Securing Future Internet and 5G using Customer Edge Switching using DNSCrypt and DNSSEC

Slawomir Nowaczewski and Wojciech Mazurczyk*
Warsaw University of Technology, Warsaw, Poland
{slawomir.nowaczewski, wojciech.mazurczyk}@pw.edu.pl

Received: April 21, 2020; Accepted: August 13, 2020; Published: September 30, 2020

Abstract

Customer Edge Switching (CES) serves an extension of the classical firewall functionality that is able to communicate with other security devices to establish whether network traffic should be considered as benign or malicious. CES is envisioned to be utilized in future generation networks like 5G. In this paper, we first describe the CES concept and how it uses Domain Name System (DNS) protocol. Then, we discuss the attack model and how the current CES implementation that lacks DNS encryption/authentication can be exploited through the man-in-the-middle (MitM) attacks. Finally, we extend the current CES implementation to fix this gap by adding DNSCrypt and DNSSEC functionalities. Obtained experimental results prove that most of the attacks can be easily defended by these countermeasures.

Keywords: Customer Edge Switching, CES, DNSCrypt, DNSSEC, 5G, Future Internet

1 Introduction

5G is the next evolution of mobile networks. From the security point of view, it is really needed that 5G addresses already known security threats, as well as implement countermeasures which can fix new and emerging threats. In brief, 5G should guarantee better security than we currently have [1], [2]. In this paper we focus on a security framework called Customer Edge Switching (CES) and how it fixes, in particular, Internet weaknesses and ensure better handling of evolving security threats [3]. In CES we have policy-based communication, whereby the sender and the receiver need to meet the same requirements [4]. This is not known in the current state of Internet where any endpoint can send anything it wants to a destination host. CES can defend the attacks based on techniques such as address spoofing or DoS [5], [6]. In CES we also have a cooperative firewall and the term *cooperative* here means that it can find out what traffic is suspicious and appropriately filter it. In brief, CES is an extension of the classical firewall which can communicate with other firewalls and negotiate what traffic is benign and what is not [5], [6]. The deployment of CES is only visible at networks edges, where it just replaces Network Address Translation (NAT) [7]. It is also worth to mention here that CES supports incremental deployment where one site can have CES already deployed and the other side is not using it. The function that enables incremental deployment is called Realm Gateway (RGW) and it supports communication between CES-enabled network and network which does not have CES enabled. CES architecture is presented in Fig. 1. The figure shows two private domains, each with its own CES node, separated by provider network.

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), 11(3):87-106, Sept. 2020
DOI:*10.22667/JOWUA.2020.09.30.087*

*Corresponding author: Wojciech Mazurczyk, Room 313, Nowowiejska 15/19, 00-665 Warsaw, Poland, Tel: +48 22 234-77-99

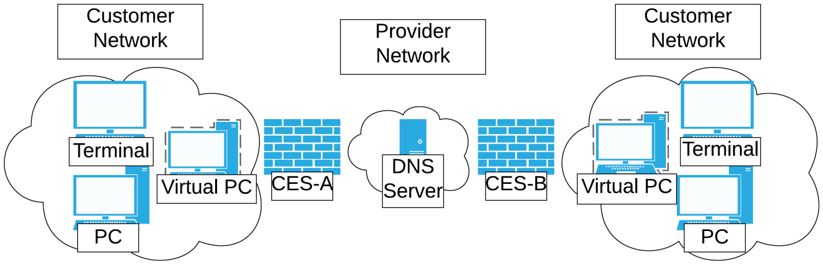
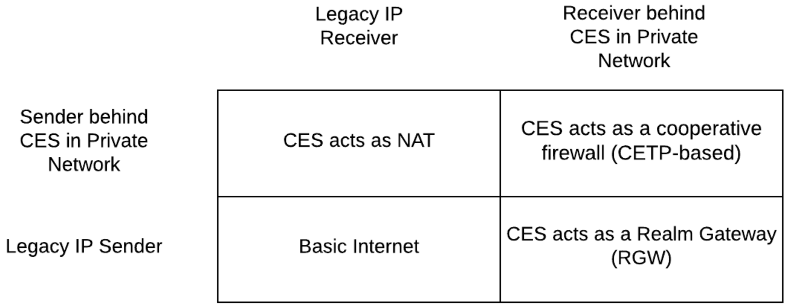


Figure 1: Customer Edge Switching Concept (note: in the currently available implementation CES-A communicates with CES-B using plaintext protocols).

CES is an improvement of NAT [8], [9]. This means that both of these solutions have very similar functions. First of all, CES and NAT work on private addresses which they translate to public addresses to allow communication. When one host, which is in the private network, wants to communicate with the different host, which is outside the private network, CES and NAT create a flow state which enables appropriate inbound flows to be delivered to the private network. If there is no state recorded, no traffic towards private network will be allowed. CES supports also a negotiation function where two devices negotiate parameters of the communication before the communication takes place. CES can work then as a cooperative firewall which communicates with other devices and exchange the policies. It is clear that the best functionality is given by CES working in cooperative mode. Other modes provide only legacy functionality for these scenarios where there is only one CES or there is nothing. The comparison between NAT and CES is presented in Fig. 2.



	Legacy IP Receiver	Receiver behind CES in Private Network
Sender behind CES in Private Network	CES acts as NAT	CES acts as a cooperative firewall (CETP-based)
Legacy IP Sender	Basic Internet	CES acts as a Realm Gateway (RGW)

Figure 2: CES and NAT comparison.

In addition to NAT, CES can be seen as an extension of the firewalls, especially the traditional ones [10], [11]. That is why it can perform additional operations to permit or drop particular packet. These operations are checking if the packets are being spoofed or authenticated, or whether the base-level policy compliance has been established or not. Most of these operations are being performed by sending special queries to the source and asking for particular attributes. However, the queries can be sent also to other entities such as Certificate Authority (CA) or Active Directory (AD) [12]. CES can react differently depending on the flow it checks. Every flow can be controlled by the different static or dynamic policies at CES or at the host-level [13]. The negotiations and the establishment of trust take place on network-

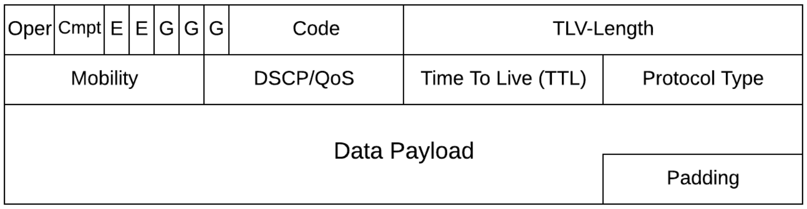


Figure 3: CETP Payload TLV.

level. A CES node is only a proxy device that works for hosts and applications behind itself. It simply exchanges policies, queries and replies with remote CES node using negotiation based on the Customer Edge Traversal Protocol (CETP). CETP exchange occurs before every communication event. CETP provides the functionality of informing other nodes about malicious traffic that it is being observed. This helps to filter the traffic as close to the source as possible [14].

Note, that the whole CES architecture heavily relies on the DNS protocol and for this reason it is vulnerable to various attacks which relate to DNS. That is why, in this paper we show how we can perform different attacks that exploit DNS traffic and what can be done to prevent them. Thus, the main contribution of this paper is to improve the security of the CES architecture by extending it with the DNSCrypt and DNSSEC modules. Using both solutions has the benefit of encrypting and authenticating appropriate DNS packets thus improving the overall CES security. To authors' best knowledge such an approach has not been tried before.

The rest of the paper is structured as follows. In Section 1 introduction to CES is presented. Section 2 introduces related work and concepts which are similar in purpose to CES. Next, in Section 3 a security analysis of the whole solution is outlined as well as what countermeasures have been already implemented there. Then, in Section 4 all important technical background is presented related to details of the CES approach and DNSCrypt/DNSSEC solutions. Section 5 is intended for discussing the utilized attack scenario for realizing DNS-related threats. In Section 6 the results of the experimental evaluation of the implemented DNSCrypt/DNSSEC modules are enclosed. Finally, Section 7 concludes our work.

2 Related work

CES architecture takes totally different approach in communication than traditional Internet. In brief, it is receiver-oriented. What it means is that before any communication occurs, both parties must check and agree to the conditions. This publisher-subscriber architecture [15] focuses on receiver and its requirements which means that nothing is delivered without being previously negotiated. Aside from CES, there are many other architectures that are described in the literature. IP Next Layer (IPNL) [16], for instance, is a NAT-extended architecture which uses domain names combined with public IP addresses to identify hosts. It adds additional IP layer to the communication. Internet Indirection Infrastructure (I3) [17] takes different approach. It uses rendezvous servers to span the communication channels between senders and receivers. This type of communication can be observed in multicast communication e.g. with shared tree. Next, Translating Relaying Internetwork Architecture Integrating Active Directories (TRIAD) [18] uses names and source routing. Mobility and Multihoming supporting Identifier Locator Split Architecture (MILSA) [19] in turn makes use of functional roles assigned to particular trust and connectivity domains. Another well-known approach is called Locator/Identifier Separation Protocol (LISP) [20] and it separates host Endpoint Identifiers (EID) from routers routing locators (RLOC). LISP is based on Domain Name System (DNS). Shim6 [21] also adds additional locator below the transport protocol and Host Identity Protocol (HIP) [22] does the same with locator by introducing identity tags and cryptography. StopIt [23] architecture uses edge filters and it does this dynamically by uploading filters to the sending node. Stateless Internet Flow Filter (SIFF) [24] takes proactive approach by tagging and prioritizing packets. PBS [25] combines proactive, filtering approaches and is based on Next Steps In Signaling (NSIS) [26] protocol suite for signaling. Both Permission-Based Sending (PBS) and SIFF requires synchronized changes on both sides which makes the implementation complex. The last approach that is worth mentioning is Metis [27] from 5G-PPP. This architecture is based on Software-Defined Network (SDN). The comparison of all mentioned solutions is shown in Table 1.

Table 1: State-of-the-art comparison between the approach and key solutions for the different network architectures

Parameters/ approaches	**Author**	**Decoupling location and identification**	**Additional protocol layer**	**Architecture**	**Key tasks**
IPNL	Francis and Gummadi (2001)	Yes Globally routable IP addresses with domain names	Yes	NAT-extended	Revealing private IP addresses
I3	Stoica et al. (2004)	Decoupling senders from receivers	Yes	Overlay network with a rendezvous server	Mobility, multicast and anycast
TRIAD	Gritter and Cheriton (2001)	Yes Name with source routing	Yes	Address realms	-
MILSA	Pan et al. (2008)	Yes ID with Locator	Yes New architecture	Functional roles for trust domains and connectivity domains	-
LISP	Farinacci et al. (2013)	Yes Endpoint Identifiers (EID) with routing locators (RLOC)	Yes LISP header	Endpoints and routing locators	Encapsulation, rewriting and mapping of IP addresses
Shim6	Nordmark and Bagnulo (2001)	Yes Additional locator	Yes	Load sharing and multi-homing	-
HIP	Moskowitz and Nikander (2006)	Yes Additional locator	Yes, HIP header	Cryptography and identity tags	Authentication and protection from DoS
StopIt	Liu, Yang and Lu (2008)	No	Yes	Filtering at the edges	Blocking unwanted traffic
SIFF	Yaar et al. (2004)	No	Yes	Tagging and prioritizing packets	Protection from DoS
PBS	Hong and Schulzrinne (2013)	No	Yes	Filtering and control plane based on NSIS protocol	Heavy cryptography
Metis	Osseiran and Boccardi (2014)	No	Yes	Control plane based on SDN	Software-defined network control

3 Customer Edge Switching - Security Analysis

CES architecture brings new security threats and countermeasures. The most important thing when we talk about CES is policy-based communication. CES negotiates policy elements on behalf hosts that it serves and provides tools that enriches security. These tools help network administrators implement security mechanisms using configurable policies. CES can also eliminate unwanted traffic, source address spoofing or DoS. By eliminating address spoofing, it can provide repudiation against sender. Moreover, CES provides many security heuristics. The first one, ACKnowledge, eliminate spoofing in the inbound traffic. The node delays connection establishment until the node is sure the source is valid. The second, CES Verification provides administrators with the ability to authenticate the remote node and collect evidence. This mechanism eliminates spoofing and requests the certificate from the sender. The certificate is used to sign the CETP header. All the changes are limited to edge nodes which also leverage security. Elimination of spoofed traffic helps with keeping battery lifetime. CES collects evidence on the sender which helps building reputation and the trust management. It acts as a cooperative firewall by seeking for policy compliance and secure identities from remote nodes. The reputation system can reduce threat levels in whole domain. CES has some vulnerabilities. We can divide them into 2 areas: Legacy Host attacks and CES-based attacks. Legacy Hosts attacks share the same Virtual Private Network (VPN) with CES devices. This can lead to situation where hosts from the same domain can generate CETP attack. CES-based attacks mean that legacy hosts are in the different VPN. There are many attacks possible. First of all, legacy host in the middle of communication can forward spoofed CETP packets towards CES node. This however can be eliminated by using cookie mechanism to authenticate sender of the packet. Next possible attack is replay attack. Attacker which is hidden before CES can replay previously seen packets. This can also be resolved by using cookie mechanism if the cookie is unique. Moreover, there is also an imitation attack where attacker node present itself as CES and communicate with the other side. This attack can be eliminated by using CES verification mechanism. Another attack is man-in-the-middle attack. The attacker can perform this kind of attack by e.g. DNS cache poisoning. Currently the countermeasures for this attack are using cryptographic signatures and Public Key Infrastructure (PKI). There is also a class of attacks using circular pool model which base on exhausting Circular Pool (CPOOL). In this paper we focus on DNS and show how CES architecture can leverage DNSCrypt and DNSSEC.

4 Technical background

In CES environment, the identification of hosts and applications is being done using constant Fully Qualified Domain Names (FQDN) which is a natural way when we talk about dynamically changing private addressing and other parameters assigned by DHCP server in the private network. These FQDNs imply that the whole CES architecture is based on Domain Name System (DNS). This means that the whole communication is based on DNS queries and replies sent for/by destination endpoint FQDN identifier. CES maintains information about the network it supports and the hosts in this network. This allows CES to prepare appropriate response. Every DNS query for a particular endpoint FQDN starts CETP service discovery. This function is running before any policy negotiation. It just checks if there is a CES in the remote network and how the hosts/services behind it can be reached [10]. CETP uses Naming Authority Pointer (NAPTR), a field defined in the DNS standard, to act with the service in the remote network. Every service is visible by using CETP + cisid format. If such value is present in the remote network, the service is available. NAPTR response transports the publically reachable address called Routing Locator (RLOC) which is needed to connect the remote CES. RLOC is written in ”ip=150.150.150.150” format. Obviously, the response can include also other fields such as IPv6 or ports. Moreover, NAPTR can also transfer alias field which supports using different transit links and CES identifier field which is used for routing. DNS records, especially NAPTR records, can be hosted on many locations. These can be customer/provider DNS servers or proxy DNS servers that keep these records in cache. To improve efficiency this functionality can also be implemented within CES [28].

4.1 CETP communication

The main responsibilities of CETP protocol are signalling and transmitting data across CES nodes [29]. Signalling is used mainly for establishing trust between CES networks, but it is also used by individual hosts or application policies, for establishing connections between two different areas. The user-generated data is tunneled using CETP session identifiers which are negotiated through CETP signalling phase. CETP session identifiers are being used to distinguish different users on the data plane [30][31].

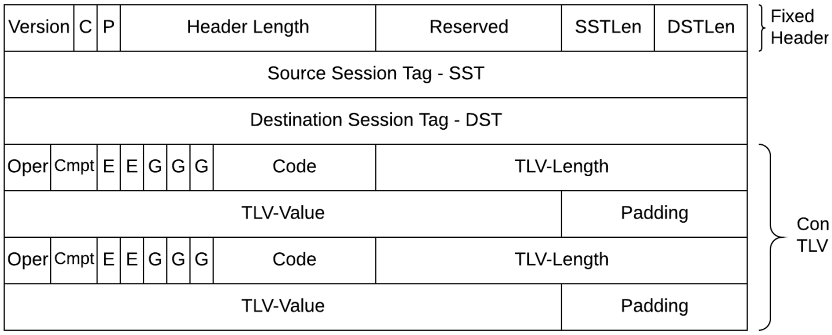


Figure 4: CETP control plane structure.

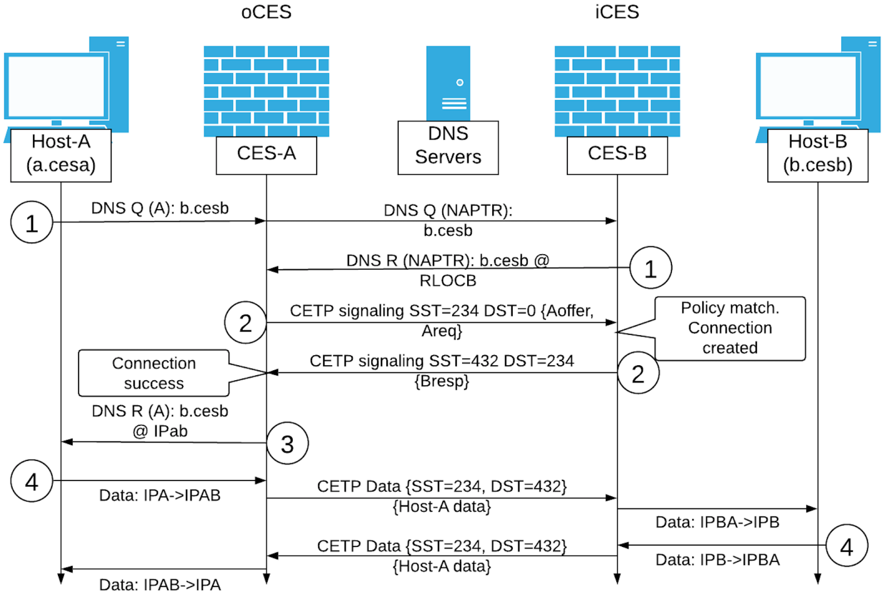

oCES
iCES
Host-A (a.cesa)
CES-A
DNS Servers
CES-B
Host-B (b.cesb)
1
DNS Q (A): b.cesb
DNS Q (NAPTR): b.cesb
DNS R (NAPTR): b.cesb @ RLOCB
1
2
CETP signaling SST=234 DST=0 {Aoffer, Areq}
Policy match. Connection created
Connection success
CETP signaling SST=432 DST=234 {Bresp}
2
DNS R (A): b.cesb @ IPab
3
4
Data: IPA->IPAB
CETP Data {SST=234, DST=432} {Host-A data}
Data: IPBA->IPB
4
CETP Data {SST=234, DST=432} {Host-A data}
Data: IPB->IPBA
Data: IPAB->IPA

Figure 5: CETP signaling – scenario with CES-to-CES communication.

4.2 CETP packet format

CETP packet is built starting from 4-byte header including the protocol version and the header length. The next fields are source and destination session identifiers. Then we have optional payload or signal information. The most important field is field containing the host or network policies which are written in a Type-Length-Value (TLV) format. CETP payload TLV and CETP control plane structure are visible, respectively, in the Figures 3 and 4. TLVs are grouped based on the Type field. Each type field can be further divided into operation, group and code fields. The operation field can take three values: info (when the policy element needs to be announced), query (this is a request for a policy element) and response (which is an answer to previous query). Table 3 presents what information can be found in CETP packets (entries have been grouped) [30], [31].

4.3 Policy negotiation

A policy includes three different sets: offer, requirements and available. Each of these is based on policy elements seen in the Table 3. The whole process of establishing communication between two particular hosts is divided into four steps (Fig. 6). First of all, Host-A needs to resolve FQDN b.cesb. This is done by CES-A which starts the CETP discovery process and creates an NAPTR query for particular FQDN. If the NAPTR is valid, the remote CES (CES-B) returns DNS response with the confirmation of availability and RLOC. The second step is CETP signalling. Source CES (CES-A) starts it to present policy offers and requirements of Host-A. The signalling traffic from CES-A to CES-B has a source session tag (SST). Destination session tag (DST) is initially empty but it will be filled by CES-B after the policy match. The next step is response to the DNS query initially sent by Host-A. Here, CES-A after gaining all required information from the remote network, sends allocated proxy address to Host-A. Finally, Host-A and Host-B can communicate without any issues using assigned in the previous steps proxy addresses. CES tunnels the data traffic using assigned session tags and RLOCs.

If there is no trust between two different CES nodes, a negotiation of policies occurs before host-to-host policy negotiation. The main reason why CES policies are being used are elimination of source address spoofing, denial of service attacks and misbehaving hosts.

The policies are the most important part of CES. CES-level policy defines how different CES nodes can communicate and negotiate with each other. This policy controls signalling and the whole cooperative aspect. There are also host-level, application-level and service-level policies which are more specific and are defined by the end users or providers [32], [33], [34].

4.4 CES - Security mechanisms

There are several security mechanisms already implemented in the current version of CES that minimize the risks from the potential adversaries [35]. These mechanisms are policy-controlled and are responsible for operations such as negotiation of ID types, routing checks and the use of secure locators [11]. As it was mentioned above, these mechanisms eliminate things like unwanted or spoofed traffic [36], [37]. Some of these mechanisms have been described below:

1. Policy-based Communication: this mechanism is responsible for negotiating communication which meets the interests of the sender and the receiver. It is also responsible for authenticating hosts and filtering unwanted traffic.

2. Header Signature: this mechanism makes it possible to provision the signed CETP header and use it in signalling where it can be verified by the receiver.

Table 2: CETP policy elements [1]

Group	Code	Description
CES	- Pow - cesid - headersignature - cace	- The proof-of-work computation - FQDN-based ID of the CES node - Signature of the CETP packet - The CA address for CES validation
Control	- Dstep - caep - terminate - warning - ack - ttl - ratelimit	- FQDN-based destination endpoint ID - The CA address for endpoint validation - Contains session terminating information - Contains the warning information - The acknowledgement number - The time to live for session - The rate limit for session
ID	- Fqdn - maid - moc - msisdn	- FQDN-based ID of the sender - The Mobile Assured ID - The Mobile Operator Certificate - The MSISDN nunber of the host
RLOC	- ipv4 - ipv6 - eth	- An IPv4 address (RLOC) of the CES - An IPv6 address (RLOC) of the CES - An MAC address (RLOC) of the CES
Payload	- ipv4 - ipv6 - eth	- IPv4 encapsulation of the user payload - IPv6 encapsulation of the user payload - Eth encapsulation of the user payload

3. CES Authentication: a local CES needs to authenticate to the remote CES before sending any traffic. For this purpose, CES nodes can either use FQDN (CES-ID) or just RLOCs. Additionally, it is also possible to use CA and X.509 certificates.

4. Secure signalling: CES can use lower layer protocols to transport signalling data. It is possible to put signalling in Transport Layer Security/Transmission Control Protocol (TLS/TCP) or IP Security (IPSec).

5. Proof-of-Work: the principle of this security mechanism is to push all computation burden to the sender, not the receiver. It makes more difficult to flood the victim.

4.5 Realm Gateway

Realm Gateway (RGW) is a functionality of CES for phased implementation of the CES-to-CES communication and, in general, interoperability. For outbound connections, RGW behaves almost the same as traditional NAT device. It creates a session and monitors outbound and inbound traffic [38], [39]. However, in opposite to NAT, RGW allows inbound connections from the Internet to the private network. It uses Circular Pool of Public Addresses (CPPA) to provide this [40]. CPPA runs whenever the device receives inbound DNS query for FQDN [41]. The CPPA algorithm offers three types of inbound traffic:

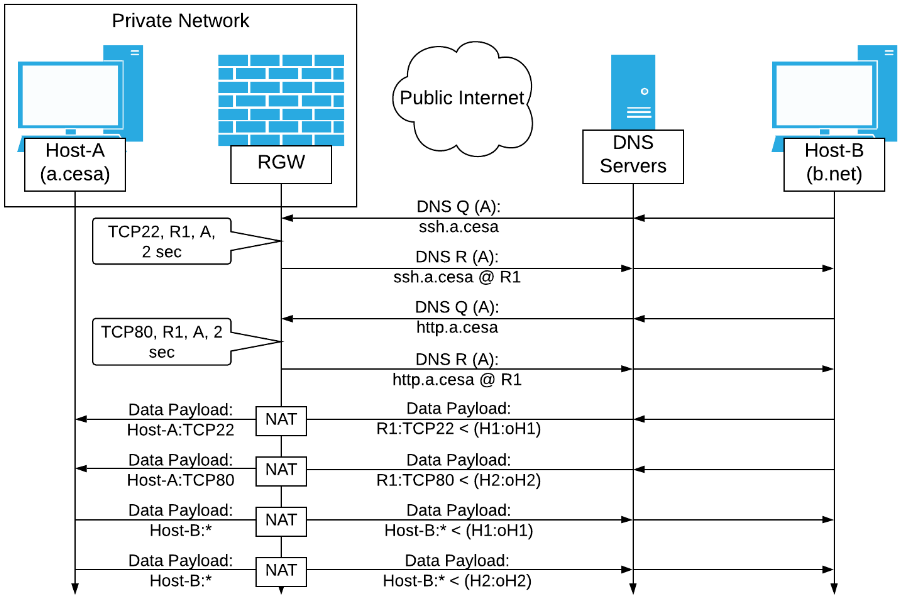


Figure 6: CETP signaling – scenario with RGW (oCES - Outbound CES, iCES - Inbound CES.

1. a general purpose connection served by CPPA when DNS query with FQDN of the host or service has been found.
2. incoming HTTP(S) traffic handled by the reverse HTTP proxy.
3. inbound mapping similar to port forwarding in NAT.

First of all, CPPA temporarily allocates a public IP address whenever RGW receives a DNS query for FQDN. RGW replies with a DNS response carrying the allocated public address and TTL=0. CPPA creates also the half-connection state in RGW which is used for data transmission. Finally, if RGW receives any data matching created previously half-connection state then RGW upgrades the state to a full connection and returns public address to the circular pool. This is for efficiency reasons. The inbound traffic reaches the private host without any issues [42]. The process of serving the connections from the Internet by RGW is shown in Fig. 6.

4.6 RGW – Security mechanisms

RGW can be also a target for various attacks [32]. The most important method is obviously the DNS protocol. If we abuse the protocol by DNS flooding to FQDNs of the hosts and use source address spoofing, we can put RGW in the state where all addresses from CPPA will be used. Thus, every new and legitimate inbound connection will be just blocked [41] resulting in the DoS attacks. The other way is, for instance, reserving CPPA addresses by sending malicious traffic from botnets [43]. RGW has few security mechanisms that protects it from the adversaries. UDP connection state can only be created after the signalling phase: if RGW receives a packet that does not match already seen traffic then the corresponding state is monitored as potentially malicious. The state can be monitored as long as needed and by analyzing the history of these hosts can lead to blacklisting them.

Resources are being granted according to the reputation level: RGW uses white-, grey- and blacklisting to classify DNS servers. By default, DNS servers are on the gray list and have best effort access to

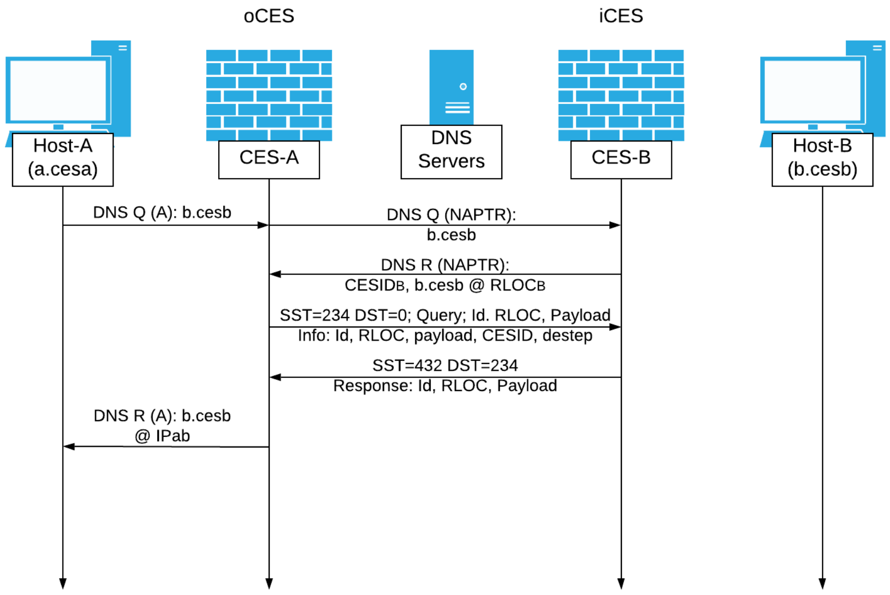


Figure 7: CETP connection establishment – 1 RTT

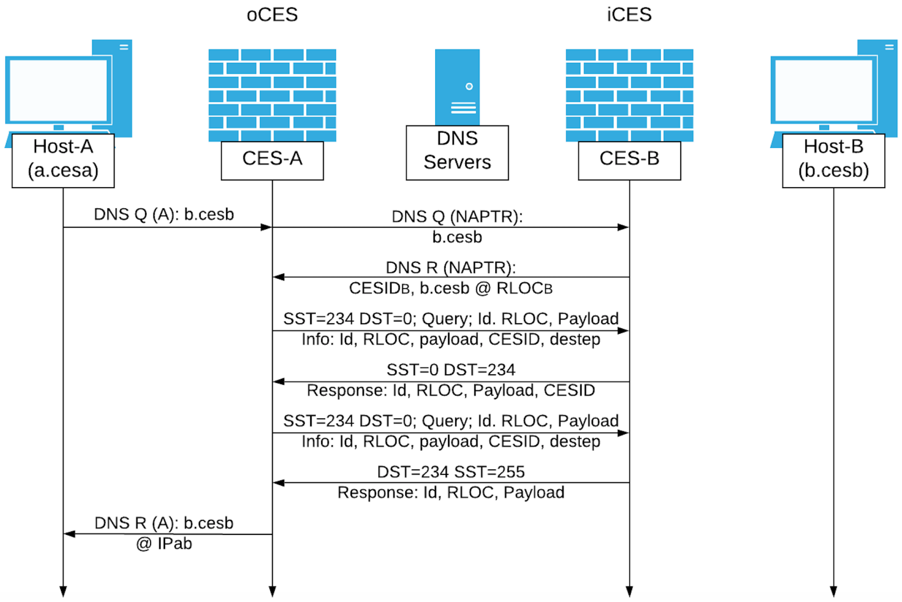

oCES
iCES
Host-A
(a.cesa)
CES-A
DNS
Servers
CES-B
Host-B
(b.cesb)
DNS Q (A): b.cesb
DNS Q (NAPTR):
b.cesb
DNS R (NAPTR):
CESIDB, b.cesb @ RLOCB
SST=234 DST=0; Query; Id. RLOC, Payload
Info: Id, RLOC, payload, CESID, destep
SST=0 DST=234
Response: Id, RLOC, Payload, CESID
SST=234 DST=0; Query; Id. RLOC, Payload
Info: Id, RLOC, payload, CESID, destep
DST=234 SST=255
Response: Id, RLOC, Payload
DNS R (A): b.cesb
@ IPab

Figure 8: CETP connection establishment – 2 RTT

the RGW. Servers can be white-listed if they meet specific criteria. They can also be black-listed if they does not meet the requirements, e.g., they are generating malicious traffic. The known prevention is also rate-limiting CPPA address allocation. Another method that is worth mentioning is TCP-Splice method which is based on challenging the sender by the RGW with a cookie embedded in the Initial Sequence Number (ISN). If the TCP handshake completes, RGW accepts the connection. TCP-splicing technique blocks however the same connections if the packets come from a blacklisted source. This is to prevent the connection hijacking.

Only authenticated hosts can create the flow state: the mechanism works based on DNS extensions or additional records that identify the source of DNS query. According to this information, aggressive host can be blocked or rate-limited [43].

4.7 DNSCrypt

In brief, DNSCrypt is a network protocol which provides the ability to authenticate and encrypt DNS traffic [44]. DNSCrypt encapsulates plain DNS traffic in an encrypted packet in order to detect tampering. The solution protects against man-in-the-middle attacks but it is also very helpful in mitigating UDP-based amplification attacks or just DNS spoofing. DNSCrypt can use either UDP or TCP with port 443. To authenticate the traffic, the client needs to trust the public key of the provider. This public key is used to verify the certificates which are downloaded by the client using DNS queries. The certificates however contain short term public keys which are used to encrypt the data. The encryption is applied in both directions – to queries and responses.

4.8 DNSSEC

The Domain Name System Security Extensions (DNSSEC) [45] is a group of specifications that secure specific aspects of DNS protocol. In general, DNSSEC is an extension of DNS protocol which helps the clients to authenticate DNS data and its integrity. The solution does not support confidentiality, so it is often used with DNSCrypt. DNSSEC was designed to protect from using malicious DNS data, e.g. by DNS poisoning. The general idea is that all DNS replies are digitally signed. By checking the digital signature, the client knows if the data is tampered. DNSSEC can protect not only IP addresses in A or AAAA fields, but also other fields such as MX, TXT etc. The received data needs to be authenticated so indirectly DNSSEC protects from DoS attacks.

4.9 DNSCrypt algorithm

The first step of the implemented DNSCrypt algorithm is to create private key for the communication. The algorithm has also to verify resolver's public key. It checks precisely if the provided key is in correct format. Now the DNSCrypt module have to query the resolver. It is preparing the appropriate DNS packet with flags, then send it to the resolver and wait for the response. When the module receives the response, it has to check if the obtained certificate is valid. If it receives appropriate certificate, it can continue the exchange and query the resolver. The query is preparing appropriate DNS packet and it concatenates all fields. Then, the algorithm chooses whether it uses TCP or UDP protocol at the transport layer. Both protocols and their functions have encryption function from the beginning. The function uses specific encryption algorithm and uses client's private key and resolver's public key. When the packet has been encrypted, it can be sent to the resolver. In the opposite order, the received encrypted traffic is decrypted by the appropriate function. The resolver encrypts traffic with client's public key and resolver's private key. Obviously, all the traffic has to match DNSCrypt traffic if it has to be properly decrypted. Otherwise, it is dropped.

4.10 DNSSEC algorithm

The algorithm starts with breaking down the domain into segments: the parent domain and the child domain. Next, the algorithm has to obtain Start of Authority (SOA) records for both domains. The zone has NS records and they have to be determined for the requested parent and child domains. The next step involves obtaining records from the parent domain nameservers Delegation Signer (DS) which refer to the DNS Public Key (DNSKEY) Resource Record (RR) and hold a hash digest of the DNSKEY RR.

In other words, DS is used to authenticate the DNSKEY RR. The algorithm queries requested domain nameservers for DNSKEY and Resource Record Signature (RRSIG) records. Then, it needs to verify whether DS and DNSKEY records are signed correctly and that signatures have not expired. The same is done for RRSIG. If the whole authentication chain from DNSSEC Trust Anchor to child domain is verified, the algorithm returns that the DNS response is valid.

5 Attack scenario

CETP connection can be established in two modes: 1 round trip time (RTT) or 2 RTT[1]. In 1 RTT scenario (Fig. 7, upon the reception of the DNS response at CES, the CES encodes a CETP packet and sends it to the remote CES which was found in the DNS response. The remote CES searches the packet it receives for query TLVs such as receiver host-ID, RLOC or payload type alongside the sender's offer. ID and Destep TLVs are used for identifying both ends of the communication. The Destep TLV identifies host behind the remote CES. There are also two unique values such as SST and DST as we already mentioned. If initial CES finds all requested TLVs in the last response packet, CES considers the connection is established. Hence, the connection is established in 1 RTT. The critical point here is that we do not have authentication or encryption of initial DNS packets we are exchanging. This means that the attacker can do whatever he likes if he is able to perform man-in-the-middle attack. DNS is not protected in the local network nor in the transit network between two CES nodes. For instance, the initial target, hostb.cesb, can be changed to different host the same way as the node can strip SSL. Next, the response can be changed too. We can modify both RLOC or CES_ID and this can affect where the next traffic will go. CETP connection can also be established in 2 RTT as it is visible in Figure 8. Note, that we can notice that the initial DNS exchange stays the same and again the attacker has access to this information. Again, this be can man-in-the-middle attack with tampering the data or just dropping particular packets to launch DoS attack. What is worth to mention here, CETP protection, e.g. IPSec, is not mandatory. This means that if the lower layers used to transport CETP are not encrypted, we can modify the CETP content too [35].

Attack scenarios for 1 RTT and 2 RTT are shown in Figures 9 and 10, respectively. Red arrows indicate which phases of DNS packets exchange can be affected directly by the attacker. It is clearly visible that the malicious party can modify the contents of these packets and thus affect the whole communication. On the other hand, orange rectangles show which CETP packets can be attacked directly or indirectly if the underlying DNS packets exchange is broken.

6 Evaluation

In Fig. 11 the utilized experimental test-bed is illustrated. The test-bed supports two different scenarios: the first is related to CES-to-CES communication and the second simulates RGW. This is the reason why one of the CES in this configuration is optional and can be disabled to switch the scenario from the first to the second. In the middle, there is a computer which is tapped in the line and listens to every packet crossing the public network. This node is able to influence all passing packets. This computer has also two physical interfaces attached to both private networks so we can simulate man-in-the-middle scenario in every network. Every node has logging turned on so we can see in the real-time manner what is exactly happening. CES-to-CES scenario engages both CES nodes and the traffic starts in one private domain and end in the second domain. RGW scenario uses only one CES node and the traffic is initiated by man-in-the-middle node staying in the middle provider block. The adversary node placed in the middle has Scapy installed on it which is a Python packet crafting tool. This tool is used to tamper with packets. The scenario that is worth showing is the one with the plaintext DNS packets. By default, every DNS

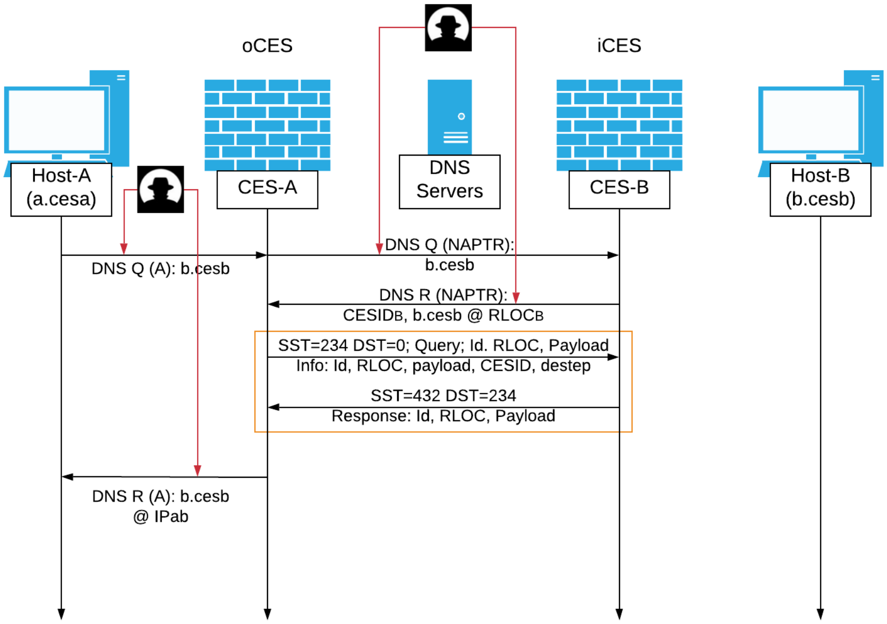


Figure 9: Attack scenario – 1 RTT

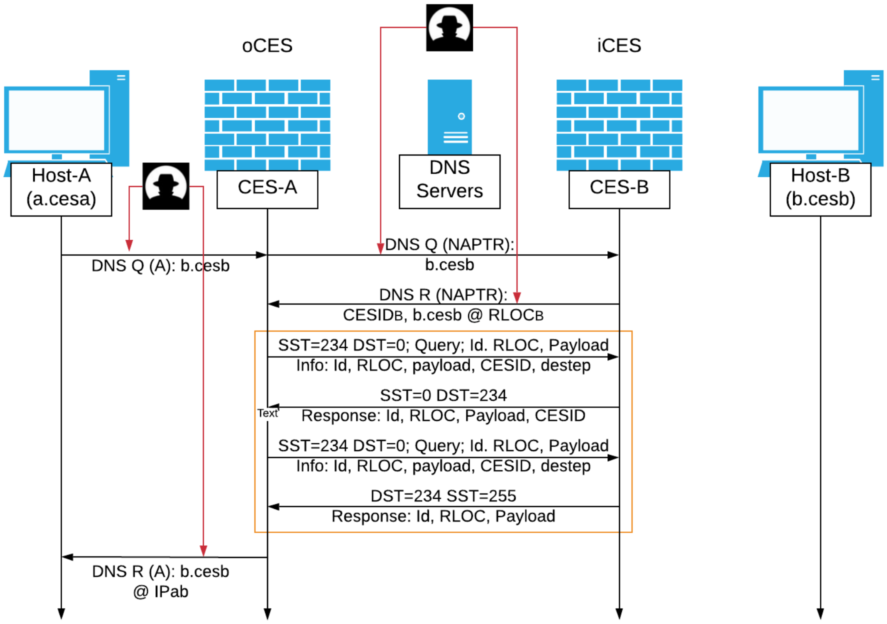

oCES
iCES
Host-A
(a.cesa)
CES-A
DNS
Servers
CES-B
Host-B
(b.cesb)
DNS Q (A): b.cesb
DNS Q (NAPTR):
b.cesb
DNS R (NAPTR):
CESIDB, b.cesb @ RLOCB
SST=234 DST=0; Query; Id. RLOC, Payload
Info: Id, RLOC, payload, CESID, destep
SST=0 DST=234
Text
Response: Id, RLOC, Payload, CESID
SST=234 DST=0; Query; Id. RLOC, Payload
Info: Id, RLOC, payload, CESID, destep
DST=234 SST=255
Response: Id, RLOC, Payload
DNS R (A): b.cesb
@ IPab

Figure 10: Attack scenario – 2 RTT

and CETP traffic are traveling in plaintext because there is no encryption. Everyone can disclose what is being transferred thereby the adversary can profile the target or tamper with the traffic using man-in-the-middle attacks and Scapy. This can be seen in Figure 11. If we add encryption to this scenario using prepared DNSCrypt algorithm, the second scenario is totally different. All DNS and CETP traffic is now encrypted when traveling through the resolver. Now, let us check the performance of both solutions. It

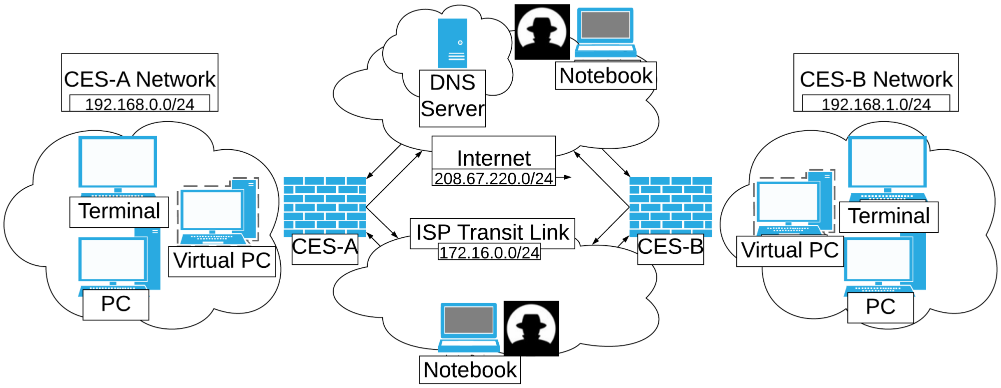


Figure 11: Implementation of the CES-to-CES and RGW test-bed.

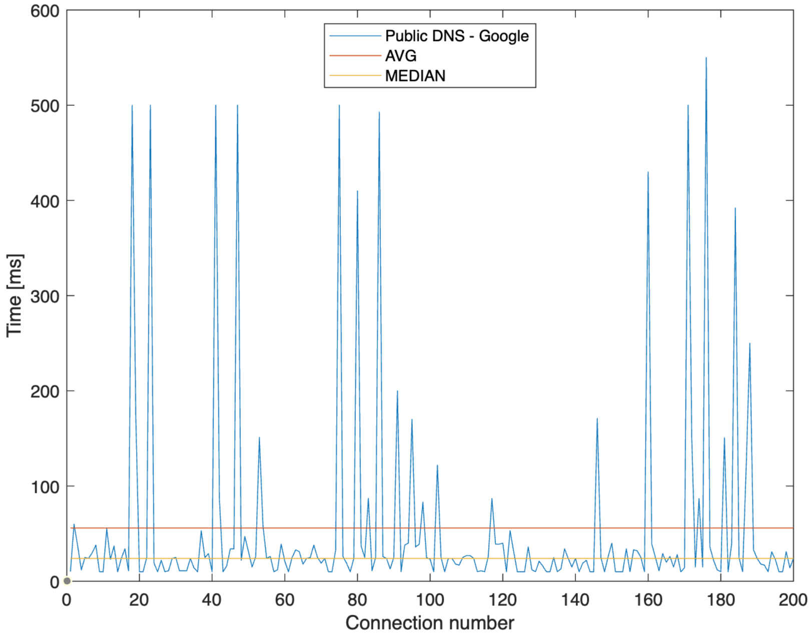


Figure 12: DNS response time for Public DNS (Google)

seems that DNS with encryption is a bit faster than that with packets being sent in plaintext. The chosen DNSCrypt resolver seems to send responses faster than the public DNS server. The differences are, however, not significant. In Figs. 12 and 13 one can see the duration of DNS responses for Public DNS – Google and DNSCrypt – OpenDNS, respectively. The average value of the response for Public DNS – Google equals 55.99 ms, the median equals 24 ms and the standard deviation equals 108.83 ms. The average value for OpenDNS equals 53.945 ms, the median equals 11.5 ms and the standard deviation equals 116.64 ms. All values were calculated based on 200 connections per each scenario. Overall DNSCrypt is a bit faster. The cumulative distribution of DNS query duration is visible in Figure 14. It is clearly visible that the DNS curve is above the public DNS curve. For instance, DNS response of 50 or less milliseconds is measured in 87% of cases for DNSCrypt and in 83% of cases for the public DNS

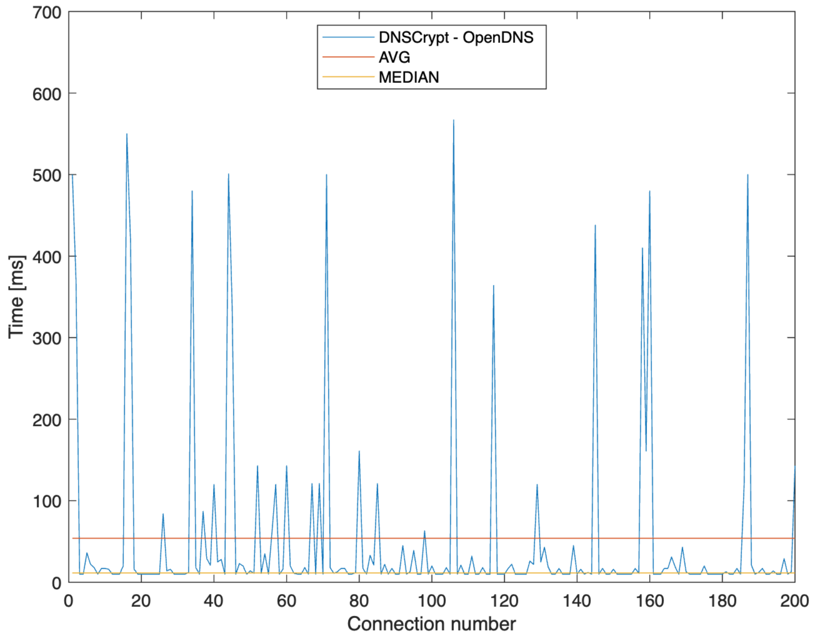


Figure 13: DNS response time for DNSCrypt (OpenDNS)

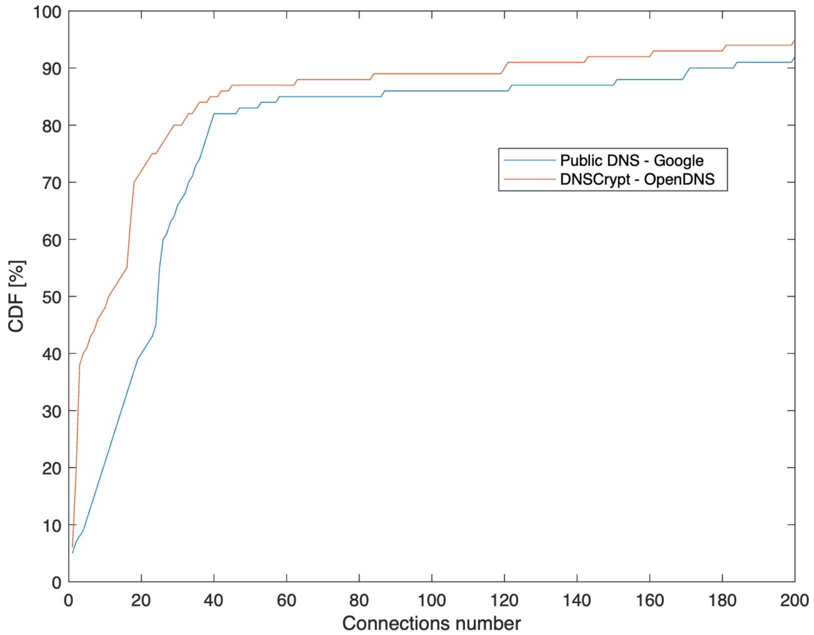


Figure 14: CDF of DNS response time for Public DNS (Google) and DNSCrypt (OpenDNS)

server. Scenario with DNSSEC is totally different. DNSSEC is much slower than usual DNS queries. This occurs because DNSSEC algorithm needs to operate on many records and compute cryptographic functions in order to authorize the domain and the whole DNSSEC Trust Anchor. In Figure 15 one can see the differences between cumulative distributions of regular DNS and DNSSEC. DNSSEC curve is flattened. For instance, DNS response of 50 or less milliseconds is measured in 83% of cases for regular

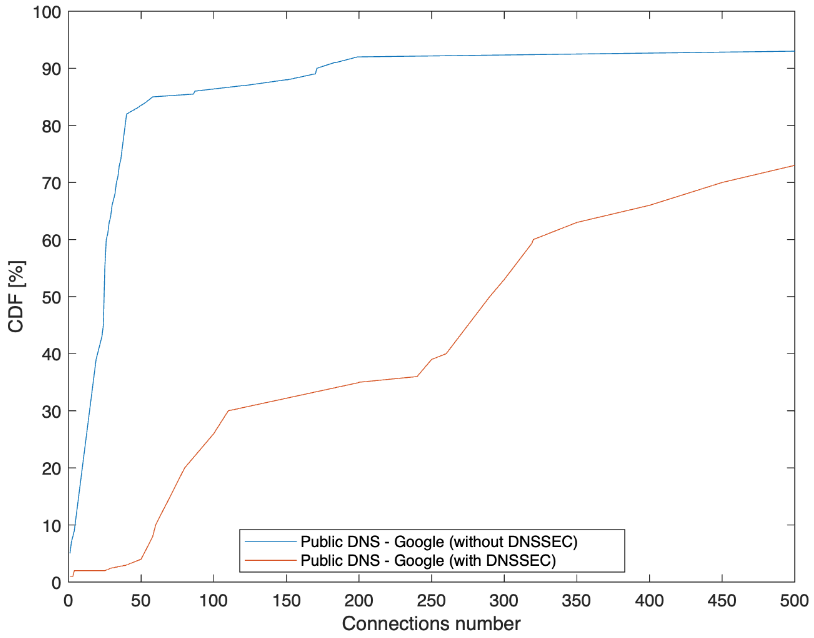


Figure 15: CDF of DNS response time for Public DNS without DNSSEC (Google) and with DNSSEC (Google)

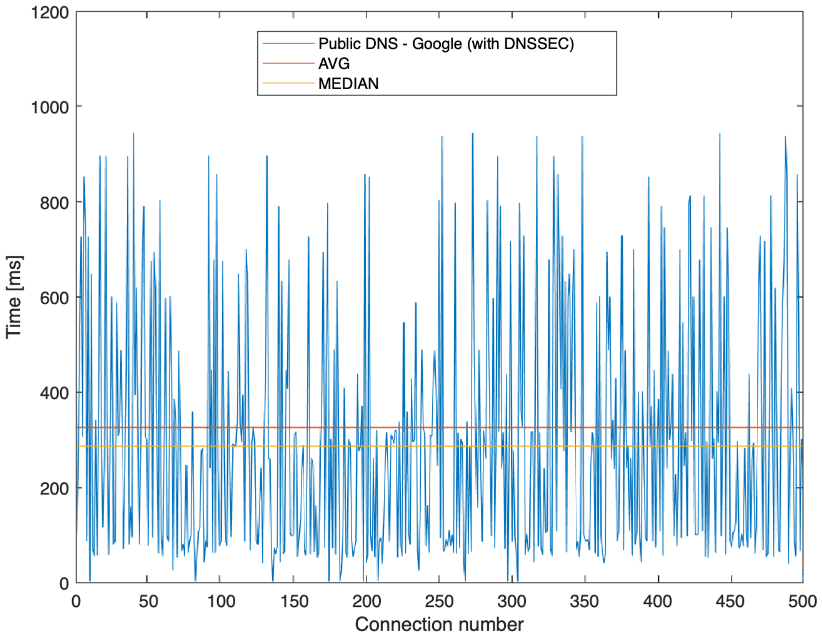


Figure 16: DNS response time for Public DNS with DNSSEC (Google).

DNS and 4.5% of cases for the DNSSEC. This is different than for the previous scenario. In figure 16 you can see DNSSEC scenario with the average value of 325.984 milliseconds, the median value of 286.5 milliseconds and the standard deviation of 294.33 ms. All calculations in these cases were based on 500 connections. The values of DNSSEC scenario are much higher than these for DNSCrypt. The reason for this is longer chain of trust that needs to be verified everytime DNS response is requested. The comparison of these values is shown in Table 3.

Table 3: State-of-the-art comparison between the approach and statistical parameters for different DNS solutions

Approaches/parameters	Public DNS - Google	DNSCrypt - OpenDNS	Public DNS with DNSSEC - Google
Average	55.99 ms	53.945 ms	325.984 ms
Median	24 ms	11.5 ms	286.5 ms
Standard deviation	108.83 ms	116.64 ms	294.33 ms

7 Conclusion

It is well-known that DNS protocol which relies on plaintext data can be attacked in many ways. It can be sniffed, mangled or just blocked. However, the attack model requires a malicious device and the attacker being located between two endpoints. In this paper, we show how implementation of the special DNSCrypt and DNSSEC modules can improve the security of Customer Edge Switching at the cost of longer DNS exchange latencies. We show that both scenarios, CES and Realm Gateway (RGW) can be affected by the attackers. Protecting DNS and CETP packets by DNSCrypt and DNSSEC gives expected results. Our main contribution, based on the experimental results, is that we evaluate the communication and show what are the additional latencies caused by these solutions. In more detail, the results show that the obtained average latency value of 63.575 ms and the median of 24 ms for Google - Public DNS server. DNSCrypt is a bit faster with the average value of 59.38 ms and the median of 11.5 ms. Finally, DNSSEC is much slower than previously mentioned solutions with the average value of 325.984 ms and the median of 286.5 ms. Considering all obtained experimental results, DNSCrypt and DNSSEC is worth implementing and should be used to secure CES. Experimental results showed that the use of DNSCrypt can be faster than traditional solution and DNSSEC adds authentication mechanism at the expense of considerable delay added to DNS packet exchange latencies.

Acknowledgements

This research was funded by the National Centre for Research and Development under Gospostrateg Programme framework, and more speciffically 5G@PL project entitled ”Deployment of 5G network in Polish market” grant agreement: Gospostrateg 1/38302/19/NCBR/2018.

References

[1] A. A. B. A. Ijaz, M. Ylianttila, M. Liyanage, and A. Gurtov, *A Comprehensive Guide to 5G Security*. Wiley, March 2018.

[2] Ericsson, “5G security. scenarios and solutions,” June 2015, https://www.lianapress.ae/releases/computers/5g-security-scenarios-and-solutions.html [Online; accessed on September 15, 2020].

[3] N. Beijar, “Celtic project mevico: Tutorial on customer edge swiching,” November 2012, mobile Network Evolution for Individual Communication Experience.

[4] R. Kantola, J. L. Santos, and N. Beijar, “Policy Based Communications for 5G Mobile with Customer Edge Switching,” *Wiley Security and Communication Networks*, vol. 9, no. 16, pp. 3070–3082, May 2015.

[5] R. Kantola, “Cooperative Security for the Internet and 5G,” January 2017, https://take-5g.org/wp-content/uploads/2017/11/RK-Cooperative-Security-at-CyberTrustSprint.pdf [Online; accessed on September 15, 2020].

[6] R. Kantola, "5G - TAKE5 Test Network and 5G@II," November 2016, http://www.re2ee.org/5G-5GatII-Elisa-17-11-2016.pptx.pdf [Online; accessed on September 15, 2020].

[7] F. A. Ed and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP," IETF RFC 4787, January 2007, https://tools.ietf.org/html/rfc4787 [Online; accessed on September 15, 2020].

[8] J. L. Santos and J. M. Tilli, "Evolved NAT and TCP SYNPROXY," March 2018, http://www.re2ee.org/SoftFIREChallenge-EIT-2018.pdf [Online; accessed on September 15, 2020].

[9] R. Kantola, "Future Internet and 5G Using Customer Edge Switching and Ubiquitous Trust Processing + what is it and what are the benefits," August 2015, http://www.re2ee.org/CES-tutorial-introduction.pdf [Online; accessed on September 15, 2020].

[10] R. Kantola, "Implementing Trust-to-Trust with Customer Edge Switching," in *Proc. of the 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA'10), Perth, Western Australia, Australia*. IEEE, April 2010, pp. 1092–1099.

[11] J. L. Santos, R. Kantola, N. Beijar, and P. Leppäaho, "Implementing NAT Traversal with Private Realm Gateway," *Proc. of the 2013 IEEE International Conference on Communications (ICC'13), Budapest, Hungary*, pp. 3581–3586, June 2013.

[12] R. Kantola, J. L. Santos, and H. Kabir, "White Paper on Cooperative Security for 5G and the Internet," November 2018, https://www.researchgate.net/publication/329070326_White_Paper_Cooperative_Security_for_5G_and_the_Internet [Online; accessed on September 15, 2020].

[13] P. Leppaaho, N. Beijar, R. Kantola, and J. L. Santos, "Traversal of the Customer Edge with NAT-Unfriendly Protocols," in *Proc. of the 2013 IEEE International Conference on Communications (ICC'13), Budapest, Hungary*. IEEE, June 2013, pp. 2933–2938.

[14] R. Kantola, H. Kabir, and P. Loiseau, "Cooperation and end-to-end in the Internet," *International Journal of Communication Systems*, vol. 30, no. 12, pp. e3268:1–18, February 2017.

[15] P. A. F. P. T. Eugster and R. a. K. Guerraoui Anne-Marie, "The Many Faces of Publish/Subscribe," *ACM Computing Surveys*, vol. 35, no. 2, June 2003.

[16] P. Francis and R. Gummadi, "IPNL: A NAT-extended internet architecture," in *Proc. of the 2001 ACM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM'01), San Diego, California, USA*. ACM, August 2001.

[17] I. Stoica, D. Adkins, S. Zhuang, and S. a. S. Shenker Sonesh, "Internet Indirection Infrastructure," *IEEE/ACM Transactions on Networking*, vol. 12, no. 2, pp. 205–0218, April 2004.

[18] M. Gritter and D. R. Cheriton, "An Architecture for Content Routing Support in the Internet," in *Proc. of the 3rd conference on USENIX Symposium on Internet Technologies and Systems (USITS'01), Berkeley, California, USA*. USENIX, March 2001.

[19] J. Pan, S. Paul, R. Jain, and M. Bowman, "MILSA: A Mobility and Multihoming Supporting Identifier Locator Split Architecture for Naming in the Next Generation Internet," in *Proc. of the 2008 IEEE Global Communications Conference (GLOBECOM'08), New Orleans, Louisiana, USA*. IEEE, December 2008, pp. 1–6.

[20] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The Locator/ID Separation Protocol (LISP)," IETF RFC 6830, January 2013, https://tools.ietf.org/html/rfc6830 [Online; accessed on September 15, 2020].

[21] E. Nordmark and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6," IETF RFC 5533, August 2001, https://tools.ietf.org/html/rfc5533 [Online; accessed on September 15, 2020].

[22] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," IETF RFC 4423, May 2006, https://tools.ietf.org/html/rfc4423 [Online; accessed on September 15, 2020].

[23] X. Liu, X. Yang, and Y. Lu, "To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-Node Botnets," in *Proc. of the 2008 ACM SIGCOMM Conference on Data Communication (SIGCOMM'08), Seattle, Washington, USA*. ACM, August 2008.

[24] A. Yaar, A. Perrig, and D. Song, "SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks," in *Proc. of the 2004 IEEE Symposium on Security and Privacy (SP'04), Berkeley, California, USA*. IEEE, May 2004, pp. 130–143.

[25] S. G. Hong and H. Schulzrinne, "PBS: Signalling Architecture for Network Traffic Authorization," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 89–96, July 2013.

[26] R. Hancock, G. Karagiannis, J. Loughney, and S. V. d. Bosch, "Next Steps in Signaling (NSIS): Framework," IETF RFC 4080, June 2005, https://tools.ietf.org/html/rfc4080 [Online; accessed on September 15, 2020].

[27] A. Osseiran and F. B. et al, "Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 26–35, May 2014.

[28] M. Mealling and R. Daniel, "The Naming Authority Pointer (NAPTR) DNS Resource Record," IETF RFC 2915, September 2000, https://tools.ietf.org/html/rfc2915 [Online; accessed on September 15, 2020].

[29] H. Kabir, J. L. Santos, and R. Kantola, "Securing the Private Realm Gateway," in *Proc. of the 2016 IFIP Networking Conference (IFIP Networking) and Workshops (IFIPNetworking'16), Vienna, Austria*. IEEE, May 2016, pp. 243–251.

[30] J. L. Santos, "CES to CES Security," August 2015, http://www.re2ee.org/CES-tutorial-day1-security.pdf [Online; accessed on September 15, 2020].

[31] M. Pahlevan, "Signaling and Policy Enforcement for Cooperative Firewalls," Master's thesis, Aalto University, February 2013.

[32] J. L. Santos, "Realm Gateway Security," August 2015, http://www.re2ee.org/CES-tutorial-day2-security.pdf [Online; accessed on September 15, 2020].

[33] M. H. B. Mohsin, "Security Policy Management for a Cooperative firewall," Master's thesis, Aalto University, September 2018.

[34] I. Fofana, "Policy Creation and Bootstrapping System For Customer Edge Switching," Master's thesis, Aalto University, November 2017.

[35] H. Kabir, "Security Mechanisms for a Cooperative Firewall," Master's thesis, Aalto University, February 2014.

[36] Z. Yan, R. Kantola, and Y. Shen, "Unwanted traffic control via hybrid trust management," in *Proc. of the 2012 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12), Liverpool, UKI*. IEEE, June 2012, pp. 666–673.

[37] L. Zhang, Z. Yan, and R. Kantola, "Privacy-preserving trust management for unwanted traffic control," *Future Generation Computer Systems*, vol. 72, pp. 305–318, July 2017.

[38] J. L. Santos, "Customer Edge Switching Realm Gateway Tutorial Session - Day 1," August 2015, http://www.re2ee.org/CES-tutorial-day1-Jesus.pdf [Online; accessed on September 15, 2020].

[39] J. L. Santos, "Customer Edge Switching Realm Gateway Tutorial Session - Day 2," August 2015, http://www.re2ee.org/CES-tutorial-day2-Jesus.pdf [Online; accessed on September 15, 2020].

[40] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. Groot, and E. Lear, "Address Allocation for Private Internets," IETF RFC 1918, February 1996, https://tools.ietf.org/html/rfc1918 [Online; accessed on September 15, 2020].

[41] H. Kabir, R. Kantola, and J. L. Santos, "Preprint of Security Mechanisms for a Cooperative Firewall," in *Proc. of the IEEE 6th International Symposium on Cyberspace Safety and Security (CSS'14), Paris, France*. IEEE, August 2014, pp. 814–818.

[42] J. L. Santos, "Private Realm Gateway," Master's thesis, Aalto University, November 2012.

[43] J. L. Santos and R. Kantola, "Transition of IPv6 with Realm Gateway 64," in *Proc. of the 2015 IEEE International Conference on Communications (ICC'15), London, UK*. IEEE, June 2015, pp. 1–7.

[44] F. Denis, "DNSCrypt Specification," June 2020, https://github.com/DNSCrypt/dnscrypt-protocol/blob/master/DNSCRYPT-V2-PROTOCOL.txt [Online; accessed on September 15, 2020].

[45] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "DNS Security Introduction and Requirements," IETF RFC 4033, March 2005, https://tools.ietf.org/html/rfc4033 [Online; accessed on September 15, 2020].

Author Biography

Slawomir Nowaczewski received the B.S. and M.S. degrees in Computer Science and Telecommunication from Gdansk University of Technology in 2012 and 2014. Currently he is a PhD student at Warsaw University of Technology. His research interests include IT security and everything related to it.

Wojciech Mazurczyk received the B.Sc., M.Sc., Ph.D. (Hons.), and D.Sc. (habilitation) degrees in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland, in 2003, 2004, 2009, and 2014, respectively. He is currently a Professor with the Institute of Computer Science at WUT and a head of the Computer Systems Security Group. He also works as a Researcher at the Parallelism and VLSI Group at Faculty of Mathematics and Computer Science at FernUniversitaet, Germany. His research interests include bio-inspired cybersecurity and networking, information hiding, and network security. He is involved in the technical program committee of many international conferences and also serves as a reviewer for major international magazines and journals. From 2016 he is Editor-in-Chief of an open access Journal of Cyber Security and Mobility, and from 2018 he is serving as an Associate Editor of the IEEE Transactions on Information Forensics and Security. He is also a Senior Member of IEEE.