APR 2015

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the April 2015 edition of In the Boxing Ring

This month, we present the first part in a two part series on Proxying the SSL protocol. Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols. They are designed to permit the authentication of clients to servers, and vice-versa, as well as protect the communications from such threats as eavesdropping, tampering, and replay. The protocols have been around for more than 10 years now, and are seeing near ubiquitous usage as the protocol of choice for secure communications of many sorts. This is discussed further on pages 2-3.

On pages 4–5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, Network Box won the Capital Outstanding Enterprise 2015 Award, for the *'Best Network Security Provider.'* Network Box is extremely proud to have won this highly prestigious award and would like to thank everyone, who voted for Network Box in this competition.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
April 2015

You can contact us here at 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:

twitter http://twitter.com/networkbox

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

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

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

Proxying SSL

part (1 of 2)

Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols. They are designed to permit the authentication of clients to servers, and vice-versa, as well as protect the communications from such threats as eavesdropping, tampering, and replay. The protocols have been around for more than 10 years now, and are seeing near ubiquitous usage as the protocol of choice for secure communications of many sorts.

The Certificate

At the core of TLS/SSL is the certificate. This is based on RSA asymmetric key cryptography, where a key pair (public and private) is generated such that one key is used to encrypt while the other is used to decrypt. So, for example, we can encrypt some text with the public key, and then only the holder of the private key can decrypt it, or vice-versa. Such asymmetric key systems can be used for encryption/decryption as well as signing/verifying (I sign with one key, then you can verify with the other).

To generate a certificate, two entities are involved.

1. Firstly, the owner of the certificate generates a random public+private key pair, and then puts the public key plus his identifying information into a certificate request, and sends it to a trusted certificate authority.
2. Secondly, the certificate authority generates its own public+private key pair (or more commonly uses one previously generated) and then uses its own private key to sign the owner's public key in the certificate request.

The result of this process is a certificate containing the owner's identifying information and public key, signed with the private key of the trusted certificate authority.

In addition, the trusted certificate authority puts its own public key into a certificate and typically self-signs it with it's own private key (or in some cases gets it signed by an another upstream trusted certificate authority), then publishes that certificate.

Certificate Verification

Now, when a client connects to a server talking TLS/SSL, the server can provide it's own certificate to the client.

When the client receives this certificate, it can verify the authenticity by checking against a list of trusted certificate authorities it maintains. By using the certificate authority's public key (inside a certificate), the client can verify the signature on the certificate presented by the server. You can see that for this to work, the certificate authority who signed the server's certificate must also be trusted by the client (ie; in the list of trusted certificate authorities installed on that client).

Once the certificate has been verified, key exchange can be safely performed using the public key inside the certificate (so that only the server that has the matching private key can decrypt the information).

Of course, the above is a vastly simplified overview of a complex process, but you should be able to see the basic mechanics of how this works. The key points to take away from this are:

1. Data encrypted with a public key can only be decrypted with the matching private key. This is asymmetric key cryptography, and works both ways public->private and private->public.
2. The certificate contains a public key, as well as matching identification information for the owner.
3. The certificate is signed by the private key of a certificate authority trusted by both the client and the server.
4. The client can verify the signature using the public key of the trusted certificate authority.
5. The client can send data securely to the server using the verified public key of the server (as only the server has the matching private key used to decrypt).

Man In the Middle

So, say that as an organizational policy, we want to be able to inspect TLS/SSL protected traffic. We want to ensure that TLS/SSL protected web sites being visited over the HTTPS protocol conform to organizational policy, and that the files transferred do not contain malware. We also want to ensure that proper validation of the TLS/SSL certificate is performed, and protocol exploits protected against.

The way to do this is with a so-called man-in-the-middle interception.

The idea is that when the client connects to the server, that connection is intercepted by the proxy. The proxy then maintains two separate TLS/SSL connections - one from the client to proxy and the other from the proxy to the server. This is performed as follows:

1. The proxy itself has its own certificate (with public and private key) and this certificate is installed as a trusted certificate authority into the client.
2. The proxy negotiates TLS/SSL with the server, and validates and ensures the correctness of this connection.
3. The proxy takes the server certificate, replaces the public key with one of it's own, and then self-signs that certificate with it's own certificate authority private key.
4. The proxy uses this modified certificate to negotiate a TLS/SSL connection with the client.

When talking to the server the proxy sees the server's certificate signed by a certificate authority trusted by both the server and the proxy. The server's public key (contained in that certificate) can be used to securely communicate with the server. But, the client sees the server's certificate signed by the intercepting proxy with the proxy's public key, and the proxy's public key (contained in that modified certificate) can be used to securely communicate with the proxy.

With such an arrangement, the proxy decrypts the traffic from the client, examines it for policy enforcement, then encrypts it and forwards it on to the server. Return traffic from the server can be decrypted by the proxy, examined for policy enforcement, then re-encrypted and forwarded on to the client. The communications client-proxy and proxy-server are secure, but the traffic is subject to policy enforcement.

Strengths and Weaknesses

Such an arrangement removed the weak link (the end-user policy decision) from the TLS/SSL protocol, by allowing policy enforcement to be made by administrators at the network gateway. It also allows for protocol upgrading, and protection against exploit of browser and other client-side vulnerabilities. A good example of this is the recent FREAK vulnerability - Network Box 5 SSL proxy users have been protected against exploit of that from day #1, as the Network Box 5 SSL proxy already enforces secure cryptographic cipher selection at the gateway (irrespective of the vulnerability at the client).

However, there are two main areas such an arrangement may not work:

1. Client-Side Certificates. The TLS/SSL protocol allows for client side certificates. If these are used, the traffic cannot be intercepted (as the client certificate provided to the server could not be modified without access to the server's trusted certificate authority list - which is not practical).

2. Certificate Pinning. Some client side applications using TLS/SSL perform an extra validation step which is to verify the identity of the certificate authority used to sign the server's certificate. For example requiring the certificates presented by server X must be signed by authority Y. Such traffic cannot be intercepted (as the client side application would object to the certificate authority used by the intercepting proxy).

In such cases, policy rules are normally put in place, at the proxy, to bypass such sites from TLS/SSL interception.

The other restriction is that the certificate authority used by the intercepting proxy must be trusted by the clients (normally meaning that the proxy's SSL certificate must be installed into the trusted certificate store of the client). We are often asked why this is a requirement, and the answer is simple - if it wasn't a requirement, then we could simply and easily intercept, monitor and modify TLS/SSL communications transparently to the client and the security and integrity of the world's financial networks would be destroyed.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th April 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features
April 2015

This month, for Network Box 5, these include:

- Enhanced support for the 'all' and 'none' options in web client safe search policy
- Enhanced search facility for web client urlsite site search
- Improvements to filter naming in web client configurations
- New GMS sensor 'ldapsync' for reporting status of LDAP directory synchronisation
- New GMS sensor 'provisioning' to report status of device provisioning
- Improvements to column sorting in admin web portal
- Provide a download link, in admin web portal, for SSL certificate installation guide
- Introduce an admin console facility to permit the customisation of sender email address used for reporting
- Improvements to DHCP peerdns configurability, on bridge interfaces
- Automatically update the box information and notes, viewable in console, based on Box Office contract
- Improvements to release of quarantined eMails with large attachments
- Improvements to reduce memory utilisation in mail scanning subsystem
- Introduction of system hooks for SSL vpn UP/DOWN and vpn client CONNECT/DISCONNECT events
- Increase of default message size limit to 100MB, for on-the-box mail server.
- Add the box ID to filename, when report downloaded via administrative web portal
- Improvements to case insensitivity in personal whitelists/blacklists
- Improvements to case insensitivity in entity names
- Introduction of a new command 'show intrusion log' to directly search intrusion logs
- By default, for new installations, use 127.0.0.1 as default name server
- Add support for disk volumes on trace partitions (#2 onwards)
- Introduce a capability to specify IPSEC hub-spoke configurations
- Improvements to SSL VPN user disconnect, and general VPN status, logging
- Improvements to VPN mapping in administrative web portal
- Introduction of a new PDF/CSV report for exporting device configuration
- Updates translations for simplified and tradition chinese
- Improvements in anti-spam mail scanning, introducing signature-based top-level domain support
- Improvements in SPF policy enforcement, for mail scanning
- Introducing a 'reload configuration' option for administrative web portal web client configuration changes
- Various improvements to performance and stability of NBSYNC connections, particularly on NOC servers
- CVE-2015-0286: openssl: ASN1_TYPE_cmp improper boolean-type comparisons
- CVE-2015-0289: openssl: PKCS#7 NULL pointer dereference
- CVE-2015-0293: openssl: SSLv2 assertion failure
- CVE-2015-0209: openssl: Use-after-free vulnerability in the d2i_ECPrivateKey function
- CVE-2015-0287: openssl: ASN1_item_ex_d2i data structures reinitialize
- CVE-2015-0928: DCERPC parsing issue

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

Network Box 3 Features April 2015

On Tuesday, 7th April 2015, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Enhancements to Box Office related to device provisioning and optional services
- Improvements to license key issue arrangements for high availability devices
- Movement of administrator's manual PDF to the cloud (reducing on-device disk storage requirements)
- Various (mostly internal) enhancements to several internal support systems

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.

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	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

Network Box
Capital Outstanding Enterprise Award 2015

Network Box won the Capital Outstanding Enterprise 2015 Award, for the *'Best Network Security Provider.'* The awards ceremony took place on the 1st of April 2015, at the Conrad Hotel, Hong Kong

LINK: http://www.network-box.com/sites/default/files/files/Capital%20Outstanding%20Enterprise%202015%20Award.pdf

Network Box Germany
INNOVATIONSPREIS-IT 2015

Network Box won an INNOVATIONSPREIS-IT 2015 award, of the 'innitiative mittelstand' in Germany. This is an Award for Innovative IT Solutions in the field of SME businesses.

Link: http://network-box.eu/index.php/news/best-of-innovationspreis.html