Ning

Computer Security

18 September 2019

Class Summary

[OPENING]: The class is about the general overview of computer systems security, touching up on the subjects of encryption as it relates to computer security.

[INFO]: Professor Eduardo Solana ([eduardo.solana@unige.ch](mailto:eduardo.solana@unige.ch)), TAs: Joakim Tutt and Alexandre-Quentin Berger ([joakim.tutt@unige.ch](mailto:joakim.tutt@unige.ch), [alexandre-quentin.berger@unige.ch](mailto:alexandre-quentin.berger@unige.ch))

[GRADING]: There will be three (3) mandatory TPs, and you must submit two (2) of them in order to qualify for the exam. The exam will be an oral exam, and will encompass five (5) out of the six (6) points. You must also make a presentation on an approved topic (in a team), and attend others presentations and be responsible for learning the material that the other teams present, as they will appear on a specific section of the exam.

[SUMMARY]: The three pillars of security: Confidentiality, Integrity, Availability. Professor Solana considers availability to be the weakest link in computer security in the meta, since the infrastructure is just not there for the majority of the world (bar four or five big companies like Amazon, Google, Apple, Microsoft, etc.) Internet authentication is a topic that is relevant today, the EU passed an internet authentication bill on the 14th of September, and that new regulation will be rolling out. It involves two-factor authentication, and the attempt to make it the standard, since the idea is that a password and a piece of data is insufficient to provide enough security. Internet of Things allows for new avenues of attacks, Professor Solana gave an example of a casino in Vegas being breached via the thermometer in a fish tank being exploited, as it was connected to the internet network. A digest is the output from a hash function. A standard digest size is 256 bits. A hash function is insufficient itself to provide integrity, you need to also preserve the integrity of the digest (an example was to post the digest publicly). In hashes, collisions for SHA256 theoretically exist, but you can’t calculate them since it is too big (it is 2256, and even SHA1 is 280). However, in the case of SHA1, someone found a way to compute collisions in less than 280, which is why we don’t really use SHA1 commercially anymore.