ICP-3011 Computer & Network Security

Reflect And Relate

Max Petts - *eeub35*

17 - **04.10.2020**

Week 1 - SSH Remote Access

Concept learnt:

- Authentication

In order to permit or deny access to the rightly entitled resources, the security system must be able to differentiate between users; this is identification. When discussing authentication the user being identified is called the Principal. Authentication is the act of validating the claimed identity, and so contains two parts: identification and verification.

Authentication is apparent in many day to day tasks for example, when you get tested for Covid-19 the nurses will ask you to recite your name and address, as to verify you're the person you claim to be. Your name and address is called a credential and is used to verify the principal being claimed is entitled to. Without this step Principal may get their test back positive, when it is actually negative, or vice versa. Some methods of authorization are less user friendly and become laborious, but these credentials are the most secure, as they are harder to brute force due to them using something the principal owns, or the principal themselves (retina scans).

I use git to track changes to my projects which authenticates the user with a public key, instead of inputting my username and password, before any changes can be pushed to the repository; if this repo contained sensitive information then the key should use ECDSA, as RSA is vulnerable to timing attacks[1].

Week 2 - GPG - GNU Privacy Guard

Concept learnt:

- The CIA (Confidentiality Integrity Availability) Triad

The CIA triad is described by f5.com as "so foundational to information security that anytime data is leaked ... you can be certain that one or more of these principles has been violated."[2]. The center point of this model is the data being stored, whereas other models focus on Identity and Access Management(IAM), permissions management and data classification. A multitude of security models should be used so defence in depth can be achieved, instead of just the CIA triad.

Confidentiality ensures that data "is not made available or disclosed to unauthorized individuals, entities, or processes."[3]. An example of a breach in confidentiality, that has happened to me, would be a new employee using a current employees login to do their training and viewing a confidential file already open.

Integrity is defined in the oxford dictionary as "the state of being whole and not divided"[4], but in the InfoSec(Information Security) realm it refers to the reliability, authenticity and correctness of the stored data. The Principal is usually the one responsible with keeping all information up to date. This relates to the new GDPR regulations, "Article 5(1)(f) of the GDPR concerns the ‘integrity and confidentiality’ of personal data"[5]. The CIA triad is also heavily referenced throughout the document, affirming its importance.

Availability mostly refers to the hardware aspects of security systems, as ensuring the system remains powered on and connected to the internet is vital, no matter the literal application. A few examples of breaches in availability are: power outages and DDoS(Distributed Denial of Service) attacks. Power outages may be circumvented through the use of a UPS(Uninterruptible Power Supplies), whereas preventing DDoS attacks are harder than buying a new piece of equipment.

Without can't gaurantee secure transfer of information at all. Encryption ensures that transmitted data remains private

Week 3 - E-Mail Spoofing

Concepts learnt:

- Security from the start Building on top of previous security layers means nothing if not secure.

Week 4 - 'Real World' Cracking

Concepts learnt:

- Validation "Trust is the root of all compromise"

References

[1] http://crypto.stanford.edu/~dabo/papers/ssl-timing.pdf

[2] https://www.f5.com/labs/articles/education/what-is-the-cia-triad#content

[3] https://books.google.co.uk/books?id=DvdICAAAQBAJ&lpg=PA100&pg=PA100#v=onepage&q&f=false

[4] https://www.oxfordlearnersdictionaries.com/definition/english/integrity?q=integrity#integrity_sng_2

[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf