CS431

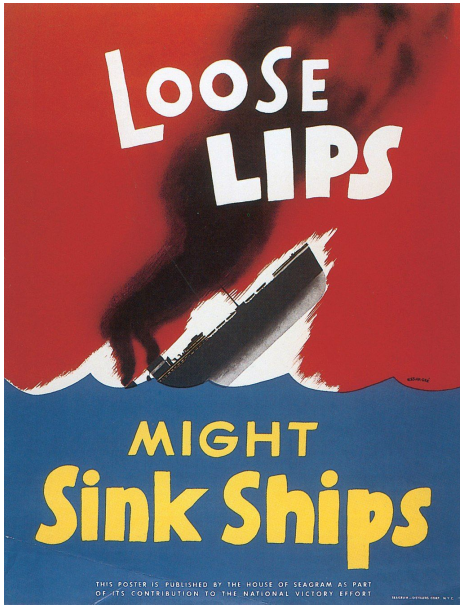
Computer and Network Security

Basic Security Properties

Abhishek Bichhawat

16/01/2024

Confidentiality, Privacy and Secrecy



- Keeping information secret from those not authorized to see it

- Confidentiality : obligation to preserve someone else's information secret
  - Bank ensures confidentiality of Alice's CC no.
- Privacy : keeping personal information secret
  - Alice protects her privacy by not revealing her age to anyone
- Secrecy : hiding information from *certain* individuals or groups

Integrity

- Ensuring that information has not been altered by unauthorized or unknown means
  - using a secure physical channel that prevents adversaries from changing the contents of the messages they exchange
  - bit-parity checking after downloading a file from the server to ensure the integrity of the downloaded file, i.e., that the contents are correct

Authentication

- Corroboration of the identity of an entity
  - Aadhaar identifies you as yourself at various places
  - By logging in using your login ID and password, you can identify yourself to various online systems.
  - Also “identification” or “entity authentication”

Authentication

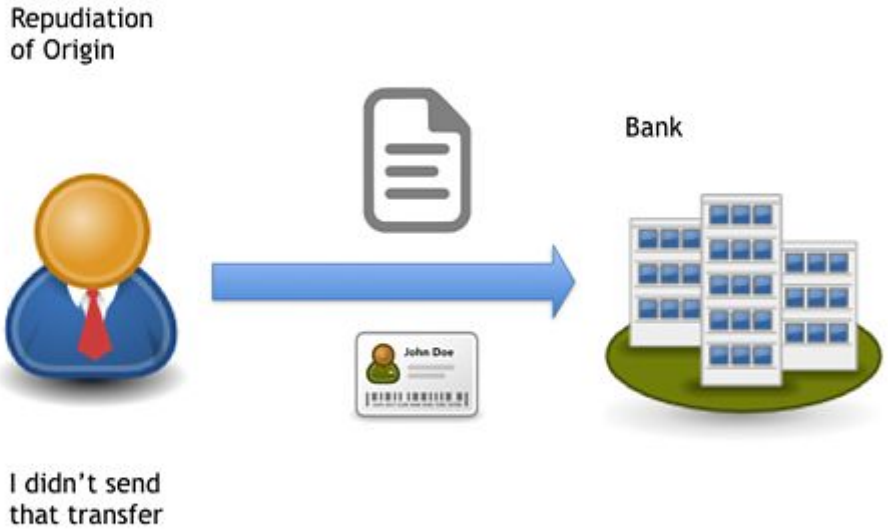
- Corroboration of the identity of an entity
  - Aadhaar identifies you as yourself at various places
  - By logging in using your login ID and password, you can identify yourself to various online systems.
  - Also “identification” or “entity authentication”
- Corroborating the source of information
  - Also known as “data origin authentication”
  - Authenticating that a cheque is received from the right source by checking signature

Anonymity

- Concealing identity of a participant

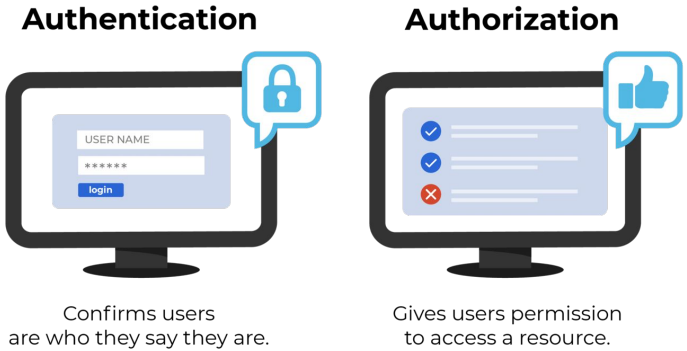
Non-repudiation

- Non-repudiation
  - Assurance that someone cannot deny something
  - In the context of security, it often involves digital signature



Authorization, Access-control, Certification and Revocation

- Authorization
  - official sanction to do something or be someone
- Access control
  - Restricting access to resources to privileged entities
- Certification
  - Endorsement of information by a trusted entity
- Revocation
  - Retraction of certification or authorization



Availability

- Services/resources are available to rightful entities
  - You can access the internet once you pay Airtel/Jio
  - Bank customers can do online banking 24x7

What Goes Wrong!

What Goes Wrong – The Policy

- Some airlines allowed business-class tickets to be changed at any time, no fees.
  - Is this a good policy?

What Goes Wrong – The Policy

- Some airlines allowed business-class tickets to be changed at any time, no fees.
  - Is this a good policy?
  - What if, in some systems, ticket could have been changed even AFTER boarding!
    - Adversary can keep boarding plane, changing ticket to next flight …

What Goes Wrong – The Policy

- Detailed Institute Policy:
  - Student can access only his/her own files in the system.
  - Admin has access to everyone's files.
  - Teachers can add new students to their class.
  - Teachers can change password of students in their class.
- It went wrong when a student got hold of a teacher’s password!
  - What can go wrong?

What Goes Wrong – The Policy

- Detailed Institute Policy:
  - Student can access only his/her own files in the system.
  - Admin has access to everyone's files.
  - Teachers can add new students to their class.
  - Teachers can change password of students in their class.
- It went wrong when a student got hold of a teacher’s password!
  - What can go wrong?
  - Student can become teacher and then add Admin as student, change the password, access all files!

What Goes Wrong – The Policy

- Someone wanted to break into the gmail account of Honan, an editor at wired.com:
- Gmail password reset: send a verification link to a backup email address.
  - Google helpfully prints part of the backup email address.
  - Mat Honan's backup address was his Apple @me.com account.
- Apple password reset: need billing address, last 4 digits of credit card.
  - Address is easy, but how to get the 4 digits?
  - Let’s check Amazon for his credit card number
- Amazon requires username/password to get access to account. However, …

What Goes Wrong – The Policy

- Add a credit card to an Amazon account.
  - No authentication required,
    presumably because this didn't seem like a sensitive operation.
- Call Amazon tech support again, and ask to change the email address on an account.
  - Authentication required!
  - Tech support accepts the full number of any credit card registered with the account.
  - Can use the credit card just added to the account.
- Now go to Amazon's web site and request a password reset.
  - Reset link sent to the new e-mail address.
  - Now log in to Amazon account, view saved credit cards.
  - Amazon doesn't show full number, but DOES show last 4 digits of all cards.
    Including the account owner's original cards!
- Now attacker can reset Apple password, read gmail reset e-mail, reset gmail password.

What Goes Wrong – Attack Assumption

- Assuming a particular kind of a solution to the problem
  - use CAPTCHAs to check if a human is registering for an account
  - to prevent mass registration of accounts to limit spam

What Goes Wrong – Attack Assumption

- Assuming a particular kind of a solution to the problem
  - use CAPTCHAs to check if a human is registering for an account
  - to prevent mass registration of accounts to limit spam
- Adversaries found another way to solve the same problem
  - Human CAPTCHA solvers in third-world countries.
  - Human solvers are far better at solving CAPTCHAs than even regular users.
  - Cost is very low (fraction of a cent per CAPTCHA solved)

What Goes Wrong – Attack Assumption

- Assuming your hardware is trustworthy
  - If ~~the government~~ someone with access to the hardware is adversary, it breaks the security
  - See *Clipper chips* (https://en.wikipedia.org/wiki/Clipper_chip)

What Goes Wrong – Attack Assumption

- Assuming the system is secure
  - Long back, DES was a secure encryption algorithm
    - In late 90s, it became easy to break it (within a day!)
  - People study quantum crypto for a reason!

What Goes Wrong – Attack Assumption

- Machines not on internet are secure?

What Goes Wrong – Attack Assumption

- Machines not on internet are secure?
  - Easy to spread viruses using USB sticks
  - Stuxnet worm (2010) spread that way!
    - May have damaged Iran's nuclear program

What Goes Wrong – Bugs

- Bugs/missing checks are reportedly one of the top 5 security issues
- Apple's iCloud password-guessing rate limits
  - Users have often used weak passwords
  - rate-limit login attempts (e.g., 3 attempts)
  - Implemented in photo-sharing, file-sharing, email-sharing services
  - But, missed implementing in “Find my iPhone” service

What Goes Wrong – Bugs

- Bugs/missing checks are reportedly one of the top 5 security issues
- Missing access control checks in Citigroup's credit card website
  - Citigroup allowed credit card users to access their accounts online.
  - Login page asks for username and password.
  - If username and password OK, redirected to account info page.
  - The URL of the account info page included some numbers.
    - e.g. x.citi.com/id=1234
    - id related to the user's account number
  - Adversary tried different numbers, got different people's account info.
    - The server didn't check that you were logged into that account!