ISS - Crypto Part 1 - cw2

1 Overall Context

Your organisation has offices in Warwick out of which work a team of around 200 mobile users. As part of their day to day commercial activity, these mobile users connect their Linux laptops to arbitrary hotel access points whilst out and about on the road. Currently, there is no systematic protection of communication between Warwick and the mobile users. The organisation has all its online assets within the domain:
`<team-name>.cyber.test`. For the purpose of this assignment, you must substitute your specific team's name in place of *<team-name>*.

In Warwick, your organisation uses the private IP address range `192.168.87.0/24` internally with a public IP address range of `213.1.133.98/27` to `213.1.133.126/27` with the default gateway at the ISP of `213.1.133.97`.

Two new VPN gateways are planned for `gw1.<team-name>.cyber.test` at `213.1.133.98` and `gw2.<team-name>.cyber.test at 213.1.133.99.` gw1… is to be a WireGuard realisation of an IPSec gateway. gw2... is to be a StrongSwan gateway.

A new Apache web server for the organisation is planned for `www.<team-name>.cyber.test` at `213.1.133.100`. In the fullness of time, this will go behind a DNATed firewall in a DMZ but for now, it will be placed directly on the public Internet. For the purposes of phase 1 and phase 2 of this assignment, do not concern yourself with the naïve stupidity of this poor security architecture.

2 Your overall tasks

1. Notify the tutor of your team's membership. The tutor will notify you of your team's name.
2. Implementing an internal x509 certificate authority hierarchy that suits the organisation's needs.
3. Protect traffic leaving one group of mobile users' devices via a VPN into your Warwick office over WireGuard to gw1.
4. Protect traffic leaving a second group of mobile users' devices via a VPN into your Warwick office over IPsec to gw2.
5. Protecting transactions with the Apache web server via HTTPS.
6. Generating (individual) GPG keys with which to sign your work and decrypt confidential material for your eyes only.

3 Your specific tasks

1. Adapt the VPN netkit laboratory, used during the teaching sessions to represent your organisation on the Internet.
2. Instantiate the x509 certificate authority hierarchy.
3. Configure the necessary components to achieve what you consider the most appropriate VPN implementations.
4. Evaluate your VPN configurations against each other.
5. Configure the necessary components to achieve what you consider the most appropriate HTTPS server configuration.
6. Provide assurance that the various configurations work correctly.
7. Use your personal GPG keys appropriately.

4 Assessment (35% weighting)

The assessment will comprise two parts :

- conventional submitted material via tabula.
- a short demo / viva where you will be asked to demonstrate some of the claims made in the conventional submitted material.

Note that cw3 (5%) is related to the individual GPG keys that you submit for this coursework

5 Deliverables

Your submission will comprise the following six files, submitted via Tabula. Be careful to satisfy the **specific case-sensitive naming constraints** placed on them

5.1 Report

A succinct report in pdf format named `iss-cw2.pdf`
The report is to have five sections corresponding with Phase 1, Phase 2, and Phase 3 (see marking scheme below), Evaluation, and References In each of the sections for Phases 1, 2, & 3, you are advised to tabulate:

- the significant design, implementation / configuration decisions that you made (your claims) ranked in order of significance,
- the team-member(s) primarily responsible for each claim,

- the evidence that exists to support your claims. This typically would be of the form File xxx : Lines-nnn-mmm or pcap ppp : frames fff-ggg
- the further work that is needed but that you were unable to realise.

The Evaluation section relates to the evaluation between IPSec and WireGuard and forms part of the Phase 3 marking.

The References section should contain full Harvard Bibliographic references to any source material that you have used to inform your submission. You should cite inline references in comments in your config files, just above the configuration lines that they influence.

5.2 Netkit Implementation

A netkit implementation file named `iss-cw2.tar.gz` which:

- was created using `tar -cvzf iss-cw2.tar.gz iss-cw2/` (where `iss-cw2/` is the directory you have used for your development)
- contains the configuration files for the netkit-ng prototype (`lab.conf, xyz.startup, xyz/etc/important-config-file` etc) to start automatically via `lstart`.
- does **not** contain the virtual disk files (`xyz.disk` etc - they are too big),
- contains a script which articulates precisely how the x509 components were created.
- contains any essential additional files that you refer to in your report which demonstrate the robustness of your implementation such as pcap files. Make these as small as possible to demonstrate whatever point you are making. Use a clear naming convention.

5.3 File of Hashes

- A file (named `iss-cw2-hashes.sha256`) that contains the sha256 hashes of the individual files contained within `iss-cw2.tar.gz`. This will be sampled at the demo to confirm no significant changes have been made between the submission and the demo / viva. One way to generate these hashes is via

```
find ./iss-cw2 -type f -print0 | xargs -0 sha256sum | tee iss-cw2-hashes.sha256
```

5.4 GPG public key

Your ascii-armoured GPG public key. Name this file `cyber.pub.key.asc` This public key will be used:

- to verify the detached signatures mentioned below.
- for you to undertake your challenge / response of cw3.

5.5 Digital signature of the pdf

- Detached, ascii-armoured, digital signature of the submitted pdf, signed with your private key. Name this file `iss-cw2.pdf.sig.asc`

5.6 Digital signature of the tar.gz

- Detached, ascii-armoured, digital signature of the submitted targz, signed with your private key. Name this file `iss-cw2.tar.gz.sig.asc`

6 Marking scheme

6.1 Phase 1:

To achieve a mark up to 50% you must:

1. satisfy all the file name and content requirements of all the deliverables.
2. define and implement a credible x509 certificate hierarchy for the organisation, consistent with the script of instructions used to achieve this,
3. submit a GPG public key that is consistent with your University of Warwick email and valid until at least September 2025,
4. provide the correct GPG fingerprint of your public key on the front cover of your pdf submission,
5. have digital signatures that successfully verify the submitted pdf and targz against your supplied public key,
6. achieve VPN connectivity for at least two sample mobile workers over WireGuard.
7. have evidence that the VPN functions correctly,
8. correctly use allocated IP addresses and domain names,
9. have hashes at the demonstration that match the hashes in the submission `iss-cw2-hashes.sha256` file (ie provide evidence that nothing significant has changed between the submission and the demonstration).

6.2 Phase 2

Once you have satisfied all the requirements of Phase 1, you can achieve a mark of up to 70%, by additionally satisfying the following:

10. implement several sample mobile workers with successful VPN connectivity to both gateways
11. make a compelling case for your scalable design and implementation of both VPNs using the x509 certificate authority hierarchy as appropriate,
12. implement a robust HTTPS configuration of the Apache web-server,
13. make a compelling case for your HTTPS implementation,
14. have your submitted public key signed by at least three other students' submitted public keys.
15. have correctly used the private key associated with your submitted public key to sign the submitted public keys of at least three other students in the class,
16. have clean, well organised, well commented configuration files throughout,

6.3 Phase 3

Once you have satisfied all the requirements of Phase 2, you can achieve a mark of up to 100%, by additionally satisfying the following:

17. Make a compelling evaluation of your VPN configurations against each other.
18. implement a robust and compelling DNSSEC configuration,
19. have robust configuration throughout,
20. make thoughtful use of sub-keys, key size and key validity periods in your submission.
21. have your signed public key, available on as many of the following keyservers as are functional just prior to the submission deadline:
    1. `hkp://keyserver.ubuntu.com`
    2. `hkp://keyserver.2ndquadrant.com`
22. demonstrate comprehensive mastery of all aspects of the the submission at all scales (detail through to overall concept). This should be reinforced by at least one additional crypto related features of your choice.

6.4 Cw3 (advanced warning)

The mark for cw3 will be derived from your continued possession of the private key for your personal public key that you submit as part of this cw2 assignment. Cw3 will require you to:

- decrypt an email, sent to your University of Warwick email account, encrypted with your public encryption key, consistent with the identity of your University of Warwick email account.
- act on the instruction contained in the message,
- submit a response, signed by you and encrypted for the specific recipients:

7 Important Constraints

a) This is an assignment that should be carried out in twos/threes of your own choosing. The same criteria will be used whatever the group size.

b) The two common deliverables (the netkit implementation tar.gz file, and the file of hashes) should be identical for all team members. The pdf report should be identical in all aspects except the for the coversheet. The coversheet should have the partner(s) IDs differently organised and a different public key fingerprint. The public key and digital signature components of the submission must be individual.

c) All activity must be conducted legally and ethically.

d) All source material must be referenced using the Harvard referencing convention. Use comments in config files to reference sources in References section of the report.

e) In order to achieve a given mark, there must be consistency between the claims made in the submission and evidence at the demo/viva. Evidence at the demo / viva is fundamentally of two types: firstly technical evidence via the execution of commands, observation of outputs etc in the Netkit realisation of of the infrastructure; secondly intellectual ownership evidence through familiarity with all aspects of the submission.

f) Changes in hashes discovered at the viva will be penalised to a maximum equivalent of a 10 day late submission penalty.

g) The demo / vivas are **provisionally scheduled to take place in late February / early March 2023.** The detailed demo / viva schedule will be published on Moodle for the module.

h) The demo / vivas will predominantly take during timetabled lab sessions over MSTeams. They will be recorded.

i) Your submission will comprise six separate files, submitted via tabula.

j) **Failure to attend the viva will result in a mark of zero**.

k) At the demo / viva, all team members must be fully familiar with all aspects of the submission that represent any change from the original starter pack. Evidence at the viva of lack of familiarity may be reported as possible academic misconduct. **Be sure you re-familiarise yourself with your submission shortly before your viva**.

l) Exceptionally brilliant submissions may exceed the stated mark band for each phase.

m) The default assumption is that all members of the team contributed equitably to the assignment. Where there is clear evidence at the viva that it would be grossly unfair to allocate the same mark for the shared aspect of the submission, then exceptionally, individual marks will be allocated.

n) The file naming and GPG key submission aspects are individual. Where individuals within the team differently satisfy the file naming and GPG submission requirements, then team members potentially fall into different mark bands.

o) If you submit your files before the submission deadline, and prior to the submission deadline, you decide to change one of your submitted files, you must upload all six files again. Tabula will regard this as a new submission and remove everything from the previous submission.

8 Submission Deadline

There will be two deadlines associated with this assignment. The conventional Tabula submission and the viva. The mark for the assignment will be supplied within 20 days of the final viva. The recording of the viva represents part of the feedback for the assignment.

8.1 Initial file submission

Files associated with the main part of the submission are to be submitted to Tabula by **12:00 noon 16th February 2023**.

8.2 Viva schedule

This will be notified via Moodle nearer the time.

9 Late Submission Penalties

Work that is received on Tabula after the submission time (UK time), will be recorded as having arrived the next working day.

Work that is not submitted on Tabula by the deadline will be considered late. Penalties for lateness are applied at the rate of 5 percentage points per university working day after the due date, up to a maximum of 10 university working days late. After this period, the work will be counted as a non-submission.

10 Learning outcomes

The following module learning outcomes are addressed by this coursework:

1. Reason about the relationship between human trust and the technological tokens that represent trust in cyber systems.
2. Design a security architecture that satisfies the security needs of a given scenario.
3. Configure systems, applying cryptographic techniques as needed, to achieve desired security objectives.

11 Submission Coversheet

Your submission coversheet on the pdf should have the following fields:

MODULE TITLE: Implementing Secure Systems

MODULE CODE: WM242-24 (cw2)

TEAM NAME: *<team-name>*

ID NUMBER: *<your-id>*

PARTNER ID NUMBER(S): *<p-id1>, <p-id2>*

YOUR GPG Fingerprint:

xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx xxxx