

Assignment 4: “Trust me”

eSoc 488: Privacy Technology in Context

Due: Thursday, 18 October 2018

Total Homework/Assignment Points: 100

In this assignment we will explore delegated trust relationships, with PGP and TLS. Your submission should include files called: ‘mr_phony_pants.asc’, ‘nemo.asc’, and your last name followed by ‘.asc’; ‘foo’, and ‘check_sig’; and finally ‘certificate_investigation.’

You and me and PGP

1. [10] Create three key pairs: two should be 4096 bit RSA keys, and one should be ECC with Curve 25519. The RSA keys should be in the names ‘Mr. Phony Pants’ and your own **first and** last name, respectively; the ECC key should use the name ‘~~Nemo~~’ **‘Outis’**. Export the public key to files named ‘mr_phony_pants.asc’, your name followed by ‘.asc’, and ‘nemo.asc’, respectively.¹
2. [5] Create a file called ‘foo’ with exact content: ‘I am the very model of a modern major general.’ Write a script called ‘check_sig.ksh’ that uses gpg to sign the file ‘foo’ with Nemo’s key.
3. [10] Modify the keys so that only the key in your name is ultimately trusted, and Mr. Phony Pants “acts like a certificate authority” for all keys—that is, all keys are valid to each other **only** via Mr. Phony Pants’s key.
4. [5] Verify the signed file ‘foo’ using your own key. ~~Nemo’s~~ Outis’s key should be *fully valid* (but not ultimately trusted): in a comment at the bottom of check_sig.ksh, explain how you know that the signature is from a valid key.

Stuart is a Pirate

Create a file called ‘certificate_investigation,’ and answer the following questions each on a separate line.

1. [10] Find a way to access the web page for our server over TLS. Briefly and clearly describe what you did, and explain why you had to do it.
2. [10] Write a command to print just the certificate fingerprint.
3. [10] Write a command to display the certificate in text form, without printing the encoded version of the request.
4. [10] What does each part of the certificate mean? (Include the OID description).
5. [10] Who is the issuing certificate authority (give the CN)? Why does this matter (i.e., why are you warned when you visit the site)?
6. [20] There is a file symmetrically-encrypted in your directory called ‘hmm.gpg’—can you decrypt it now? Answer, in the file called ‘certificate_investigation.’ What is the decrypted file? Enjoy!

¹These edits were needed due to a bug in gpg, which requires at least five characters for a name. Bah!