NETWORK BOX | NEXT GENERATION MANAGED SECURITY

www.network-box.com

In the Boxing Ring APR 2023

Network Box Technical News

from Mark Webb-Johnson

Chief Technology Officer, Network Box

Welcome to the April 2023 edition of In the **Boxing Ring**

This month, we are talking about **SSL/TLS Certificates and Authorities.** As more and more Internet services adopt the SSL/TLS protocol, and Network Box offers various services to secure and protect such traffic; we need clarification and understanding regarding the fundamentals of the protocols - particularly concerning certificates, certificate authorities, and trust. On pages 2 to 4, we discuss how certificates provide the core foundational security of the TLS protocol, how they protect against man-in-the-middle and other such attacks, and how the trusted Certificate Authorities have become such a security concern.

On page 5, we highlight the set of enhancements and fixes to be released in this quarter's Patch Tuesday for Network Box 5 and our cloud services.

In other news, Network Box is pleased to announce that the company has been awarded **ISO 31000** certification. Additionally, APAC Insider named Network Box as **Managed Cyber Security Provider of the Year** at the 2023 Singapore Business Awards. And in this month's global security headlines, there were security issues in Android and iOS devices, Oracle, Linux Servers, Facebook, and Fortinet.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2023

Stay Connected

You can contact us here at Network Box HQ by email: **nbhq@network-box.com**, or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

https://twitter.com/networkbox

https://www.facebook.com/networkbox
https://www.facebook.com/networkboxresponse

https://www.linkedin.com/company/network-box-corporation-limited/

https://www.youtube.com/user/NetworkBox

In this month's issue:

Page 2 to 3

SSL/TLS Certificates and Authorities

In our featured article, we discuss how certificates provide the core foundational security of the TLS protocol, how they protect against man-in-the-middle and other such attacks, and how the trusted Certificate Authorities have become such a security concern.

Page 5

Network Box 5 Features

The features and fixes to be released in this quarter's Patch Tuesday for Network Box 5 and our cloud services.

Page 6

Network Box Highlights:

- **Network Box**
  - ISO 31000 Certification
- **Singapore Business Awards 2023**
  - Managed Cyber Security Service Provider of the Year
- **Global Security Headlines:**
  - Android / iOS Devices
  - Oracle
  - Linux Servers
  - Facebook
  - Fortinet

SSL / TLS Certificates and Authorities

As more and more Internet services adopt the SSL/TLS protocol, and Network Box offers various services to secure and protect such traffic; we need clarification and understanding regarding the fundamentals of the protocols - particularly concerning certificates, certificate authorities, and trust. This article aims to clarify this and show how SSL/TLS can be securely implemented. However, note that we will limit our explanation here to server-side certificates and not outbound (client-side) SSL proxying, which is an entirely different topic.

SSL/TLS

Over the years, the original SSL (Secure Sockets Layer) protocol has morphed into TLS (Transport Layer Security). Earlier versions of the protocol were called SSL; later versions were TLS, but the core ideas and mechanisms behind the protocol are the same. To simplify things, in this article, we'll call it TLS, which fundamentally provides the following:

- Bi-directional encryption of a data stream between a client and server
- Protection against replay attacks, interception, or tampering with that data stream
- The ability for a client to verify that the server is who it says it is
- The optional ability for the server to verify that the client is who it says it is.

The protocol runs on top of another encapsulating protocol - typically TCP/IP (Transmission Control Protocol/Internet Protocol), but may also be UDP/IP (User Datagram Protocol/Internet Protocol) - requiring simply a bi-direction data stream between the client and the server. TLS connections may be directly established (such as to HTTPS port tcp/443) or 'turned on' once an underlying connection has been established (such as the STARTTLS command on an established tcp/25 SMTP connection). Most Internet protocols nowadays provide either a mandatory/alternative TLS port or some mechanism to upgrade a connection to TLS.

Public Key Cryptography

TLS relies on public key encryption. The concept here is that rather than one symmetric encryption key (aka 'password') being used for both encrypting and decrypting, the key is split into two parts - public and private - and it is mathematically infeasible to derive one key from the other. Any of these public/private keys can encrypt data, with the matching pair being used for decryption. The public key can be released or published without concern, while only the private key needs to be protected. In such a system, the public key can encrypt data that only the private key holder can decrypt, or vice-versa. This provides for some interesting approaches - the holder of the private key can prove they have it by demonstrating being able to decrypt data encrypted with the public key or by being able to encrypt data with their private key that is then able to be decrypted with the public key.

This is fundamental. To illustrate, here is an example:

- If User A, the private key holder, wants to prove they hold the key, User B can provide User A with some data.
- User A can encrypt the data with the private key.
- User B can verify that by decrypting it with the public key and comparing the results.

Certificates

At the heart of TLS is the concept of a certificate. Things here can get complex, so the explanation below is simplified and ignores some of the more modern, sophisticated implementations.

Fundamentally, a TLS certificate is a public key, along with some identifying information for the private key holder and a digital signature. This is used for two things: 1) to be able to encrypt data (with the public key) that only the holder of the private key can decrypt, and 2) to be able to verify that the holder is who they say they are. But what is this digital signature? It is produced by digitally signing the certificate data using the private key of some other party trusted by both ends of the communications link. These signatures are protected by the same public key cryptography in that the signer's public key can be used to verify the signature.

An example:

- Certificate A contains the name 'network-box.com' and the public key of services running at Network Box. It is signed by Certificate B.
- Certificate B is a trusted intermediary and contains that intermediary's public key along with its name. It is signed by Certificate C.
- Certificate C is a trusted top-level authority and contains the authority's public key along with its name. It is signed by itself (i.e., the private key of Certificate C).

That example shows just three levels, but there is no specific limit to the number of levels possible. Nowadays, certificates in everyday use have between zero and two or three intermediary certificates before we get to the top-level (sometimes aka 'root') certificate.

Now, say a user wants to make a TLS connection to that Network Box service. The user does a DNS lookup on the name 'network-box.com' and makes a TCP connection to that IP address. The user then goes through a TLS negotiation and typically gets back Certificates A and B. The user then verifies Certificate A (making sure the name in it matches the name 'network-box.com' the user connected to), and ensures it hasn't expired, etc. As A is signed by B, the user can do the same verification on B and do the extra step of verifying B's signature on A by using B's public key. Finally, the user sees that B was signed by C, and the user has a local copy of C (as a 'trusted Certificate Authority' in the user's local storage), so the user can verify C's signature on B using C's public key. This way, the entire certificate chain can be verified based on the trust that both ends place in 'C.'

Trusted Certificate Authorities

In the previous example, C is a trusted Certificate Authority (CA). Typically, these are well-regulated and mutually trusted certificates available to both ends of the connection. The server side trusts C not to sign anyone else as network-box.com without verification, and the client side trusts C to have correctly signed and to vouch for the authenticity of the network-box.com certificate that they signed.

Nowadays, TLS implementations (such as those used in web browsers) include a hundred or more trusted CAs. Each of these CAs have some validation process that they go through to authenticate that someone requesting them to sign a certificate is actually who they claim to be in the certificate. The most common of these validations is domain validation, where they only validate the right to administer that domain, but other more advanced forms of validation are possible (such as company name, etc.).

Typically, in a public network, these root, top-level, trusted certificates are the only ones permitted to be self-signed. All other certificates should be part of a chain of trust leading up to one top-level self-signed trusted certificate. There is nothing stopping you from self-signing a certificate - the issue is getting someone else to trust you.

So now we can see how the TLS protocol works. The client connects to the server, indicates its desire to communicate using TLS, and digitally signed certificates may be exchanged. Typically, a server certificate is always sent to the connecting client for verification, but also, in some cases, client certificates may be sent to the server for mutual verification. The public key cryptography outlined above is used to verify these certificates back to a mutually trusted Certificate Authority.

Certificate Issue/Renew

So now that we've got a good understanding of the system's basic mechanics, let's talk about the creation and renewal of these certificates.

A certificate is created by generating a highly random private+public key pair, putting the requestor's information and public key into a Certificate Request file. That is then sent to the Certificate Authority to issue the certificate. The CA then takes steps to validate the information in the certificate (often just the CN - the Common Name field, usually the DNS name for the service) by validating that the requestor also has control over that DNS domain name. Once validated, the CA re-packages the Certificate Request into a Certificate, signs it with their own private key, and delivers it back to the requestor. As each certificate has an expiry date, the certificate should be renewed before expiry - a process similar to issuing a new certificate except that the original public/private key pair can be re-used.

The requestor will typically validate that they control the domain in the CN of the certificate by one of a selection of validation mechanisms:

- Receiving, and responding to, a secret email to the administrative owners of that domain (proving organizational roles of postmaster, admin, etc.).
- Being able to put a provided secret into the DNS records for the domain (proving administrative control over the domain).
- Being able to put a provided secret into a file in the web server for the domain (proving administrative control over the website for the domain).

It should be noted that certificates can contain just one domain name in the CN, use a wildcard domain (*.network-box.com, for example), or list multiple alternative CNs to cover multiple services in one certificate. Certificate Authorities must validate all such types and all such domains referenced.

Nowadays, there are typically three options for obtaining a signed certificate:

1. Sign it yourself (but only practical in private networks due to the trust issue).
2. Getting a traditional CA to sign your certificate. In such cases, they typically verify just your Common Name, the certificate will expire in a year, and they charge anywhere from US$3 to US$300 per year.
3. Use the ACME (Automated Certificate Management Environment) to issue and renew your certificates. Such certificates are typically issued, renewed, and verified but expire in a month or two, so automatic verification and renewal are essential. A few trusted CAs support this free of charge.

In the April 2023 patch Tuesday, Network Box announced support for the ACME protocol in NBRS-5 - allowing us to support automatically issuing and renewing certificates using this protocol directly. This is particularly important for TLS services offloaded to the Network Box.

Hopefully, by reading this article, one should be able to see how certificates provide the core foundational security of the TLS protocol, how they protect against man-in-the-middle and other such attacks, and also how the trusted CAs become such a security concern (given the vital role they play in domain validation). This month's release of direct support for the ACME protocol in NBRS-5 will go a long way towards simplifying the secure issuing, renewing, and deployment of certificates and implementation of TLS protection.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 4th April 2023, Network Box will release our patch Tuesday set of enhancements and fixes. Due to the upcoming easter holidays, the regional SOCs will delay rollout of these patches until after Monday 10th April, and will be deploying the new functionality in a phased manner over the subsequent 14 days.

Network Box 5 Features

April 2023

This quarter, for Network Box 5, these include:

- Enhanced support for service control visibility in config for advanced routing protocols.
- Revisions to support for SSL/TLS over TCP/IP in optional SIEM log output target.
- Revisions to support for SSL/TLS over TCP/IP in optional SYSLOG log output target.
- Support certificate issue and renewal with ACME protocol.
- Introduce external scan configuration (both from Network Box and custom providers) to standardise mechanism for supporting external network scans.
- Improvements to UTF-8 support in logging.
- Support optional disabling of ARP check and/or update on network interface startup.
- Enhanced support for dynamic host names in IPSEC tunnels (rather than static IP address configuration).
- Support AES-GCM and AES-CTR encryption in IPSEC tunnels.
- Frontline control over TCP Timestamp Information Leakage (default: disable TCP timestamps now).
- Frontline control over ICMP Timestamp Information Leakage (default: disable ICMP timestamps now).
- Expanded support for increased number of routing tables.
- Change to show configuration history in box local timezone (was UTC).
- Support to show cloud mail backup status in nbconsole and admin web portal.
- Support for show cloud DNS backup status in nbconsole and admin web portal.
- Support network speed test as console command.
- Introduce support for new 2023 S-80i box model.
- Regular periodic updates to several databases and engines (Geo location, application identification, etc).
- Improvements to SOC systems for console and configuration.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

Network Box HIGHLIGHTS

Network Box ISO 31000:2018 Certification

Network Box is proud to announce that the company has been assessed, meeting the guidelines of risk management practices for effective management and corporate governance - and has been awarded the **ISO 31000:2018** (Risk Management Standard) certification by the Academy of Professional Certification (APC). This takes Network Box's total number of ISO certifications to four:

- ISO 9001:2015
- ISO/IEC 20000-1:2018
- ISO/IEC 27001:2013
- ISO 31000:2018

Network Box Singapore Singapore Business Awards 2023

Network Box is pleased to announce that it won the **Managed Cyber Security Service Provider of the Year** award at the Apac Insider: Singapore Business Awards 2023.

Global Security Headlines

The Hacker News

Spyware Vendors Caught Exploiting Zero-Day Vulnerabilities on Android and iOS Devices

LINK: https://bit.ly/3GcbT0M

Network World

Oracle outages serve as warning for companies relying on cloud technology

LINK: https://bit.ly/40WGoj4

The Hacker News

New ShellBot DDoS Malware Variants Targeting Poorly Managed Linux Servers

LINK: https://bit.ly/3KrDLjR

Bleeping Computer

Facebook accounts hijacked by new malicious ChatGPT Chrome extension

LINK: https://bit.ly/42Z3CqM

The Hacker News

New Critical Flaw in FortiOS and FortiProxy Could Give Hackers Remote Access

LINK: https://bit.ly/3m09a3A

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2083
Fax: +852 2736-2778

www.network-box.com