CS2107 Live Class Lec2

$_/|/|U_Ch@NgRu!$

May 11, 2021

1 Authentication

1.1 Definition

Authentication is the procerss of assuring tha t the communication entity, or origin of a piece of information, is the one that it claims to be

2 Password

In any password system, there are two stages

1. BootstrappingL server anduser establish a common password. Server keeps a file recoing the identity and password
   This is done by
   (a) Server.user chooses a password and sends it to the user/server throught another communication channel
   (b) Defaust password
2. Authentication: server authenticates and entity by asking the entity to give the correct password corresponding to the claimed identity, the entity eill deemed authentic. This can be done either with or without interaction

The way how the server and the client transport the password also matters, and there are two types:

1. weak authenticaiton: the user and server send the password to each other in plaintext; If eavesdropper sniff the password, he can impersonate one party with the password
2. Strong authentication: the user and server send the encrypted password to each other, where even if eavesdropper sniff the transportes contends, he cannot know the contends of

the password

2.1 Attacks on Password System

Password system may be compromised via

1. Attack on bootstrapping: Password can be intercepted during bootstrapping(eavesdropper for even Mallory)
2. Searching for password
   (a) Guessing password from social information
   (b) Dictionary attacks
   (c) Stealing password: shoulder surfing, sniffing, viruses, keylogger, login spoofing, phishing, spear phishing, etc.
   (d) Cache of shared workstation
   (e) insider attack

2.2 Preventive measures to protect the password system

1. Use strong password that is either random ,mix of special characters
2. Password policies, which presents weak passwords during bootstrapping and prevents dictionary attack.guessing by locking account after some failed attempts
3. Layered protection on password files through hashing(What stores in password files are layered hashed password)

2.3 Security Questions

Security question is viewed as mechanism for fallback authentication. or a self-services password reset
Choice of security questions need to be memorable, consistent, nearly universal(applied to everyone) and safe(no one else knows)

2.4 Biometric

Biometric uses unique physical characteristics of a person for authentication. It consists of two stages

1. Enrollment: During enrollment, a template of an user's biometric data is captured and stored

2. VerificationL during verification, biometric data of the person-in-question is captured and compared with the template using a matching algorithm. TH algorithm decides whether to accept or reject, there are two important factors:

   (a) False Match Rate, FMR=$\frac{number\,of\,successful\,false\,match}{number\,of\,attemted\,false\,matches}$

   (b) False Non Match Rate, FMR=$\frac{number\,of\,rejected\,genuine\,match}{number\,of\,attemted\,genuine\,matches}$

   The matching algorithm typically makes decision based on some adjustable threshold. Usually, there is a tradeoff between FMR and FNMR
   Some other rate:

   (a) Equal error rate: the thresshold when FMR=FNMR

   (b) False-to-enroll rate: Some users' biometric data cannot be captured during enrolment

   (c) Failure-to-capture rate: Biometric data may fail to be captured during authentication

   Biometric system is secure is the scanner and the communication channel to matching algorithm is secure. Additonal protection may include liveness detection(Avoid a picture to open a face ID)

3 n-factor authentication

n-factor authentication requires at least two different authentication factors

1. who u are: biometric
2. what u have: security token, mobile phone
3. Something u know(password,security question)

4 One time password token

One time password token is a hardware that generates one time password. Each token and the server share some secrete keys used to generate the OTP by

1. either time-based: based on the shared secret and current time interval, a password K is generated which is know to both serve and the user
2. Sequence-based: an event triggers the chang eof the password