Learning Objectives

- Define the common authentication methods
- Identify authentication vulnerabilities
- Enumerate common types of attacks on authentication
- A quick look at social engineering
- Meet a couple of secure protocols

The Gold Standard

- **Authentication**
  - The process of verifying, with some degree of certainty, that a principal (user, computer, program) is who or what it claims to be
- **Authorization**
  - The process of determining whether an authenticated principal may access a requested resource.
- **Audit**
  - Provision of a chronological record of events that support the concept of accountability

Authentication Strategies

- **Reusable passwords**
  - Based on something you know
  - Easy to use
    - Comes with the platform
  - Cheap solution
    - No additional hardware required
  - Subject to
    - Brute-force attacks
    - Dictionary attacks
    - Replay attacks
Authentication Strategies

- Account lockout
  - Disable the account after M invalid passwords in N minutes
    • Requires administrator action or time delay before login is re-enabled
- Prevents password guessing
- Enables an attack
  - Suppose you want to prevent someone else from authenticating?

Authentication Strategies

- One-Time Passwords
  - Each password is only good once
  - Server maintains a list of valid passwords
    • Client delivers password N
    • Server advances to password N+1
    • Stealing password N won’t help you guess password N+1
    • Effective countermeasure to replay attacks
  - Must be integrated with your platform
    • Client has to maintain the list too
  - Only provides authentication
    • Superseded by ssh

Authentication Strategies

- Multi-factor Authentication
  - Based on:
    • Something you know
    • Something you have
    • Something you are
  - Effective countermeasure to
    • replay attacks
    • dictionary attacks

Authentication Strategies

- Two-Factor Authentication
  - Based on something you know and something you have
    • Know a password (or PIN)
    • Have a one-time password token
  - Example:
Authentication Strategies

- **Biometrics**
  - Measure some physical characteristic
    - Fingerprint, retinal pattern, finger length, ...
  - Usually defeated with non-technical attacks
  - Expensive solution
  - Not reliable
    - False positives - bad guy authenticated
    - False negatives - legitimate user refused
  - Iris scans are best
  - Can be stolen

- **Single signon**
  - Authenticate once, then access multiple arbitrary systems with this set of credentials
  - Authenticate once, then access multiple systems that have been designed to interoperate
  - Example: U-M CoSign environment
  - But those credentials are vulnerable
    - Replay attack

Risks of Biometrics

- **Biometrics**
  - Usually defeated with non-technical attacks
  - Expensive solution
  - Not reliable
    - False positives - bad guy authenticated
    - False negatives - legitimate user refused
  - Iris scans are best
    - Can be stolen

Password Storage

- When you create an account somewhere and set a password, the system should not ever store your plaintext password
- If the system is compromised or the data is lost, the bad guys have your password just by looking at it
- So systems stored hashed passwords

http://en.wikipedia.org/wiki/Password_cracking
Password Hashing

- Your plaintext password is run through a hashing step and the system stores the hashed password
  - When you come back later and present your password it hashes the new password and compares it to the stored hash
  - If they match, you are logged in

```
fluffy → SHA1 → d9d71ab718931a89de1e986bc62f6c988ddc181
kitten → SHA1 → 44060752d7f7ae069c8187120455195325af0cca
```

Hashes

- Hashes are one-way functions
  - Easy to compute a fixed-length hash from a variable-length input text
- A good hash function has two properties
  - Non-invertibility (very hard to compute the input text from the hash)
  - Collision resistance (very hard to find two different input texts with the same hash)
- Popular hash functions include MD5 and SHA-1
  - MD5 is no longer secure; SHA-1 not broken (yet)
  - Use SHA-2 while waiting for SHA-3

Losing Password Hashes

- If a system or data is compromised and reveals the hashed passwords, your password is not immediately available
- But with enough time, they can guess a password, hash it and compare it to your password until they find a match…
- Your choice of password can either make it easy or hard for them to guess your password…

Pass Phrases

- Good pass phrases are long strings
  - Example: “I wish we could use 2Factor authentication instead of passwords”
  - Very strong protection against attacks
  - Easy to remember, a bit longer to type
- Passwords are short complex strings
  - Example: “@Rag0Rnru13z”
  - Hard to remember
  - Often difficult to type
  - Not resistant against current attacks
    - Obvious substitutions are quickly broken
- Summary: Long easily-remembered phrases are better than short complex passwords
Some Common Bad Passwords

http://www.boingboing.net/2009/01/02/top-500-worst-passwo.html

Authentication Vulnerabilities

- All possible passwords can be tried
  - AKA brute-force attack
- Weak passwords can be guessed
  - AKA dictionary attack
- Eavesdropper can record password for later use
  - AKA replay attack

Some types of Attacks

- Active online
- Offline
- Surveillance
- Non-electronic

Active Online Attacks
Replay Attack

- Access and record raw network traffic
- Wait for an authentication sequence
- Record the sequence
- Replay it later

Considerations
- Relatively hard to perpetrate
- Must be trusted by one or both sides
- Tools less widely available
Active Online Attacks
Man-in-the-Middle Attack

- Somehow get access to communications channel
- Wait for an authentication sequence
- Proxy the authentication traffic
- Considerations
  - Relatively hard to perpetrate
  - Must be trusted by one or both sides
  - Tools less widely available

Active Online Attacks
Password guessing

- Try different passwords until one works
- Made easier by
  - Bad passwords
  - Lack of password guessing controls
- Considerations
  - Assuming good passwords, is this even feasible?
    - Complex 8 character password space \(69^8\)
    - Password expires in 90 days
    - Need to guess 66,074,893 pwds/sec
    - Need throughput of 8 Gbps
    - Gigabit Ethernet = 1 Gbps
  - Easily detected and stopped
  - Core problem: Bad passwords

Offline Attacks
Password guessing

- Attacker has database of password hashes
  - Hard to do: Need to be admin or have physical access
- Can attack at leisure – Attack types:
  - Dictionary attack
    - Very Fast
    - Core Problem: Bad Passwords
  - Brute Force attack
    - AlphaNumerics then AlphaNumerics + Upper Row Symbol, etc
    - Slow, but will eventually find all passwords
  - Hybrid
    - Start with Dictionary, add templates (word spelled backwards, etc), then brute force
    - John the Ripper does this
- Considerations
  - Moore’s law

Offline Attacks
Rainbow Tables

- What if you precomputed the password hashes?
  - All Windows LM Hashes: 166 Terabytes
  - All Windows NT Hashes < 15 chars: 140,959,235,198 Exabytes
- This would result in faster cracking, at the cost of storing all those hashes
  - This is the Time-Memory tradeoff
  - Implemented using hash chains
    - Clever way to link the hashes into chains
    - Only store 1 in 10,000 hashes
- Rainbow tables improve on hash chains
  - Reduce collisions (overlapping chains)
- http://ophcrack.sourceforge.net/
Surveillance

- **Shoulder surfing**
  - Watching someone type their password
  - Common and successful

- **Keystroke loggers**
  - Preserve user input for intruder
    - Accounts, passwords, credit card numbers, social security numbers, …
  - Hardware loggers cheap and hard to detect
    - Fit between video port and cable
  - Software loggers cheap and hard to detect
    - Installed by malware
  - Both can be controlled remotely

Example

**The Michigan Daily**

Binge of computer hackings creates fear

BY WONGJONG CHANG

Daily News Editor on 9/14/03

An anonymous Rackham student is more careful now when using public computers and keeps close track of her e-mail account. She said the cause of her new precautions is former Rackham student Xing Ma, who allegedly hacked into her e-mail accounts and personal networks of more than 200 University students and professors.

Ma, who was arrested and arraigned two weeks ago, has been charged by Attorney General Mike Cox on 15 counts involving wiretapping and unauthorized access to computers.

Department of Public Safety spokesperson Diane Brown said that Ma was arraigned on additional charges of extorting and intimidating a police officer on the day of his arrest. She said Ma is still in jail as he has not posted the $200,000 he needs for bail. DPS would not confirm specific charges or Ma’s victims because of the ongoing investigation.

James Biddle, associate professor for academic, information and instructional technology affairs at the community, said he used a keystroke tracking program to build into e-mail accounts and changes personal network storage areas. The technology can detect every word typed, every mouse click, every e-mail sent, etc. and can be purchased by anyone who wants to monitor their personal or other, or in Ma’s case, public computers.

Surveillance

- **Recover input from “hidden” records**
  - Stored files
  - Sticky notes
- **Recover input by monitoring audible keystrokes**
- **Recover displayed or transmitted data by monitoring electromagnetic radiation**
  - TEMPEST
Social Engineering

Tricking people into giving up secrets

- Pretexting
- Phishing

An attack on the “wetware”

Examples

A tale of two studies

- University of Sydney study (1996)
  - 336 CS students were asked to reveal their passwords
    - Pretext: “validate” password after suspected break-in
  - 41% returned their passwords; 9% returned invalid passwords; 60% reset their passwords afterwards

- Stockholm University Study (2008)
  - Researcher asks employees of an IT consulting firm social engineering questions
  - Out of 110 respondents, 73% would send pretexter their time report, 77% would download & install pretexter’s patch, 36% would reveal their passwords