6.033 Lecture 23
Security IV

Americo De Filippo

July 12, 2023

References

[1] Saltzer, Jerome H. and M. Frans Kaashoek. Principles of Computer System Design: An Introduction (2009): **Section: 11.4 - .6**

In this lecture we are gonna wrap up our discussion about security, and indeed this will be the last lecture of this course. The last time we talked about building a secure comm channel throught authorization, that will be handle in 2 ways: or ACLs or Tickets.

1 Athentication Protocol

From the last example where B send some request to W trought a secure communication channel. The thing that we are gonna focus on is: how is gonna know B that he has the right public key or W, and no one is impersonating W. We (as usual) are gonna use a certificate authority, that is gonna tell to B is that is the right key of W. Now is the question is: How B is gonna trust the cetificate authority, how is gonna enstablish the communication with it?

1.1 Authentication Logic (BAN logic)

What BAN is gonna do is basically give us reasons to trust some certificate authority. One thing to do this is by a "web of trust", let's say that we trust B then we are gonna ask B is he knows some people that he trustes that can verify that a private key of A is actually what is saying to be.

Make Assumptions Explicit

- Assume signature is not forgeable
- Assuming private keys are actually private

This assumptions are usen when for example, we call sign(m, k_A), I infer from this that A says m, also I'm assuming that the private key of A is actually private.

Establishing initial trust

- The way of doing this is by the previus metioned method (web of trust).
- Does W know/trust P?
  How does it decide? Usually for some data that is good. Like for amazon.com could be the credit card company gives some kind of allowence to trust the user.
- How does P trust W? Usually on the internet is via a certificate authority, from this arise issues. Like to know how do i trust the certificate authority? On the internet usually or you allow to the system a specific list of an exernal certificate authority. Or in most of the case an operating system comes out with a default list of certificate that the machine trusts. Also when you install a browser it will come out with a list of certificate authority that it trust.