

Deriving ChaCha20 Key Streams From Targeted Memory Analysis

Peter McLaren, William J Buchanan, Gordon Russell, Zhiyuan Tan
School of Computing,
Edinburgh Napier University,
Edinburgh, UK.

Abstract—There can be performance and vulnerability concerns with block ciphers, thus stream ciphers can be used as an alternative. Although many symmetric key stream ciphers are fairly resistant to side-channel attacks, cryptographic artefacts may exist in memory. This paper identifies a significant vulnerability within OpenSSH and OpenSSL and which involves the discovery of cryptographic artefacts used within the ChaCha20 cipher. This can allow for the cracking of tunneled data using a single targeted memory extraction. With this, law enforcement agencies and/or malicious agents could use the vulnerability to take copies of the encryption keys used for each tunnelled connection. The user of a virtual machine would not be alerted to the capturing of the encryption key, as the method runs from an extraction of the running memory. Methods of mitigation include making cryptographic artefacts difficult to discover and limiting memory access.

Index Terms—network traffic; decryption; memory analysis; Virtual machine introspection; Secure Shell; Transport Layer Security; stream ciphers; ChaCha20

I. INTRODUCTION

There is an increasing challenge between the rights of citizens to privacy and the rights of society to protect itself from adversaries [1][2]. The breaking of encryption tunnels is thus one of the major debating points, and where law enforcement agencies often aim to gather tools and methods which break these tunnels, or where we fix vulnerabilities in tools in order to avoid these tunnels from being broken. In most cases we now perform a key negotiation phase – typically with ECDH (Elliptic Curve Diffie-Hellman) – and then use a symmetric key method to encrypt the traffic within the tunnel.

The cracking of the key exchange process and of the symmetric key used in the tunnel are, in most cases, too costly to crack. Unfortunately, the key exchange process can leave behind trails of evidence in memory which can provide significant clues to the symmetric key being used. While this has been demonstrated for block ciphers, such as for the Advanced Encryption Standard (AES) [3][4], this paper outlines how well-used applications such as OpenSSH and OpenSSL allow for every generated key in the ChaCha20 stream cipher to be revealed within a fairly fast discovery time. As virtualized environments enable access to virtual machine resources from more privileged levels such as hypervisors or hypervisor consoles, applications operating at that level can extract live virtual machine memory. Extraction is most effective when a virtual machine is paused but it is not necessary. So, virtualized environments present an opportunity to find

keys without impacting the target and for target applications to be unaware of extraction.

The rest of the paper is structured as follows. Section II discusses related research including side-channel studies and background on stream ciphers and ChaCha20 cipher implementations is presented in Section III. Section IV provides relevant details of the framework and its implementation is given in Section V. The results are presented and discussed in Section VI and conclusions drawn in Section VII.

II. RELATED WORK

This paper focuses on the decrypting network traffic encrypted with ChaCha20-Poly1305 cipher. Prior studies have investigated potential vulnerabilities in cipher design and in cipher implementation. Researchers have found no vulnerabilities in ChaCha20 design. For example, differential attacks using techniques such as identifying significant key bits only succeeded with reduced cipher rounds and significant volumes of plaintext-ciphertext pairs [5][6]. Combined linear and differential analysis improves performance, but is similarly restricted [7].

ChaCha20 implementations may be vulnerable to side-channel attacks. While the cipher design may prevent timing attacks [8], correlating power electromagnetic radiation when specific cryptographic activities are performed may leak key stream information [9][10]. Engendering instruction skips, for example by using a laser or electromagnetic pulse, could potentially produce the key stream but timing the activity would be challenging [11]. Furthermore, these approaches may be impractical in real-world scenarios.

Cryptographic artefacts have been found in device memory. For instance, RSA keys may be discovered in virtual machine images [12] [13]. Studies have also discovered DES and AES cipher keys in cold-boot attacks [3], Skipjack and Twofish key blocks in virtual memory [4], and AES session keys in virtual memory [14]. Although these approaches use entropy measures to determine possible keys, they do not decrypt ciphertext encrypted with ciphers such as AES in Counter mode and ChaCha20 which require nonces/initialization vectors. This study builds on the TLskex [14] and MemDecrypt studies [15] which used privileged monitors to extract identified virtual machine process memory to identify TLS 1.2 AES keys, and SSH AES keys and initialization vectors, respectively. Instead, this study uses a different algorithm to find ChaCha20

cipher keys and nonces in device memory enabling SSH and TLS sessions to be decrypted in a non-invasive manner. The approach may enable decryption of Adiantum encrypts [16], the Google disk-encryption algorithm based on XChaCha20, an extension to ChaCha20 and Salsa20 with a longer nonce [17].

III. STREAM CIPHERS

Secure protocols use encryption to provide confidentiality for secure communications between parties. While asymmetric encryption ciphers are used in secure protocol set-up stages, for performance symmetric ciphers encrypt the confidential information. Symmetric ciphers are commonly classified as being stream ciphers, where plaintext is encrypted bit-by-bit or byte-by-byte or block ciphers, where blocks of a specific size are encrypted. This paper focuses on stream ciphers.

Stream ciphers generate a random key stream from an evolving state [18]. The key stream is then typically XOR-ed with the plaintext to generate ciphertext [18]. Software implementations for stream cipher have been found to be faster than block ciphers although possibly more difficult to implement [19]. Stream ciphers have typically been used in embedded technologies such as Internet of Things (IoT) devices and smartphones [20]. Stream ciphers, as well as block ciphers, have been supported by secure protocols. However, with vulnerabilities leading to the planned deprecation of the RC4 stream cipher for protocols such as Secure Shell (SSH) [21] and Transport Layer Security (TLS) [22], alternative stream ciphers have been under consideration. In particular, the ChaCha20 stream cipher with the Poly1305 authenticator [23] has been adopted in secure protocol implementations such as OpenSSH [24], and OpenSSL [25], as well for Google Chrome on smartphones [26]. The discovery of the key stream or inputs to key stream generation may be an unacceptable vulnerability for stream ciphers including ChaCha20-Poly1305.

Stream cipher cryptographic artefacts are memory-resident at points in time. Furthermore, these artefacts, as well as the key stream are on a program stack, in the heap or in shared memory. If timely acquisition of target device memory is obtained, the stream or artefacts may be discovered. With the growth of forensic technologies that enable memory access to targets such as desktops, servers, smartphones, and IoT devices, an opportunity exists to discover these artefacts. Although researchers have investigated ChaCha20 side-channel attacks with intermediate state leakage [9] and without [10], no studies analyze memory so this paper presents a new approach to decrypting secure communications encrypted with the ChaCha20 cipher. A single memory extract suffices to find the cryptographic artefacts for decryption. Furthermore, the approach is faster and less invasive than methods that use side-channel techniques.

OpenSSH and PuTTY implement `chacha20-poly1305@openssh.com` while OpenSSL [26] versions above 1.1 implement variations where the asymmetric cipher used in key exchange vary, e.g. ECDHE-RSA-CHACHA20-POLY1305 [27]. Both implementations adhere to the RFC

ChaCha20 and Poly1305 for IETF Protocols [23] which is based on Bernstein’s ChaCha20 cipher proposal [28], a variation of the earlier Salsa20 cipher [8].

A. ChaCha20 ciphering process

The ChaCha20 cipher generates key streams of 64-bytes. Inputs to key stream generation are independent of plaintext or ciphertext similar to other eSTREAM proposals [29] but unlike stream ciphers such as Helix [8]. This enables parallel cipher-text generation with consequent performance improvement. 20 rounds of mathematical calculations using XOR, addition and rotation using as inputs four 4-byte constants, a random 32-byte key, a 4-byte counter, and a 12-byte nonce (Bernstein originally specified the nonce and counter lengths to be eight). However, this is not a material difference in the investigations). The 4-byte constants are 0x61707865, 0x3320646e, 0x79622d32, and 0x6b206574 or in ASCII ‘apxe’, ‘3 dn’, ‘yb-2’, and ‘k et’. In ChaCha20 these strings are concatenated. The counter, which typically starts at 0 or 1 increments for each 64-byte plaintext block [23].

In the `chacha20-poly1305@openssh.com` implementation, memory is allocated to hold a structure comprising key stream input fields, the 64-byte key stream itself, and an index pointer. The packet lengths are encrypted separately from the remainder of the payload so four structures are required: two for encrypting outgoing lengths and payloads, and the same again for incoming encrypted data. The memory contents of the concatenated constant string are *expand 32-byte k*. The nonce is a sequence number and counters for the encrypted packet lengths and payloads are zero and unity, respectively.

The OpenSSL implementation of ChaCha20-Poly1305 differs in a number of respects as required by IETF RFC ChaCha20-Poly1305 Cipher Suites for Transport Layer Security (TLS) [27]. As encrypting packet length is not required in TLS two memory structures are used for encrypting outgoing messages and decrypting incoming messages. Memory used for ChaCha20 inputs is temporary as the encryption structure is assembled from other sources. Also, the nonce is an XOR of the sequence number and the vector generated during the initial handshake when the cipher keys are obtained.

ChaCha20 takes a 256-bit key and a 32-bit nonce (and which includes a counter). This creates a key stream which is then XOR-ed with the plaintext stream as illustrated in Figure 1. In software-only implementations, it is often more than three times faster than AES [27], and is well suited to lower-powered devices and in real-time communications. ChaCha20 operates on 32-bit words at a time with a key of 256 bits ($K=(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$). This outputs blocks of 512 bits for the key stream (Z), and which is XOR-ed with the plaintext stream. The state of the encryption is stored within 16x32-bit word values and arranged as a 4x4 matrix:

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \quad (1)$$

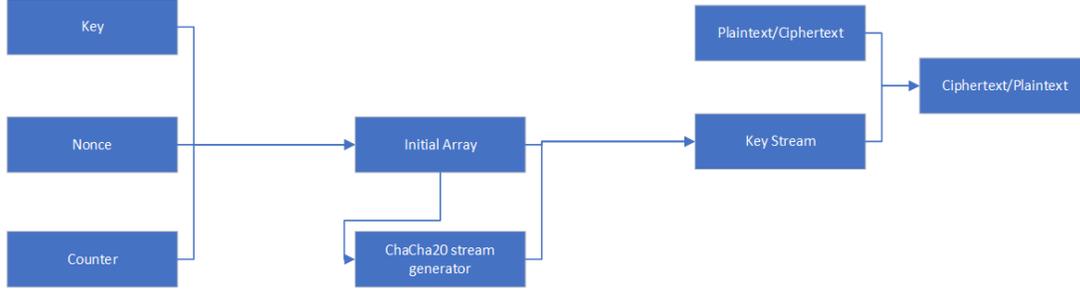


Fig. 1. ChaCha Encryption/Decryption Flow

The initial state contains 16x32-bit values with constant values (0x61707865, 0x3320646e, 0x79622d32, 0x6b206574) the key ($k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7$), the counter (c_0) and the nonce (n_0, n_1, n_2, n_3):

$$\begin{bmatrix} 0x61707865 & 0x3320646e & 0x79622d32 & 0x6b206574 \\ k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ c_0 & n_0 & n_1 & n_2 \end{bmatrix} \quad (2)$$

The counter thus has 32-bits (1 x 32 bits), and the nonce has 96-bits (3 x 32 bits). ChaCha20 then defines a quarter round as shown in Algorithm 1.

Result: QR(a,b,c,d)

```

a = a + b;
d = d ⊕ a;
d = (d) << 16;
c = c + d;
b = b ⊕ c;
b = (b) << 12;
a = a + b;
d = d ⊕ a;
d = (d) << 8;
c = c + d;
b = b ⊕ c;
b = (b) << 7;
  
```

Algorithm 1: Quarter round

There are then 20 rounds (10 for column rounds and 10 for diagonal rounds) as shown by Algorithm 2.

IV. DECRYPTION FRAMEWORK

The decryption framework is comprised of data capture, analysis, and decrypt components. Each component is modifiable or replaceable so that different devices, target operating systems, ciphers, and protocols can be addressed. Details of the component design for ChaCha20 are presented in the following paragraphs.

Data Collection. Target device network packets and volatile memory are extracted. Complete SSH and TLS sessions originating from the target device are captured for later examination. The indicator for extraction of target volatile is the client transmission of a protocol message indicating that the initialization phase is complete. These messages are *New Keys*

Data: X is created with K, c and n

Result: Z is the resultant key stream.

$y \leftarrow X$;

for $i = 0$ to 9 **do**

```

(x0, x4, x8, x12) ← QR(x0, x4, x8, x12);
(x5, x9, x13, x1) ← QR(x5, x9, x13, x1);
(x10, x14, x2, x6) ← QR(x10, x14, x2, x6);
(x15, x3, x7, x11) ← QR(x15, x3, x7, x11);
(x0, x5, x10, x15) ← QR(x0, x5, x10, x15);
(x1, x6, x11, x12) ← QR(x1, x6, x11, x12);
(x2, x7, x8, x13) ← QR(x2, x7, x8, x13);
(x3, x4, x9, x14) ← QR(x3, x4, x9, x14);
  
```

end

$Z \leftarrow X + y$

Algorithm 2: Keystream

and *Client Finished* for SSH and TLS Version 1.2 respectively. Cryptographic artefacts have then been generated and are likely to be memory-resident and memory can be extracted for any outgoing message in the network session.

Memory Analysis. Candidate cryptographic artefacts are discovered in memory extracts. Initially, the component searches for the constant string *expand 32-byte k* to discover candidate ChaCha20 data structures. Although unlikely for the string to be present in non-base structures, a second step assesses whether the 32-byte block after the constant string in a candidate base structure's might be a key. Encryption keys must be unpredictable, i.e. random. Key randomness can be evaluated using the Shannon entropy definition [30]:

$$H = - \sum_{i=1}^n p(i) \log_2 p(i) \quad (3)$$

where p_i is the normalized frequency of the i th byte in the message i.e. $p(i) = f(i)/n$. So, where the entropy of the 32-byte block exceeds a threshold, a candidate base structure is identified and the key, nonce and counter are retained.

Decrypt Analysis. Cryptographic artefacts output by the memory analysis component are input parameters in decrypt analysis. In each instance, the candidate key and nonce group is decrypted and verified according to the protocol used. For SSH, the groups are used to decrypt incoming and outgoing packet lengths and payloads. The packet length groups are

identified if the decrypted packet length meets Equation (2) for short packets, typically in the authentication and channel set-up phases. For larger packets, the decrypted packet length supports SSH packet reassembly. Decrypts with the remaining cryptographic groups are analyzed to establish compliance with SSH protocol specifications. For TLS, decrypts are analyzed to establish compliance with TLS. protocol specifications.

$$\begin{aligned} \text{packet data length} = & \\ & \text{decrypted packet length} + \\ & \text{size}(\text{packet length field}) + \\ & \text{size}(\text{MAC field}) \end{aligned} \quad (4)$$

V. IMPLEMENTATION

The framework is implemented in a virtualized environment as illustrated in Figure 2. Implementations on other technologies which facilitate packet capture and target memory access should be possible. The Xen hypervisor [31] offers benefits over alternatives including the presence of LibVMI [32] and PyVMI [33] libraries providing access to the volatile memory of live virtual machines. Because of its small trusted computing base, Xen is managed by a privileged virtual machine, which runs or initiates the framework components. The privileged virtual machine also provides the unprivileged guests with network and disk access.

The data collection component inspects virtual machine network traffic. Each packet is redirected to a local queue using an iptables rule and NetFilterQueue 0.8.1 [34], and protocol fields to determine whether SSH or TLS sessions have been initiated. Each SSH and TLS packet is written to file. Memory extraction uses PyVMI, LibVMI, and Volatility libraries [35].

Memory analysis obtains candidate ChaCha20 cryptographic artefacts. Each memory extract file is searched for the constant string. Although false positives are unlikely, additionally the entropy of the following 32-byte block is compared with a threshold, experimentally found to be 4.5. If the threshold is exceeded, a base structure has been identified and the key, nonce, and counter fields are retained for decryption as groups.

The decrypt analysis component iterates through the key and nonce groupings. For SSH, the first four encrypted bytes in packets are decrypted using the Chacha20poly1305 package with counter value 0 [36]. For a valid group the first four bytes represent the packet length and Equation (2) holds. For ChaCha20, the decrypts with other groups are validated. If the decrypted padding length obeys Equation (3) as specified in SSH Transport Layer Protocol [37] the following blocks are decrypted to evaluate compliance with the SSH authentication and channel set-up specifications [38][39]. For TLS, the entire data block is decrypted with cryptographic artefact groups. Although TLS supports other higher-level protocols such as SMTP, HTTP-over-TLS is perhaps the most commonly used and so compliance of the decrypt with the HTTP 1.1 specification [40] is assessed. Valid decrypts are retained for user

Data: Extracts folder, entropy threshold

Result: Z = candidate artefacts

for *extract* in *folder* **do**

```

i = 0;
while not extract EOF do
  i := locate 'expand 32-byte k' in extract;
  if i > 0 then
    if entropy extract[i+16:i+48] > threshold
      then
        Z += key, nonce, and counter;
        i += 64;
      else
        i += 16;
      end
    end
  end
end

```

Algorithm 3: Memory Analysis

inspection.

$$4 \leq \text{padding length} \leq 255 \quad (5)$$

The physical environment for experimentation is a Core 2 Duo Dell personal computer with 40 GB of disk storage and 3 GB of RAM. This hosts the hypervisor, the privileged virtual machine, an unprivileged Windows virtual machine, and an unprivileged Ubuntu virtual machine. The hypervisor is Xen Project 4.4.1 and the hypervisor console is Debian release 3.16.0-4-amd64 Version 1. Tests run on untrusted Windows client and Linux server virtual machines. The Windows clients runs the Windows 10 (10.0.16299) operating system with 2 GB of memory and 40 GB of disk. A Linux virtual machine runs an Ubuntu 14.04 build (“Trusty”) with 512 MB of allocated memory and 4 GB of disk storage. The PuTTY suite [41] is used for SSH client application testing with SSH server functionality provided by openssh-server. OpenSSL 1.1.0h provides TLS client and server functionality.

VI. EVALUATION

For SSH evaluation the PuTTY ‘pscp’ program is executed from the Windows command line using requests of the form:

```
pscp -P nnnn 'filename' @ipaddress:/home/name
```

where *nnnn* is the target port, ‘*filename*’ is the file being transmitted, *name* is a user account on the target Ubuntu server, *ipaddress* is the target server IP address and */home/name* is the Ubuntu server target folder for the transmitted file. An Ubuntu service is started from the bash command line to listen to client SSH messages with requests of the form:

```
/usr/sbin/sshd -f /root/sshd_config -d -p nnnn
```

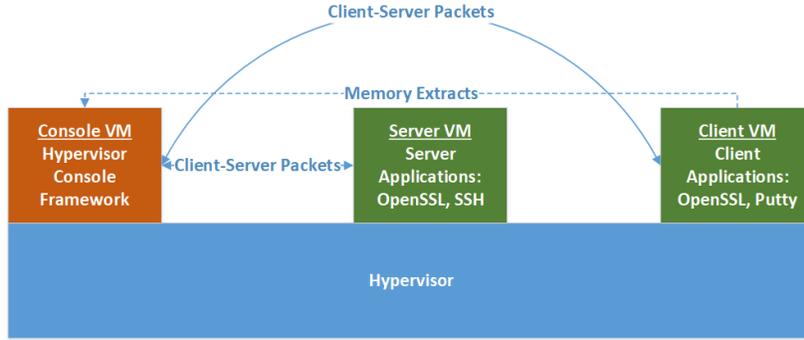


Fig. 2. Virtualized environment framework

where *nnnn* is the port number the service listens on and *sshd_config* contains configuration details. Here, *sshd_config* contains the string ‘ciphers chacha20-poly1305@openssh.com’. Client and server tests execute OpenSSL from the command line. The OpenSSL server emulates a web server with:

```
openssl s_server -accept 443 -cert crt.pem -key key.pem
-WWW
```

where *crt.pem* and *key.pem* are certificate and key files. The client connects to the OpenSSL server with:

```
openssl s_client [-cipher CIPHER] -connect a.b.c.d:443
```

where *CIPHER* identifies the encryption cipher, key exchange and authentication algorithms (here, ECDHE-RSA-CHACHA20-POLY1305) and *a.b.c.d* the OpenSSL server IP address. Client input simulates browser requests, e.g. ‘GET / HTTP/1.1’, ‘Host: a.b.c.d.’, ‘Accept-Encoding: gzip, deflate’, ‘Accept: */*’.

ChaCha20 base structures were found in 100% of instances. For the SSH chacha20-poly1305@openssh.com protocol four base structures were discovered in Windows and Linux application memory. For OpenSSL, one base structure was discovered for ECDHE-RSA-CHACHA20-POLY1305 as shown in the highlighted section of Figures 3 and 4 respectively. These discoveries leads to key stream generation and the rapid decryption of complete SSH sessions including server user credentials, file names and uploaded file contents between 150 bytes and 1 MB as well as the decryption of outgoing client TLS traffic. Differences between SSH and TLS relates to their implementations. PuTTY/OpenSSH structures are heap-resident so memory extracts for successful decryption may not be linked to client SSH message transmission. By contrast, OpenSSL structures are stack-resident and may therefore be overwritten. This limitation prevents Linux server successful searches for the constant string although high-entropy regions identify candidate encryption keys. Consequently, full SSH sessions are decryptable whereas only outgoing TLS sessions are currently decryptable when applying the algorithms. A

SSH decrypt is illustrated in Figure 5 and example output from the analysis stages is presented in Figure 6.

Memory and decrypt analysis components decrypt rapidly. The memory analysis durations are less than 0.5 (SSH) and 0.1 (TLS) seconds as shown in Table I. As single extract analysis requires a maximum 0.018 seconds, parallel processing memory extract analysis offers significant performance opportunities. Although memory analysis is independent of file size, decrypt analysis durations are proportionate to the volume of encrypted traffic.

TABLE I
MEMORY ANALYSIS DURATIONS

	SSH	TLS
Maximum	0.407	0.027
Minimum	0.007	0.011
Mean	0.144	0.021
Standard Deviation	0.153	0.006

VII. COUNTERMEASURES

Fortunately, countermeasures to discovering the ChaCha20 basic structures exist, and hiding the constant string makes discovery more challenging. Possible measures are copying the constant string segments to registers and assembling the structure in the encryption routine, encrypting the constant string, or randomly segmenting the constant string. Perhaps, the most effective approach is assembling the base structure on the stack, as for OpenSSL, and clearing stack contents immediately after the encryption process. The cryptographic artefacts can still be discovered by searching for high-entropy measures but the process is comparatively slower with durations exceeding 4 minutes.

VIII. CONCLUSIONS

Implementations of ChaCha20-Poly1305 encryption using commonly used applications and libraries for SSH and TLS communications are vulnerable to decrypt analysis on a single memory extract. As memory analysis identifies cryptographic artefacts with 100% success, the artefacts could be retained with network sessions for later decryption. This may benefit entities, such as cloud vendors, to assist state agencies

```

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00051710 49 00 4E 00 44 00 4F 00 57 00 53 00 5C 00 53 00 I.N.D.O.W.S.\.S.
00051720 79 00 73 00 74 00 65 00 6D 00 33 00 32 00 5C 00 y.s.t.e.m.3.2.\.
00051730 6B 00 65 00 72 00 6E 00 65 00 6C 00 2E 00 61 00 k.e.r.n.e.l...a.
00051740 70 00 70 00 63 00 6F 00 72 00 65 00 2E 00 64 00 p.p.c.o.r.e...d.
00051750 6C 00 6C 00 00 00 00 00 23 56 9C 5E 87 A8 00 0C l.l.....#Ve*+`..
00051760 50 97 0B 00 10 FC 0B 00 00 00 00 00 00 00 00 00 P-...ú.....
00051770 60 01 00 00 01 00 00 00 32 EA 21 00 FD FD FD FD `.....2ê!.ýýýý
00051780 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B expand 32-byte k
00051790 8C E4 DF 52 2A D9 57 B0 3B A4 C1 0A E1 AA 34 BB EaBR*ÜW";=Á.á*4»
000517A0 1B 43 8D 10 E7 4E 1C 3C F5 B3 84 2E 08 74 34 59 .C..çN.<ð³,..t4Y
000517B0 01 00 00 00 00 00 00 00 00 00 00 00 00 00 06 .....
000517C0 30 5D 60 F4 3C CA DC 6A 56 77 E5 05 C1 2E 5F D1 0]`ð<ÈÜjvwá.Á. Ñ
000517D0 C7 AF B2 DA 2A 1F 13 F6 51 79 A0 D8 0F A5 AD C0 ç²`ú*. .òQy Ø.Y.Ä
000517E0 DF E5 33 46 97 02 A7 F4 56 26 C5 59 E2 64 4A 82 .á3F-.sòv&ÁYáDJ,
000517F0 49 56 2C 65 81 AC 62 BB C7 9A 1D 48 3C D1 4F DE IV,e.-b»çð³.H<NòP
00051800 04 00 00 00 65 78 70 61 6E 64 20 33 32 2D 62 79 ...expand 32-by
00051810 74 65 20 6B 88 64 89 57 30 5E 9A 81 4D 80 D8 05 te k`d#w0^s.Meø.
00051820 A8 AD C5 E5 3F F2 4D C4 6D 1F 93 EB 0A F0 45 33 `..Áá?òMAm."e.øE3
00051830 CD EF D0 DE 01 00 00 00 00 00 00 00 00 00 00 00 fiðp.....
00051840 00 00 00 06 3A AF 2C C7 63 B2 F8 E3 29 32 05 3C ...;";,çc²øá)2.<
00051850 09 2F 3A 61 59 E0 0E 8B 34 40 22 EC 1C CE 08 EA ./:aYà.<4@"i.î.ê
00051860 F9 A7 48 39 76 85 07 64 3C E0 AA 86 37 1E 5B BB ù$H9v...d<à*+7.[»

```

Fig. 3. SSH Base Structures in Memory

```

000FDC00 30 D7 38 C6 FC 7F 00 00 48 DC 2F 8A 4E 00 00 00 0x0ÈU...HÜ/ŠN...
000FDC10 B8 94 6A E5 FC 7F 00 00 11 42 27 C6 FC 7F 00 00 ,`jáü...B'ÈU...
000FDC20 F0 DE 96 58 07 02 00 00 F0 DE 96 58 07 02 00 00 ðD-X...ðD-X...
000FDC30 40 00 00 00 00 00 00 00 B6 3C 27 C6 FC 7F 00 00 @.....q<'ÈU...
000FDC40 30 D7 38 C6 FC 7F 00 00 00 00 00 00 00 00 00 00 0x0ÈU.....
000FDC50 00 00 00 00 00 00 00 00 65 00 00 00 00 00 00 00 .....e.....
000FDC60 BC FA 24 53 83 FD 44 56 99 5E B7 4A 88 3F 77 B9 wú$SfýDVm^`J`?w²
000FDC70 94 AE 72 C4 64 63 74 C5 33 D7 FA F0 7F 57 8F 5E "ørÁdctÁ3xúð.W.^
000FDC80 7B C3 D4 D4 D0 42 F0 84 F1 E4 60 0F 35 AF EB 8B {ÃÖðBð,,ñá`.5`ē<
000FDC90 6D 43 9F F7 4D 5F 00 97 63 72 6F DA 7A 27 5C 0E mCÿ+M.-croÜz'\.
000FDCA0 65 78 70 61 6E 64 20 33 32 2D 62 79 74 65 20 6B expand 32-byte k
000FDCB0 FB 71 9A C1 9A 80 B9 90 1B AB C4 75 4E 75 D2 EA ðqšÁše¹...AuNuðè
000FDCc0 FF 13 B0 37 AB C9 34 BE DC 61 7C D4 75 B3 C1 20 y.`7«É4%0a|òu*Á
000FDCD0 02 00 00 00 8D E5 03 27 54 9C FC 0C 3B EC 13 BA .....á.'Tøü.;i.º
000FDCe0 A4 3E 3E 0C 72 FB 00 00 DB 3A 27 C6 FC 7F 00 00 w>>.rû..Û:'ÈU...
000FDCf0 87 EB B4 00 07 02 00 00 B0 33 C1 0D 00 00 00 00 †è'.....³Á.....
000FDD00 D8 3A 1F 0A 00 00 00 00 87 EB B4 00 00 00 00 00 Ø:.....†è'.....
000FDD10 8E 09 A7 0C 00 00 00 00 54 76 93 0F 00 00 00 00 ž.š.....Tv".....
000FDD20 38 4D 96 58 07 02 00 00 20 00 00 00 00 00 00 00 8M-X.....

```

Fig. 4. TLS Base Structure in Memory

```

SSH client service request: name: ssh-userauth
SSH authorisation request: name: █████ service: ssh-connection auth type: none
SSH authorisation request: name: █████ service: ssh-connection auth type: password: █████
SSH channel open: channeltype: session
SSH channel request: channel: simple@putty.projects.tartarus.org
SSH channel request: subsystem: sftp
SFTP Initialisation: Version no: 3
Stat: Data: /home/█████
SFTP Open: Data: /home/█████/test2.txt
Write: Data:
Close:
SSH session close:]

```

Fig. 5. SSH Client Decrypt Example

in decrypting criminals' communications, without conflicting with local privacy laws. To achieve this aim, future work should focus on performance improvements such as multi-threading and pipe-lining, as well as investigating other protocols, encryption ciphers and modes, and technologies that uses encrypted communications channels.

REFERENCES

[1] Z. Bauman, D. Bigo, P. Esteves, E. Guild, V. Jabri, D. Lyon, and R. B. Walker, "After snowden: Rethinking the impact of surveillance," *International political sociology*, vol. 8, no. 2, pp. 121–144, 2014.

[2] R. Iphofen, "Safety is more important than privacy," *Times Higher Education*, <https://www.timeshighereducation.com/features/safety-is-more-important-than-privacy>, 2016, [Online; accessed 29-Jan-2019].

[3] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten, "Lest we remember: cold-boot attacks on encryption keys," *Communications of the ACM*, vol. 52, no. 5, pp. 91–98, 2009.

[4] C. Maartmann-Moe, S. E. Thorkildsen, and A. Årnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys," *digital investigation*, vol. 6, pp. S132–S140, 2009.

[5] J.-P. Aumasson, S. Fischer, S. Khazaei, W. Meier, and C. Rechberger, "New features of latin dances: analysis of salsa, chacha, and rumba," in

```

INFO:TLS Memory Analyser:Extract analysis started for CHACHA20 on
folder h:\opensslchacha\28Jan at 29-Jan-19 16:39:23.108 with entropy 4
INFO:TLS Memory Analyser:chacha20 state found in
h:\opensslchacha\28Jan\092109\openssl.exe.092116.364774424576-364775473151.dmp
at 29-Jan-19 16:39:23.123
INFO:TLS Memory Analyser:Extract analysis completed at 29-Jan-19 16:39:23.135

INFO:TLS Decrypt Analyser:ChaCha20 Decrypt Analysis started at 29-Jan-19 16:39:30.883
INFO:TLS Decrypt Analyser:No of client keys = 2, IVs = 2
INFO:TLS Decrypt Analyser:Decrypt GET HTTP 1.1
Host: 192.168.137.3
User-Agent: Mozilla/5.0
Accept-Encoding: gzip, deflate
Keep-Alive: 300
Pragma: no-cache
AND THAT is all she wrote
THE END
INFO:TLS Decrypt Analyser:ChaCha20 decrypt successful
INFO:TLS Decrypt Analyser:Packet analysis complete at 29-Jan-19 16:39:30.905

```

Fig. 6. TLS memory and Decrypt Analysis Output

- International Workshop on Fast Software Encryption*. Springer, 2008, pp. 470–488.
- [6] S. Maitra, “Chosen iv cryptanalysis on reduced round chacha and salsa,” *Discrete Applied Mathematics*, vol. 208, pp. 88–97, 2016.
- [7] A. R. Choudhuri and S. Maitra, “Differential cryptanalysis of salsa and chacha—an evaluation with a hybrid model,” *IACR Cryptology ePrint Archive*, vol. 2016, p. 377, 2016.
- [8] D. J. Bernstein, “The salsa20 family of stream ciphers,” in *New stream cipher designs*. Springer, 2008, pp. 84–97.
- [9] B. Jungk and S. Bhasin, “Don’t fall into a trap: Physical side-channel analysis of chacha20-poly1305,” in *2017 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2017, pp. 1110–1115.
- [10] A. Adomnicai, J. J. Fournier, and L. Masson, “Bricklayer attack: A side-channel analysis on the chacha quarter round,” in *International Conference in Cryptology in India*. Springer, 2017, pp. 65–84.
- [11] KDDI Research Inc., “Security Analysis of ChaCha20-Poly1305 AEAD,” <https://www.cryptrec.go.jp/exreport/cryptrec-ex-2601-2016.pdf>, 2015, [Online; accessed 29-Jan-2019].
- [12] F. Rocha and M. Correia, “Lucy in the sky without diamonds: Stealing confidential data in the cloud,” *Proceedings of the International Conference on Dependable Systems and Networks*, pp. 129–134, 2011.
- [13] J. T. Saxon, B. Bordbar, and K. Harrison, “Efficient retrieval of key material for inspecting potentially malicious traffic in the cloud,” in *2015 IEEE International Conference on Cloud Engineering*. IEEE, 2015, pp. 155–164.
- [14] B. Taubmann, C. Frädrieh, D. Dusold, and H. P. Reiser, “Tlskex: Harnessing virtual machine introspection for decrypting tls communication,” *Digital Investigation*, vol. 16, pp. S114–S123, 2016.
- [15] P. McLaren, G. Russell, W. J. Buchanan, and Z. Tan, “Decrypting Live SSH Traffic in Virtual Environments,” *Digital Investigation*, vol. 29, pp. 109–117, 2019.
- [16] P. Crowley and E. Biggers, “Adiantum: length-preserving encryption for entry-level processors,” *IACR Transactions on Symmetric Cryptology*, pp. 39–61, 2018.
- [17] D. J. Bernstein, “Extending the salsa20 nonce,” in *Workshop record of Symmetric Key Encryption Workshop*, vol. 2011, 2011.
- [18] A. Biryukov, “Block ciphers and stream ciphers: The state of the art,” *IACR Cryptology ePrint Archive*, vol. 2004, p. 94, 2004.
- [19] A. Klein, *Stream ciphers*. Springer, 2013.
- [20] C. Manifavas, G. Hatzivasilis, K. Fysarakis, and Y. Papaefstathiou, “A survey of lightweight stream ciphers for embedded systems,” *Security and Communication Networks*, vol. 9, no. 10, pp. 1226–1246, 2016.
- [21] L. Camara, “Deprecating RC4 in Secure Shell (SSH),” <https://tools.ietf.org/id/draft-ietf-curdle-rc4-die-die-die-10.html>, 2018, [Online; accessed 29-Jan-2019].
- [22] A. Popov, “Prohibiting RC4 Cipher Suites,” <https://tools.ietf.org/html/rfc7465>, 2015, [Online; accessed 29-Jan-2019].
- [23] Y. Nir, “ChaCha20 and Poly1305 for IETF Protocols,” <https://tools.ietf.org/html/rfc7539>, 2015, [Online; accessed 29-Jan-2019].
- [24] OpenSSH, “OpenSSH,” <https://www.openssh.com/>, 2018, [Online; accessed 29-Jan-2019].
- [25] OpenSSL Software Foundation, “OpenSSL: Cryptography and SSL/TLS toolkit,” <https://www.openssl.com/>, 2017, [Online; accessed 29-Jan-2019].
- [26] Ianix, “ChaCha Usage and Deployment,” <https://ianix.com/pub/chacha-deployment.html>, 2019, [Online; accessed 29-Jan-2019].
- [27] A. Langley, W. Chang, N. Mavrogiannopoulos, J. Strombergson, and S. Josefsson, “Chacha20-poly1305 cipher suites for transport layer security (tls),” *Internet Engineering Task Force*, 2016.
- [28] D. J. Bernstein, “Chacha, a variant of salsa20,” in *Workshop Record of SASC*, vol. 8, 2008, pp. 3–5.
- [29] D. Hutchison and J. C. Mitchell, “New stream cipher designs,” in *New stream cipher designs*, vol. 4986. Springer, 2008.
- [30] C. E. Shannon, “A mathematical theory of communication,” *Bell system technical journal*, vol. 27, no. 3, pp. 379–423, 1948.
- [31] Xen Project, “Xen Project Software Overview,” https://wiki.xen.org/wiki/Xen_Project_Software_Overview, 2018, [Online; accessed 29-Jan-2019].
- [32] LibVMI, “LibVMI Project,” <http://libvmi.com/>, 2013, [Online; accessed 29-Jan-2019].
- [33] B. D. Payne, “pyvmi – A Python adapter for LibVMI,” <https://github.com/libvmi/libvmi-backup/tree/master/tools/pyvmi>, 2013, [Online; accessed 29-Jan-2019].
- [34] Kerkhoff Technologies, “NetFilterQueue,” <https://pypi.org/project/NetfilterQueue/>, 2017, [Online; accessed 29-Jan-2019].
- [35] Volatility Foundation, “NetFilterQueue,” <https://www.volatilityfoundation.org/>, 2016, [Online; accessed 29-Jan-2019].
- [36] D. Klinec, “Chacha20poly1305,” <https://github.com/ph4r05/py-chacha20poly1305>, 2018, [Online; accessed 29-Jan-2019].
- [37] T. Ylonen and C. Lonvick, “The secure shell (ssh) transport layer protocol,” *Internet Engineering Task Force*, 2005.
- [38] —, “The secure shell (ssh) authentication protocol,” *Internet Engineering Task Force*, 2005.
- [39] —, “The secure shell (ssh) connection protocol,” *Internet Engineering Task Force*, 2005.
- [40] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, “Hypertext transfer protocol–http/1.1,” *Internet Engineering Task Force*, 1999.
- [41] S. Tatham, “PuTTY,” <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>, 2018, [Online; accessed 29-Jan-2019].