6.033 Lecture 22
Security III

Americo De Filippo

July 11, 2023

References

[1] Saltzer, Jerome H. and M. Frans Kaashoek. Principles of Computer System Design: An Introduction (2009): **Section: 11.5**

Today we are going to talk of authorization and confidentiality. The cyptographic primitives that we are gonna use are: Sing, Verifiy.
sign(m, k) = sig.
verify(m, sig, k_2) = outputs if m corrispondes to that signature
We also talked about Encrypt and Decrypt.
enc(m, k_1) = c
dec(c, k_2) = m

1 Secure Communication Channel

- use pub key to exchange a shared key
- use shared key to enc. comm

2 Confidentiality

Is the protection of information exchenge between Alice and Bob, the idea is that Alice create some message encypt it, and send it over ethe internet, and arrives to Bob that will decrypt it with its key. The proprieties is that the people into the internet cannot read the message.

2.1 + Authentication

The way that we do this is via sign a message, encypt it, and add some kind of key.

3 Authentication

Let's say that we have some browser B communicate to a Web server W through a secure communication channel (SSL: secure socket layer), the channel has been authenticate from a CA (certificate authority). How does W know that B is authorized to access W? The issue is that once the protocol is enstablished they can communicate with each other, so B as to have some kind of protocol for knowing which information is B authorized to access. This will be done in 3 steps.

1. Rendezvous (setup, logging in)
2. Verification (mediate, allowing to log)
3. Revoke

There are 2 windely used approches: Lists and Tickets

Steps	Lists	Tickets
Set up	add to list	generate ticket
Mediate	search list, check credentials	table lookup
Revoke	remove from list	invalidate ticket