Norwegian University of Science and Technology
TTM4135 Applied Cryptography and Network Security, Spring 2020
Web Security Lab
Group NN

Ola Nordmann Ola Nordmann Jr. Other Student
Their Friend

Introduction

Q: Generating a symmetric key k just for encrypting that one message seems like an unnecessarily complicated step. Why does GPG do that, instead of just encrypting the message with p?

A: ...

Q: How many bytes does PGP use to store the private signing and public verification keys for each of the two signature types?

A: ...

Q: How many bytes does PGP use to store the signatures in each of the four cases (both long and short messages)?

A: ...

Q: How long, on average, does PGP uses for signature generation and verification in each of the four cases?

A: ...

Q: Discuss your results for the above three measurements. In particular, how well do they correspond to what you expect from what was studied in the lectures? Include an explanation of how the different elements of the keys are stored (such as modulus, exponents, generators).

A: ...

Q: What assurances does someone receive who downloads your public key from the server where you have uploaded it? What is the difference between the role of the certification authority in X509 and the key server in PGP, with regard to the security guarantees they give?

A: ...

Q: Who typically signs a software release like Apache? What do you gain by verifying such a signature?

A: ...

Q: Why did you obtain a certificate from Let's Encrypt instead of generating one yourself?

A: ...

Q: What steps does your browser take when verifying the authenticity of a web page served over `https`? Give a high-level answer.

A: ...

Q: Have a look at the screenshot. What does the string `TLS_DHE_RSA_WITH_AES_128_CBC_SHA` in the bottom left say about the encryption? Address all eight parts of the string.

A: ...

Q: The screenshot is obviously from a few years ago. Do you think the encryption specified by this string is still secure right now? Motivate your answer.

A: ...

Q: What is the purpose and format of an SCT certificate field? Why might a certificate with an SCT not appear in any certificate transparency log?

A: ...

Q: What restrictions on server TLS versions and ciphersuites are necessary in order to obtain an A rating at the SSL Labs site? Why do the majority of popular web servers not implement these restrictions?

A: ...

Q: What are the values of the client and server nonces used in the handshake? How many bytes are they? Is this what you expect from the TLS 1.2 specification?

What is the value of the encrypted pre-master secret in the client key exchange field sent to the server? Is this the size that you would expect given the public key of your server?

A: ...

Q: What was the value of the pre-master secret in the session that you captured? Is this the size (in bytes) that you expect from the TLS specification? Explain how Task 16 shows that this session does not have forward secrecy.

A: ...

Cooperation and Experience

References