CLAIMS

1. A client system comprising a hardware processor and a memory, the hardware processor configured to execute a virtual machine, an introspection engine, and a network filter, the introspection engine and the network filter executing outside of the virtual machine, wherein:

the virtual machine is configured to carry out a communication session with a remote party, the communication session comprising a handshake message followed by an encrypted payload, wherein the handshake message contains an encryption parameter used by the client system to derive an encryption key, and wherein the encrypted payload is encrypted with the encryption key;

the network filter controls a network adapter of the client system and is configured to intercept the handshake message and in response, transmit a notification to the introspection engine; and

the introspection engine is configured to:

infer an occurrence of a first session event of the communication session according to the notification,

identify within the memory a target memory page according to whether a content of the target memory page has changed between the occurrence of the first session event and an occurrence of a second session event of the communication session, and

in response, transmit the content of the target memory page to a decryption engine configured to decrypt the encrypted payload according to the content.

2. The client system of claim 1, wherein the first session event comprises sending the handshake message from the client system to the remote party or receiving the handshake message at the client system.

3. The client system of claim 2, wherein the communication session complies with a Transport Layer Security (TLS) protocol, and wherein the handshake message comprises a ClientHello message or a ServerHello message.

4. The client system of claim 1, wherein the second session event comprises sending an encrypted data packet from the client system to the remote party or receiving the encrypted data packet at the client system, and wherein the data packet is encrypted with the encryption key.

5. The client system of claim 4, wherein the communication session complies with a

Transport Layer Security protocol, and wherein the data packet comprises a part of a ClientFinished message or a part of a ServerFinished message.

6. The client system of claim 4, wherein the data packet comprises a part of the encrypted payload.

7. The client system of claim 1, wherein identifying the target memory page comprises:

selecting a candidate memory page from a pool of memory pages used by the virtual machine;

in response to detecting the occurrence of the second session event, determining according to a page table entry of the candidate memory page whether the candidate memory page has been written to prior to the occurrence of the second session event;

in response to determining whether the candidate memory page has been written to, when the candidate memory page has been written to, selecting the candidate memory page as the target memory page.

8. The client system of claim 1, wherein:

the introspection engine is further configured, in response to the occurrence of the second session event, to copy the content of the target memory page, and in response, to transmit a second notification to the network filter; and

the network filter is configured to intercept a data packet destined for the virtual machine, and in response, to delay delivery of the data packet to the virtual machine until receiving the second notification.

9. The client system of claim 1, wherein the introspection engine is further configured, in response to an occurrence of a third event, to identify the target memory page further according to whether the content of the target memory page has changed between the occurrence of the first session event and the occurrence of the third event, wherein the occurrence of the third event is caused by another communication session concurrent with the communication session.

10. A server computer system comprising a hardware processor configured to execute a decryption engine configured to carry out decryption procedures for a plurality of client systems, a decryption procedure comprising:

receiving an encrypted payload of a communication session carried out between a virtual machine executing on the client system and a remote party; and

in response, decrypting the encrypted payload according to the content of the target memory page,

wherein the communication session comprises a handshake message followed by the encrypted payload, wherein the handshake message contains an encryption parameter used by the client system to derive an encryption key, wherein the encrypted payload is encrypted with the encryption key, and

wherein the client system is configured to execute an introspection engine and a network filter, the introspection engine and the network filter executing outside of the virtual machine, wherein:

the network filter controls a network adapter of the client system and is configured to intercept the handshake message and in response, transmit a notification to the introspection engine, and

the introspection engine is configured to:

infer an occurrence of a first session event of the communication session according to the notification, and

identify the target memory page within a memory of the client system according to whether the content of the target memory page has changed between the occurrence of the first session event and an occurrence of a second session event of the communication session.

11. The server computer system of claim 10, wherein decrypting the encrypted payload comprises:

deriving a candidate decryption key from the content of the target memory page; and

attempting to decrypt the encrypted payload using the candidate decryption key.

12. The server computer system of claim 10, wherein the first session event comprises sending the handshake message from the client system to the remote party or receiving the handshake message at the client system.

13. The server computer system of claim 12, wherein the communication session complies with a Transport Layer Security protocol, and wherein the handshake message comprises a ClientHello message or a ServerHello message.

14. The server computer system of claim 12, wherein the second session event comprises sending an encrypted data packet from the client system to the remote party or receiving the encrypted data packet at the client system, wherein the data packet is encrypted with the encryption key.

15. The server computer system of claim 14, wherein the communication session complies with a Transport Layer Security protocol, and wherein the data packet comprises a part of a ClientFinished message or a part of a ServerFinished message.

16. The server computer system of claim 14, wherein the data packet comprises a part of the encrypted payload.

17. The server computer system of claim 10, wherein identifying the target memory page comprises:

selecting a candidate memory page from a pool of memory pages used by the virtual machine;

in response to detecting the occurrence of the second session event, determine according to a page table entry of the candidate memory page whether the candidate memory page has been written to prior to the occurrence of the second session event;

in response to determining whether the candidate memory page has been written to, when the candidate memory page has been written to, select the candidate memory page as the target memory page.

18. The server computer system of claim 10, wherein:

the introspection engine is further configured, in response to the occurrence of the second session event, to copy the content of the target memory page, and in response, to transmit a second notification to the network filter; and

the network filter is configured to intercept a data packet destined for the virtual machine, and in response, to delay delivery of the data packet to the virtual machine until receiving the second notification.

19. The server computer system of claim 10, wherein the introspection engine is further configured, in response to an occurrence of a third event, to identify the target memory page further according to whether the content of the target memory page has changed between the occurrence of the first session event and the occurrence of the third event, wherein the occurrence of the occurrence of the third event is caused by another communication session concurrent with the communication session.

20. The server computer system of claim 10, wherein the hardware processor is further configured to determine whether the client system comprises malicious software according to a result of decrypting the encrypted payload.

21. A non-transitory computer-readable medium storing instructions which, when executed by a hardware processor of a client system further comprising a memory, cause the hardware processor to form an introspection engine and a network filter, the introspection engine and network filter executing outside a virtual machine executing on the client system, wherein:

the virtual machine is configured to carry out a communication session with a remote party, the communication session comprising a handshake message followed by an encrypted payload, wherein the handshake message contains an encryption parameter used by the client system to derive an encryption key, and wherein the encrypted payload is encrypted with the encryption key;

the network filter controls a network adapter of the client system and is configured to intercept the handshake message and in response, to transmit a notification to the introspection engine; and

the introspection engine is configured to:

infer an occurrence of a first session event of the communication session according to the notification,

identify within the memory a target memory page according to whether a content of the target memory page has changed between the occurrence of the first session event and an occurrence of a second session event of the communication session, and

in response, transmit the content of the target memory page to a decryption engine configured to decrypt the encrypted payload according to the content.

22. A method of decrypting encrypted communications between a client system and a remote party, wherein the client system is configured to execute a virtual machine, wherein:

the virtual machine is configured to carry out a communication session with the remote party, the communication session comprising a handshake message followed by an encrypted payload, wherein the handshake message contains an encryption parameter used by the client system to derive an encryption key, and wherein the encrypted payload is encrypted with the encryption key,

the method comprising:

employing at least one hardware processor of the client system to intercept the handshake message;

employing the at least one hardware processor to infer an occurrence of a first session event of the communication session according to the interception;

employing the at least one hardware processor to identify within a memory of the client system a target memory page according to whether a content of the target memory page has changed between the occurrence of the first session event and an occurrence of a second session event of the communication session;

employing the at least one hardware processor to harvest the encrypted payload; and

decrypting the encrypted payload according to the content of the target memory page.