Multi Service Proxy: Mobile Web Traffic Entitlement Point in 4G Core Network

Dalibor Uhlir, Dominik Kovac, Jiri Hosek

***Abstract*—Core part of state-of-the-art mobile networks is composed of several standard elements like GGSN (Gateway General Packet Radio Service Support Node), SGSN (Serving GPRS Support Node), F5 or MSP (Multi Service Proxy). Each node handles network traffic from a slightly different perspective, and with various goals. In this article we will focus only on the MSP, its key features and especially on related security issues. MSP handles all HTTP traffic in the mobile network and therefore it is a suitable point for the implementation of different optimization functions, e.g. to reduce the volume of data generated by YouTube or similar HTTP-based service. This article will introduce basic features and functions of MSP as well as ways of remote access and security mechanisms of this key element in state-of-the-art mobile networks.**

***Keywords*—4G cellular network, LTE, Mobile traffic, Multi Service Proxy, Security, SSL, Web services.**

I. Introduction

Mobile networks went throw a huge development during last 30 years. From NMT (Nordic Mobile Telephony, 1G) based on analog technology, over GSM (Groupe Special Mobile, 2G) with both data and voice signals sent over circuit switched network and 3G, where voice is sent via circuit switched and classic data is sent as IP (Internet Protocol) based flow, to LTE (Long Term Evolution, 4G) network where both data and voice (VoLTE – Voice over LTE) use IP channel. Current mobile network is complex communication system composed of large number of nodes. However, the emerging LTE deployment includes three key parts: 1) RAN (Radio Access Network), 2) core network and 3) IMS (IP Multimedia Subsystem) as optional but very common component (see Fig. 1).

The current situation in utilization of cellular networks and growing demands of their users introduce several challenges to which the mobile operators will have to face sooner or later. Especially the following facts need to be taken into a consideration:

- Traffic from wireless and mobile devices will exceed traffic from wired devices by 2016 [1].
- HTTP traffic is taking the pole position in residential broadband Internet traffic [2], [3].
- Around 34% of HTTP traffic was found to be multimedia [4] and one of dominant multimedia server is YouTube.

This paper is addressing the MSP server located in LTE core network and describes mainly security access for its managing via TSL (Transport Layer Security) and also a protection of user's secure entitlement traffic. The article discusses the system of certifications and their renewal used by MSP and moreover offers the way how to increase security using current solution and shows alternative ways for certification. The article also critically analyzes the key weaknesses of core network components in today's environment and explain potential security holes.

D. Uhlir, D. Kovac and J. Hosek are with the Department of Telecommunications, Brno University of Technology, Czech Republic e-mail: xuhlir15@stud.feec.vutbr.cz, xkovac23@phd.feec.vutbr.cz, hosek@feec.vutbr.cz
Manuscript received June 6, 2015.

II. Multi Service Proxy

MSP (Multi Service Proxy) is the element in mobile core network which contains several types of nodes. The key part is the database system composed of several servers which handle network traffic. The other parts of MSP include the traffic servers (TS), administration nodes and the jump start server. Figure 1 shows logical position of MSP in mobile network and its interconnections to other core nodes.

MSP network elements are deployed as several chassis (each chassis has several blades) within one rack. Each chassis is de facto the UNIX machine with web server, database server and NetBackup solution installed.

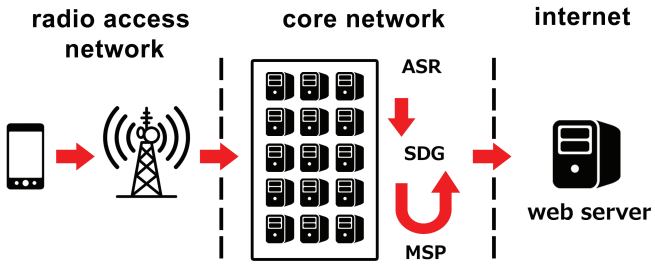


Fig. 1: MSP in core network

MSP is located on the same level as ASR (Accounting Start Request) which is an extended edge router providing functionality of SGW/PGW (Serving Gateway / Packet Data Network Gateway) and SDG (Service Delivery Gateway). The SDG works beside others also as load balancer. S/P gateways in LTE networks have similar functionality as SGSN (Serving GPRS Support Node) and GGSN (Gateway General Packet Radio Service Support Node) in 3G networks.

MSP is located between SDG and Internet so when a user using his smartphone, laptop or other mobile device sends HTTP message, the SDG forwards it automatically to MSP. Then, the MSP processes this kind of traffic and sends the message back to SDG. After that, SDG sends traffic to Internet. The HTTP traffic is recognized by a source or destination port 80. Besides HTTP, MSP processes also secure entitlement traffic which is utilizing HTTPS. However, it represents smaller percentage share of all web traffic. The detailed topology of LTE core network is depicted in Fig. 2).

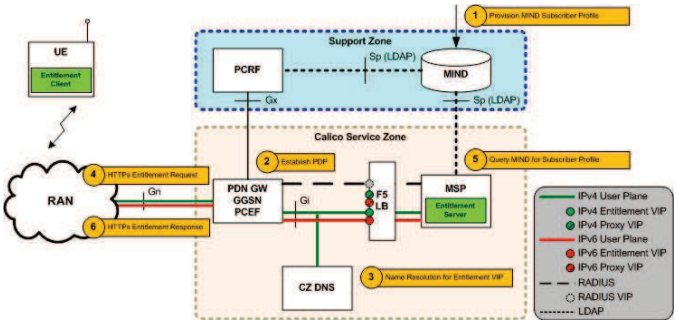


Fig. 2: LTE core network solution including the MSP

There are several methods how to process HTTP traffic on MSP. The most frequently used mechanisms are a header enrichment, compression, implementation of URL (Uniform Resource Locator) rules, pacing, etc. Traffic compression for example is mostly applied to following video formats: mp4, quicktime, x-f4v, x-flv and 3gpp.

When the network traffic is processed by MSP and sent back to SDG, it than goes to ASR and RAN network. This is default behavior for each user, but can be changed by custom configuration of MSP which means that MSP will not modify the traffic for selected users. This is done exceptionally, usually based on a user's request (if confirmed by network provider). From the point of view of physical implementation, the SDG, ASR and MSP are all located in the same rack.

III. MSP Administration

MSP is managed via MSA (Multi Site Admin) to assure service and network availability and sufficient performance of MSP. MSA client is running in web browser which connects to web server running on a database server in MSP system.

Via MSA GUI (Graphical User Interface, see Fig. 3) a network administrator maintains the configuration of MSP. It is possible to manage whole chassis, traffic servers, database server and admin server as well. The configuration management is used to view and edit the values of centrally stored parameter used for browsing, streaming and push services. In order to keep the configuration as efficient as possible, the centralized approach is applied. It means that a network administrator connects to MSP database server does his job (update the settings) and then database server propagates all updates to traffic servers automatically.

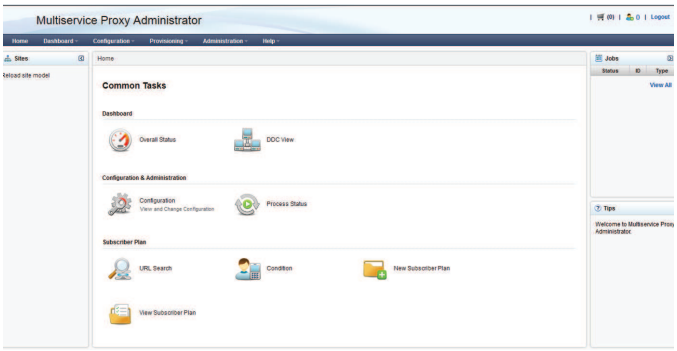
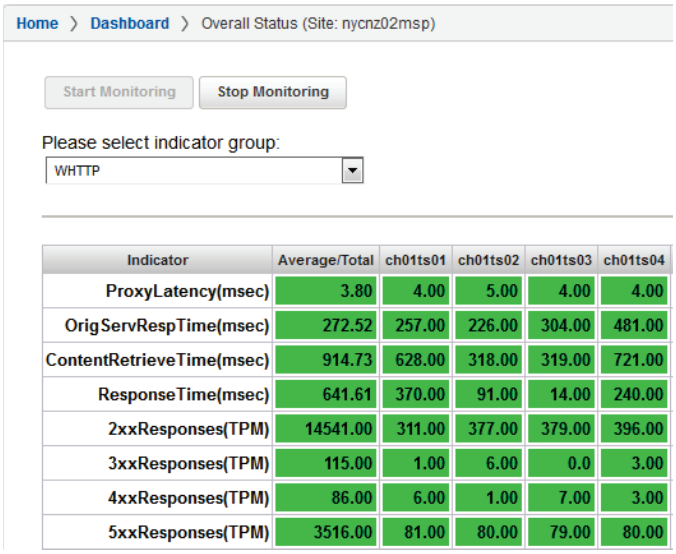


Fig. 3: MSA web interface to maintain MSP

MSA GUI provides also the dashboard which enables to check the current status of MSP and see its performance introduced as KPIs (Key Performance Indicators) collected via SNMP (Simple Network Management Protocol) from each node (see Fig. 4). The KPIs includes the following metrics [4]:

- amount of traffic,
- percentage of successful requests from users,
- distribution of HTTP status codes received by users,
- services running on TS and their status,
- utilization of memory, processors and file systems on all MSP elements.



Indicator	Average/Total	ch01ts01	ch01ts02	ch01ts03	ch01ts04
ProxyLatency(msec)	3.80	4.00	5.00	4.00	4.00
OrigServRespTime(msec)	272.52	257.00	226.00	304.00	481.00
ContentRetrieveTime(msec)	914.73	628.00	318.00	319.00	721.00
ResponseTime(msec)	641.61	370.00	91.00	14.00	240.00
2xxResponses(TPM)	14541.00	311.00	377.00	379.00	396.00
3xxResponses(TPM)	115.00	1.00	6.00	0.0	3.00
4xxResponses(TPM)	86.00	6.00	1.00	7.00	3.00
5xxResponses(TPM)	3516.00	81.00	80.00	79.00	80.00

Fig. 4: Example of MSP dashboard

One of available settings on MSP (manageable via MSA) is video content adaptation (see Fig. 5), sometimes referred also as multimedia content adaptation, content re-purposing, content reuse or re-authoring. Using this technology, mobile operators are able to reduce amount of network traffic and so save the bandwidth. The content adaptations is based on the transformation of logical set of video streams, images, text and other media from a source to one or more destinations. The most frequently used mechanism is the media transcoding to another format (format conversion) in order to reduce the bitrate.

MSP acts as proxy server and sends the requests to the server on behalf of the client. When the reply from server is received, MSP performs the content adaptation and sends adapted data to the client. The content adaptation covers five basic techniques:

- information abstraction,
- modality transformation,
- data transcoding,
- data prioritization,
- purpose classification.

IV. Entitlement Traffic and Server

The Secure Service Based Entitlement (SSBE) architecture is secure method for an entitlement client on a device to query

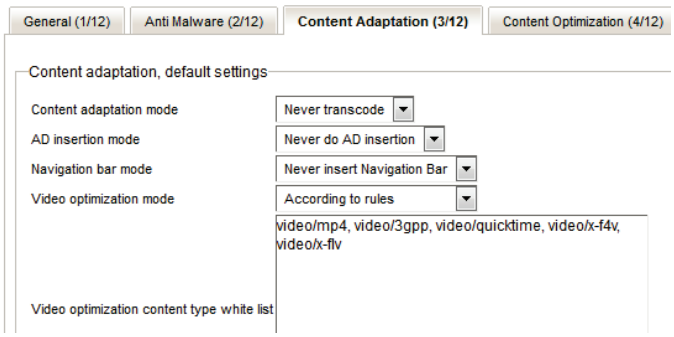


Fig. 5: Video content adaptation on MSP

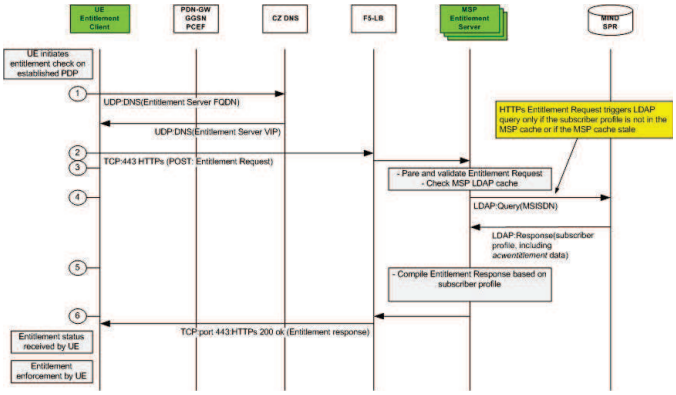


Fig. 6: Secure entitlement workflow

provider's network for entitlements of specific services (tethering, FaceTime, etc.). It is enhancement to MSP to provide SSBE functionality. The entitlement server is a software running as daemon on MSP which processes queries entitlements of services. Entitlement enforcement is in responsibility of the client (e.g. smartphone).

The entitlement client is configured with an entitlement URL and communicates with the MSP secure entitlement server. Entitlement server (daemon located on traffic servers) contains workflow scripts to handle incoming HTTP requests from mobile devices requesting entitlement status of a service. There are two kinds of entitlements - simple one utilizing HTTP and secure one which is carried over HTTPS. The location of entitlement server and client is shown in Fig. 2 as green boxes.

A. Secure Entitlement

In case of secure entitlement traffic, the load balancer (SDG) forwards TCP:443 HTTPS POST Entitlement requests (included in the body of HTTPS POST request) to MSP. In secure entitlement, two requests are supported: getEntitlement and getPhoneNumber. The getEntitlement is used by the device to query the entitlement server for the entitlement status of services that this subscriber should or should not be allowed to use. On the other side, the getPhoneNumber is used by the device to request the entitlement server to inform about the MSISDN (Mobile Subscriber/Station Integrated Services Digital Network) and corresponding signature. In order to generate such signature, a certificate and entitlement server's private key files need to be configured in the secure entitlement parameters subgroup in MSA. The algorithm used to encrypt the message is SHA1 (Secure Hash Algorithm). More detailed description is provided in the next section V.

When a GetPhoneNumber action is received within the secure entitlement request, the entitlement server will generate a signature that will be sent back to the client as part of the response. The whole secure entitlement workflow process is shown in Fig. 6 [5].

Secure entitlement traffic can be created by different applications. One example is the FaceTime which is videotelephony and voice over IP application from Apple [6]. At the beginning, the FaceTime worked only via WiFi networks, however starting with iOS 6 also the support for mobile networks is implemented. To be able to operate FaceTime over mobile network, carrier's support is required. Apple devices have the mechanism to decipher the request sent by MSP. In other words, user equipment (UE) resolves the entitlement FQDN (Fully Qualified Domain Name) in the entitlement URL to the secure entitlement server via DNS (Domain Name System). Then the UE sends a HTTPS POST entitlement request to one of the secure entitlement servers (selected by load balancing process on SDG). The MSP secure entitlement server parses and validates the entitlement request. For valid requests, the secure entitlement server uses the IP source address of the UE to check the MSP LDAP DDC (Lightweight Directory Access Protocol Distributed Data Cache) cache for the profile of the subscriber. MSP retrieves the subscriber profile and based on it, the secure entitlement server compiles the entitlement response. After that, MSP sends a HTTP 200 back to the UE for valid requests. The HTTP message body contains the complete entitlement response.

B. Simple Entitlement Architecture

In a simple entitlement architecture, the requests are sent in form of HTTP GET request with an empty body. The workflow scripts that support simple entitlement requests are configured as subscriber plan specific scripts. Here are two possible response codes as an answer to a simple entitlement request:

- 200 OK - if the client is entitled to the requested service.
- Pre-configured 4xx response - in case the client is not entitled or an internal error occurs.

The entitlement server can be then configured to add, remove or modify entitlement services on a URL basis (entitlement URL) for both secure and simple entitlements. Each entitlement URL is associated with an entitlement protocol, an entitlement service, LDAP attribute and entitlement value. Example of simple entitlement is the determination of whether a subscriber is allowed to use tethering with their rate plan. The entitlement enforcement is responsibility of each client.

V. SSL Certificates

SSL (Secure Socket Layer) is cryptographic protocol that performs a security related functions and applies secure communication. SSL encrypts data of network connections in

the application layer of OSI model and uses both symmetric (communication between client and server - AES, DES) and asymmetric key (to authenticate and change symmetric key) [7]. There are three types of SSL certificates: extended, organization and domain validation. In mobile network we need to authorize network engineers on servers in network and carrier's clients to access services [8], therefore SSL is also used for the connection to maintenance interfaces of MSP.

A. MSA SSL Certificate Implementation

MSA SSL certificate is installed on database servers to allow a secure connection to the MSA GUI. Client (network engineer) connects to MSA via HTTPS (to requests secure page). The database server sends back to client its public key and certificate (generated with keytool command and received with the signature from Certification Authority). A client checks whether the certificate was issued by a trusted Certificate Authority (CA), if the certificate has valid date and if it is related to MSA. Then client uses this public key (which was sent from database server together with the certificate) to encrypt a random symmetric encryption key and sends it to the server (together with request for the web page). The server decrypts the symmetric encryption key using its private key and uses the symmetric key to decrypt requested URL and sends requested page (HTML) to client.

Based on information from [9], in order to receive the certificate for MSA and get it implemented, the VeriSign Managed PKI Server Certificate Registration Request is sent via Security Request Center (SRC) as first. This is an internal process in any carrier's communication system.

When approved, the Certificate Signing Request is generated (CSR file) on database server using UNIX command "keytool -genkey" (a new pair of private and public keys is generated) and "ketytool -certreq" (generates the certificate request using the private key created in previous step). In other words, when public and private keys are generated the certificate request is sent to CA. File *request.cer* is generated and uploaded to Authority Servers Managed PKI for SSL Subscriber Services. After that the certificate (.cert file) together with primary, secondary and root certificates are received back from CA and implemented using UNIX command "keytoll -import".

B. SE SSL Certificate Implementation

When it is approved to request certificate via Security Request Center (following the same internal process as described above), RSA (Rivest Shamir Adleman) private key is created using "openssl genrsa -out file.key" command, see Fig 7.

```
hstnz01msp4ts11:~/test # openssl genrsa -out server.key.new 2048
Generating RSA private key, 2048 bit long modulus
.....................................................................................+++
.....................................+++
e is 65537 (0x10001)
hstnz01msp4ts11:~/test # openssl rsa -noout -text -in server.key.new
Private-Key: (2048 bit)
modulus:
    00:ad:27:25:f2:a7:7a:93:1a:64:5c:08:7e:e6:6c:
    4c:c8:0a:26:ce:10:bf:47:74:ca:8d:a2:f8:e6:87:
    03:55:a3:89:0d:7b:17:ef:bd:5c:8f:b8:8c:9f:56:
    1b:24:c6:76:c4:d8:76:4d:72:2f:39:94:3c:9e:52:
    bc:ab:94:08:f5:60:f0:4a:a4:2e:98:6c:a1:18:68:
    36:98:28:f3:35:ee:3e:06:41:74:8c:45:93:01:ef:
    43:cd:f3:7f:2c:c8:3b:21:4e:93:0e:4e:44:74:1c:
    cf:a6:bf:80:17:07:f3:bf:29:ff:2a:d6:94:b2:a4:
```

Fig. 7: Private key generation

Then the file.csr (request for certificate) is created from file.key (private key generated in the step before) using command "openssl req -key file.key -out file.csr", see Fig 8 and so the CSR is obtained. This file is sent to CA and later the SSL certificate (.pem file) is received as answer. Together with intermediate certificates and private file.key, the SSL certificate is uploaded to MSP traffic server.

```
hstnz01msp4ts11:~/test # openssl req -new -key server.key.new -out server.csr.new
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CZ
State or Province Name (full name) [Some-State]:Bohemia
Locality Name (eg, city) []:Brno
Organization Name (eg, company) [Internet Widgits Pty Ltd]:VUT
Organizational Unit Name (eg, section) []:FEKT
Common Name (e.g. server FQDN or YOUR name) []:Dalibor
Email Address []:dalibor.uhlir@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Fig. 8: Certificate request

Container file server.pem (contains public certificate) is used to sign the response for entitlement request if user is entitled for the services. The getPhoneNumber request signed with the public key from secure entitlement server can be sent (after using certificate to make sure that the key is valid) and the response sent from secure entitlement server is decoded by mobile devices utilizing the already mentioned built-in function.

As signature algorithm, the SHA1 is used and signature of the issued key (x509) in server.pem has to match signature of the certificate (RSA) in the server.key file.

VI. Attacks Against MSP

Mobile carriers need to have a good level of security to protect especially the nodes and systems used for billing and users' data privacy purposes. Without those security mechanisms, any technically skilled users would be able to manage the billing of his service profile their data to another user's account. Another potential risk (when no security is implemented) is a sniffing and modifying mobile network traffic and so get access to users private information like for example their accounts' credentials. Therefore, the SSL and other security algorithms utilized in mobile networks play crucial role. However, even that the security is implemented there are several recognized types of attack against the SSL:

- beast TLS attack [10],
- renegotiation attack [11],
- version rollback [12],
- poodle attack [13],
- RC4 attack [14],
- Heartbleed [15],

Besides the above listed SSL attacks examples, there are other possible security issues related to HTTP traffic and its processing in mobile network. Some of them is e.g. the CA issue. Nowadays, there are too many CAs and some of them could be compromised or they can be corrupted so they issue certificates even for addresses that are banned to require a certificate (e.g. localhost) or CA can issue even a

fake certificate. Another well-known vulnerability point is a carrier's own employee.

In order to avoid the security problems, there are several standard ways how to improve it:

- Increase the length of private key.
- Change the fundamental principles of security system. Currently, the web browsers expect that server sends SSL certificate and browser then validates it against the set of root CA integrated in a browser or operating system. Assuming this we can implement different models:
  1) DNSEC (Domain Name System Security Extension) - mapping public key on DNS
  2) Web of trust - everyone can generate own PGP (Pretty Good Privacy) key
  3) Perspective project - new approach to help computers communicate securely on the Internet [**?**]

VII. Conclusion

In this article, the MSP element as one of key components of state-of-the-art mobile networks has been introduced. The focus has been given especially to its mechanisms for HTTP / HTTP traffic processing and adoption. Also the implemented security algorithms and means to maintain the MSP have been introduced. We have also discussed some potential security risks and offers solutions which decrease possibility of successful attack. The network traffic optimization is currently highly discussed issue in 4G networks and therefore the development of MSP and similar solutions is very active. The key contribution of this paper lies in uncovering the internal procedures and mechanisms used in the core part of cellular network in order to relieve the network load. Such information is usually protected by vendors and operators, however, to develop high quality mobile service, it is important to understand inner processes employed by the network nodes.

Acknowledgment

For this research, the infrastructure of the SIX Center was used.

References

[1] Cisco Visual Networking Index: Forecast and Methodology, 20132018 http://www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html/

[2] G. Maier, A. Feldmann, V. Paxson, and M. Allman, On dominant characteristics of residential broadband internet traffic, in Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference, ser. IMC 09. New York, NY, USA: ACM, 2009, pp. 90102

[3] C. Labovitz, S. Iekel-Johnson, D. McPherson, J. Oberheide, and F. Jahanian, Internet Inter-Domain Traffic, in Proc. of the ACM SIGCOMM 2010 Conference on SIGCOMM, New Delhi, India, Aug. 2010.

[4] J. Erman, A. Gerber, M. T. Hajiaghayi, D. Pei, and O. Spatscheck, Network-Aware Forward Caching, in WWW. ACM, 2009, pp. 291 300.

[5] A. Kalgaonkar: ATT Matrix 1.0 Project - Workflow Scripts Administration Guide, 2013.

[6] Apple Inc., iOS Security - White Paper, 2015.

[7] Wikipedia contributors. "Public-key cryptography." Wikipedia, The Free Encyclopedia. 2015.

[8] C. Timberg: "Huge flaw that undermines privacy of mobile phone networks revealed by German researchers", Washington Post, 2014.

[9] F. Herrgoss, Gus Bourg, Kieran Kavanagh: Calico 2.3, 2011.

[10] I. Ristic, Is BEAST Still a Threat?, Qualys Blog, 2013. Available from: https://community.qualys.com/blogs/securitylabs/2013/09/10/is-beast-still-a-threat

[11] M. Ray, Understanding the TLS Renegotiation Attack, Educated Guesswork, 2009. Available from: http://www.educatedguesswork.org/2009/11/understanding_the_tls_renegoti.html

[12] H. Zhang, Three attacks in SSL protocol and their solutions, University of Auckland, 2011. Available from: https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/725zhang.pdf

[13] B. Maller, T. Duong, K. Kotowicz, This POODLE Bites: Exploiting The SSL 3.0 Fallback Security Advisory, Google, 2014.

[14] J. Lv, B. Zhang, D. Lin, Distinguishing Attacks on RC4 and A New Improvement of the Cipher, 2013. Available from: https://eprint.iacr.org/2013/176.pdf

[15] A. Borges, How to perform a Heartbleed Attack, 2014. Available from: http://alexandreborgesbrazil.files.wordpress.com/2014/04/heartbleed_article_rev_b.pdf