Core notes

Jonathan Lam

09/22/2021

Contents

1 Why systems fail:

- **Relability**: accidental failures
- **Usability**: user/operational failures

- **Security**: intentional failures by an intelligent adversary

2 Security goals

- **Confidentiality**: concealment of information (from eavesdropping/copying by others)
- **Integrity**: prevention of unauthorized changes (from tampering)
- **Authenticity**: knowing who you're talking to (from assuming soneone else's identity)
- **Availability**: ability to use information or resources (from DOS, infrastructure disruption)

3 Threat models

- **Assets**: who are we protecting, and how important is this stuff?
- **Adversaries**: who is attacking, and why?
- **Vulnerabilities**: how might the system be weak? (technical details)
- **Threats**: what actions would an adversary take? (actions that are taken to attack the system)
- **Risk**: how important are the assets? How likely is the exploit? Economic incentives? (probability and reasons)
- **Defenses**: what can we do to prevent/detect/respond to attacks

4 Approaches to security

- **Prevention**
- **Detection**
- **Response**

5 Considerations for secure systems

- **Weakest link / defense in depth / asymmetry advantage**
- Security policy considerations
  - Requirement bugs (goals)
  - Design bugs (wrong use of security features, e.g., cryptography or randomization)
  - Implementation bugs
  - Usability bugs
- Ecosystem of participants: many participants (including adversaries) with different goals

6 Security goals for identification/authentication

- **Accountability**: ability to identify and authenticate users and audit actions
- **Non-repudiation**: unforgeable evidence that a specific action has occurred

7 How to prove who you are

(These are the "F" in "MFA".)

- **What you know** (passwords, answers to questions only you know)
- **Where you are** (IP address, geolocation)
- **What you are** (biometrics)
- **What you have** (secure tokens, mobile devices)

8 List of password issues

- **Credential stuffing**: credentials from other sites
- **No rate limiting**
- **No MFA**

- **Weak password recovery**
- **Application timeouts too long**
- **Keystroke loggers**
- **Shoulder surfing**
- **Broken implementations**: e.g., timing attack
- **Usability**: hard-to-remember passwords, or carry physical object
- **DOS**: account locked after multiple uses
- **Social engineering**

9 Problems with linked accounts

- Different companies may have incompatible security policies
  - Security has to be considered as part of the greater ecosystem
  - Systems that are secure on their own may not be secure when used with other systems
- MFA should stop these attacks
- Back up devices; can easily run your own backup on a separate device
- Easy to do: we hand out personal information (e.g., credit card information) all the time

10 Attempts at improving passwords

- **Biometrics**: e.g., voice, key/mouse dynamics; private, but not secret; shared between systems; impossible revocation, physically identifying
- **Graphical passwords**: easier to remember? (But also predictable?)
- **Password managers**: can still have security vulnerabilities; generate secure passwords and don't have to remember them; autofill
- **MFA/2FA**
- **Mutual authentication**: prevents phishing

- **Trusted path**: e.g., Ctrl+Alt+Delete
- **Display number of failed attempts**: prevents some MITM attacks
- **Timeouts and limits**: prevents online guessing

11 Access control

- Teminology:
  - **Policy**: specifies who can do what
  - **Principal**: entity requesting access
  - **Object**: resource that is being requested
  - **Reference monitor**: manages authentication and authorization of users
  - **User identity**: authenticated user
  - **Process**: the thing that communicates with the reference monitor directly on behalf of the user identity
  - **Subject**: the thing that actively communicates with the reference monitor
  - Difference between principal and subject is not really meaningful; in this case it is also the process (thing making the request)
  - **Access right** or **permission**: right to perform an access or operation
  - **Privilege**: set of privileges given directly to roles
  - **Access mode**: two access modes: observe or alter an object
  - **Bell-LaPadula model**: four access rights: execute, read (observe), append (alter), write (observe, alter)
  - **Access rights (Unix)**: r/w/x
  - **Authorization** (alternate definition): process of setting policies
  - **Access control structure**: format/organization of a policy
  - **Access control matrix**: specifies for each subject and object the set of permissions
  - **Capabilities**: for each subject, list the objects and their permissions

- **Access control lists** (ACLs): for each object, list the subjects and their permissions (Unix method)
- **Discretionary vs. system-wide (mandatory) policy** (DAC vs. MAC): discretionary is set by file owner, mandatory is set by a system policy
- **Groups**: group multiple identities to have the same permissions
- **Role**: a collection of procedures ("high level access controls", with hierarchies) assigned to users
- **Intermediate controls**: better security management with more layers of indirection
- **Protection rings**: mostly for integrity protection
- **Lattice**: a hierarchical graph structure

12 Todo Items

- TODO: set up OH with Gitzel: talk about authentication/non-repudiation; understanding of the exchange in the key FOBs, nonces, MACs, CRCs, Yubikeys, etc.,
- Difference between authentication and non-repudation?
- Difference between principal, subject, and process?
- Difference between groups and roles