elliptic Curve Cryptography (ECC)

The demand for data encryption is growing, and so is ECC because it is better for mobile devices, but data centers need to plan for high-capacity encryption/decryption traffic. Radware* has a line of products optimized for high-demand ECC encryption environments.

radware
Every second counts

Introduction: Encryption Grows as the Internet Becomes Darker

One arbiter of the growth in encrypted traffic is the percentage of pages loaded over encrypted HTTPS links by Chrome users, as reported in the Google Transparency Report. The report shows encryptions levels for five operating systems (Windows, Android, Chrome OS, Linux, and MacOS). As reported in November 2017, the percentage of visits to encrypted sites grew steadily from 2015 through 2017, from at most 44 percent to at least 63 percent.[1]

Some of the reasons for the accelerated adoption of secure socket layer (SSL) traffic encryption include the following:

- The growing need for privacy has driven many online services such as Facebook* and Twitter* to encrypt client sessions.
- Google has added encryption for most of its online services including YouTube,* Gmail,* and even search engine sessions.
- Streaming media services such as Netflix* are now using encrypted communication to stream videos.
- Enterprises are adopting encryption as a best practice as they move their applications to the cloud.
- The adoption of HTTP/2 in late 2015 mandates the use of SSL from start to end in every session.

These trends mean data centers now need to process more encrypted traffic than ever before, and not all devices in data centers can accommodate this growing demand in SSL processing.

The Mobile Challenge (CPU Power, Battery, Privacy)

The extensive use of mobile devices is a key challenge to increased encryption. Computing power availability per dollar has increased by a factor of 10 roughly every four years in the last quarter of a century.[2] This means that the computing power hackers require to crack encrypted keys of a certain size becomes more readily available. Thus, there is a need to increase the size of encryption keys so that they can remain secure.

However, longer encryption keys take more computational resources to process, and that is becoming a challenge for mobile and Internet of things (IoT) devices,

Table of Contents

Introduction 1
The Mobile Challenge 1
Introducing Elliptic Curve 2
Radware's* Alteon D-line* with Intel® Technology 3
Radware Encryption Product Families. 3
Summary 4
About Radware 4
About Intel® Network Builders. . . . 4

which often have limited memory and CPU power resources. These devices also have fixed battery power, and encrypting and decrypting data places a burden on the amount of battery power required to process that traffic. This is an important factor moving the industry to look for a more processor and battery efficient traffic encryption technology.

Introducing Elliptic Curve: A Safer Traffic Encryption Protocol that Reduces Computational Requirements

The solution to reducing the computing and battery impact of encryption on mobile devices starts with the encryption protocol. Elliptic curve is an emerging standard that promises these benefits. To better understand the impact of elliptic curve, let's review today's encryption landscape.

SSL/TLS Overview

The standard security technology for establishing an encrypted link over the Internet is known as secure sockets layer/transport layer security (SSL/TLS). These cryptographic protocols ensure that all data passed between the server and its clients remain private and integral. SSL/TLS is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.

These protocols cover three main processes:

1. **Mutual authentication** (ensuring the identity of each party). Client and server use one of the following authentication algorithms (digital signatures) to authenticate each other:
   - RSA
   - Elliptic Curve Digital Signature Algorithm (ECDSA)
2. **SSL/TLS handshake for key exchange.** The SSL/TLS handshake enables the SSL or TLS client and server to agree on a shared secret key that they will use to encrypt/decrypt the data (symmetric encryption). The main methods used to establish a shared secret key (key exchange) were based on Diffie-Hellman and RSA cryptographic algorithms. Recently, a new cryptographic algorithm was introduced, called elliptic curve (which incorporates Diffie-Hellman but uses more advanced elliptic curve mathematics to generate its keys).
3. **Traffic encryption/decryption.** Application traffic transferred between client and server is encrypted/decrypted using the shared secret key established in the previous step and a symmetric key cipher like AES, ChaCha20, 3DES.

The mutual authentication and key exchange processes, which are public-key cryptography (also known as asymmetric cryptography) algorithms, are resource intensive, both in terms of CPU and memory. This is why the industry was looking for a new algorithm and standard that is computationally lighter for public key exchange.

What Is Elliptic Curve Cryptography? How Does It Help?

Elliptic curve cryptography (ECC) is an approach used for public key encryption that utilizes the mathematics behind elliptic curves in order to generate security between key pairs. Equations based on elliptic curves are relatively easy to perform but extremely difficult to reverse. In cryptography, this is a very valuable characteristic since it offers greater security while requiring less computational resources.

ECC employs a relatively short encryption key, which means there is less processing required, making it better suited for mobile devices. For example, a 256-bit ECC encryption key provides the same security as a 3,096-bit RSA encryption key.[3]

The smaller key size and lower processing requirements make elliptic curve cryptography a good fit for devices that are low on computational resources and memory such as mobile and IoT, enabling them to also consume very little battery power.

Data Center Challenges of Adopting ECC

Adopting ECC on the client side is as easy as upgrading your browser to its latest version. It will potentially bring all the benefits associated with the new ECC cyphers, including low power consumption for batteries, assuming that the server side would do the same.

However, in a data center environment, the situation is a bit different. The number of encrypted transactions per second that need to be processed is much larger, and in most cases software-based SSL processing is not enough. In such cases, hardware-based acceleration engines are used (normally incorporated in application delivery controllers—ADCs) to cost-effectively handle high volumes of encrypted traffic.

While hardware SSL cards have been doing a good job accelerating the RSA key exchange process, they were never designed to handle the elliptic curve key exchange process, and those that can support it have very poor capacity and could only process a fraction of what they did for RSA.

As a result, data centers that need to support the latest SSL/TLS standards will need to upgrade their ADCs to the latest models and ensure that they incorporate newly released SSL acceleration cards that support ECC and the latest SSL/TLS 1.3 standard (once ratified and released).

Radware's* Alteon D-line* with Intel® Technology: Cost Effectively Handling ECC Today

Radware has adopted Intel® Xeon® processors in its Alteon D-line, AppWall,* and DefensePro* attack mitigation products to enable high-capacity ECC-based SSL/TLS transaction processing with a great price-to-performance ratio across all capacity ranges.

Specifically, these processors deliver special optimizations for very efficient processing of two compute-intensive SSL/TLS cryptographic phases: session initiation and bulk data transfer. Intel has integrated these optimizations into OpenSSL,* an open standard for high performance SSL/TLS processing.

Radware worked closely with Intel engineers to understand these optimizations and capabilities so that it could expand the capacity and performance of the Alteon product. To offload encryption processing, Radware has designed its appliances utilizing the Intel® C620 series chipset Platform Controller Hub. The Intel C620 series chipset features integrated Intel® QuickAssist Technology (Intel® QAT) for dedicated and accelerated encryption and decryption processing. In Alteon, Radware was able to leverage this technology to design a special hybrid operation mode that engages both CPU resources and the Intel QAT acceleration for excellent encryption/decryption performance.

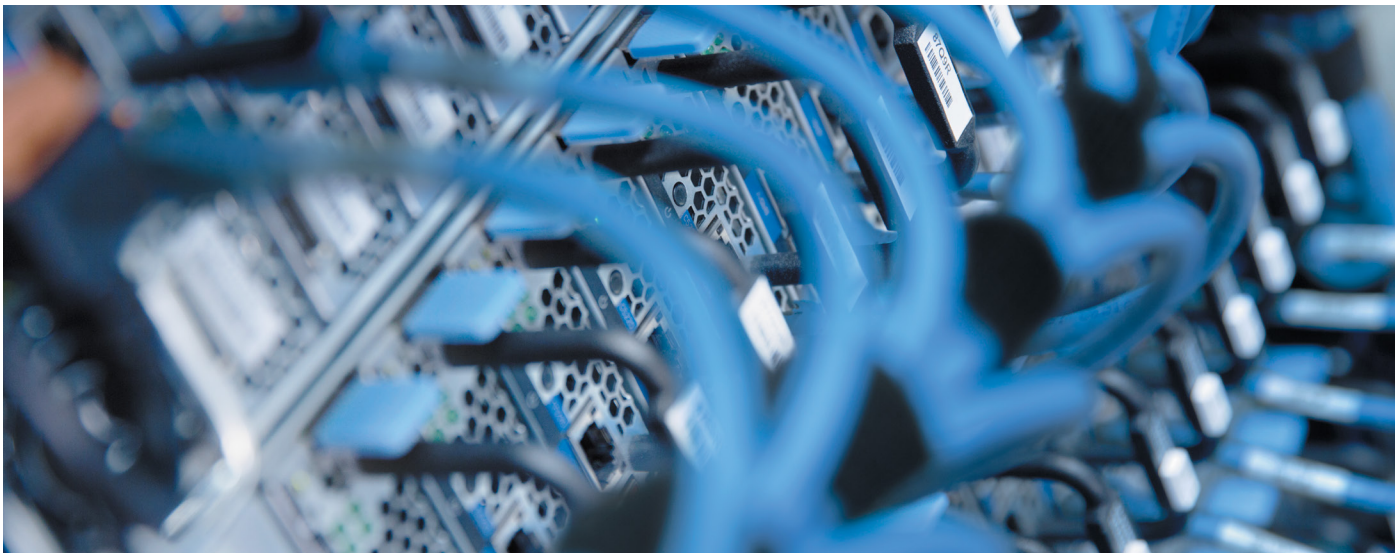
The excellent SSL/TLS processing efficiency that is a result of this hybrid approach frees up ADC resources on the Alteon D-line products for other tasks (such as layer-7 load balancing, data insertions, tighter application security and others). Radware was able to integrate the Intel QAT into its virtualized Alteon products for network functions virtualization (NFV) applications to offer outstanding SSL/TLS performance.

Radware Encryption Product Families

Alteon is Radware's next-generation application delivery controller (ADC) with load balancing features that can enforce application SLAs. It provides advanced, end-to-end local and global load balancing capabilities for all web, cloud, and mobile-based applications. Alteon load balancers combine advanced application delivery capabilities, accelerated SSL performance that supports all of the latest encryption protocols, and advanced services to companies with ongoing application lifecycle management challenges that impact the performance of web applications (such as heavier, more complex web content), mobility, and the migration to the cloud.

AppWall is Radware's Web Application Firewall (WAF). It provides fast, reliable, and encrypted delivery of mission-critical Web applications. AppWall is an ICSA Labs*-certified and PCI*-compliant WAF that helps provide protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages, and more. A core and integrated part of Radware's Attack Mitigation Solution, AppWall is a web application firewall that provides patent-protected technology to create and maintain security policies in real time for wide security coverage with low false positives and minimal operational effort.

DefensePro provides advanced DDoS protection features and IoT botnet attack mitigation. DefensePro, an award-winning, real-time, perimeter attack mitigation device, helps secure organizations against emerging network and applications threats. Part of Radware's attack mitigation solution, DefensePro provides automated protection from fast moving, high volume, encrypted, or very short duration threats, including IoT-based attacks like Mirai, Pulse, Burst, DNS, TLS/SSL attacks and those attacks associated with Permanent Denial-of-Service (PDoS) and Ransom Denial-of-Service (RDoS) techniques.



Summary

The need for efficient hardware acceleration of the elliptic curve cryptography will become greater and greater, especially once the new SSL/TLS version standard (TLS 1.3) will be finalized. One big change that is a part of TLS 1.3 is removal of support for RSA as a key exchange mechanism; only Diffie-Hellman and elliptic curve will be allowed. While the RFC has not yet been closed, browsers already support this new TLS version. Supporting ECC is no longer just about being more mobile friendly or more efficient processing of SSL traffic, it is becoming a necessity most organization can't ignore for much longer. Radware's Intel-powered Alteon D-line delivers a leading SSL solution set, which cost effectively handles high capacity of ECC-based SSL/TLS transactions and process high SSL traffic capacity across private datacenter, virtual and cloud environments.

About Radware

Radware (NASDAQ: RDWR) delivers application delivery and cyber security solutions for virtual, cloud, and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity, and achieve maximum productivity while keeping costs down. Radware Cloud Security Services provide cloud-based infrastructure protection, application protection, and corporate IT protection services to enterprises globally. For more information, please visit www.radware.com.

About Intel® Network Builders

Intel® Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software-defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.

[1] https://transparencyreport.google.com/https/overview?hl=en

[2] Trends in the cost of computing; https://aiimpacts.org/trends-in-the-cost-of-computing/

[3] A full description of both ECC and RSA encryptions is available in this NIST document: Recommendation for Key Management Part 1: General (PDF download): http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

1217/DO/H09/PDF ♻ Please Recycle 336902-001US