Chapter 2

Knock-Knock, who's there?

Introduction

• Identification and authentication
• Identification failures
• Strong authentication: based on something you know, are, or have (Physiological properties and authentication)
• Relationship between privacy/strong authentication: anonymous access and pseudonyms
• Relationship between usability/strong authentication
Identification & Authentication

Identification
Identification & Authentication

Only 'legally known' people must be allowed to logon to your IT system.

Identify a person as 'legal' and verify that he really is whom he claims to be.
Introducing Alice, Bob, ...

Hi Bob! I'm Alice.

How does Bob know that Alice is really Alice?

... and Mike!

Hi Bob! I'm Alice.

How does Bob know that Mike isn't Alice?
Sending Proof for Authentication

Hi Bob!
I'm Alice.

Hi Alice!

I am Alice!

Alice must send proof that she is who she claims to be.

Authentication mechanisms

• Common authentication options include:
  – User Name and Password
  – Logon Tickets
  – X.509 Certificates
  – PKI
  – One-time passwords
  – Biometrics
  – Multifactor
Authentication and SSO: X.509 Certificates

- X.509 certificates ("digital certificates") can be used both for initial authentication and for successive single sign-on
- Uses Secure Sockets Layer (SSL):
  - Internet standard for secure HTTP connections
  - Provides for server, client or mutual authentication and encryption
  - Uses both symmetric and public-key encryption for protection

Identification & Authentication

- Attack (threat)? Impersonation
- Sidebars 2-1 and 2-2…
Identification & Authentication

• Sidebar 2-1
  – University student hacked email account of politician to derail her election campaign
  – How?
    • He knew her email address through web search
    • Yahoo email address used for work matters
    • He said to Yahoo that he forgot the password
    • Security questions were easy to reveal from web

Identification & Authentication

• Sidebar 2-1
  – Kernell (20), student, was tried for:
    – Unauthorized access to a protected computer
    – Destroying records to impede a federal investigation
    – Wire fraud (Not convicted)
    – Identity theft (Not convicted)
Identification & Authentication

• Sidebar 2-2
  – George Bronk (23) pleaded guilty on charges:
    • Computer intrusion
    • False impersonation
    • Possession of child pornography
  – How?
    • His crimes involved impersonating women with
      data obtained from their Facebook accounts.

Identification & Authentication

• Sidebar 2-2
  – How?
    • Bronk scanned FB pages for women’s email addresses
    • Scanned for clues to help answer security questions
      – such as a favorite color or a father’s middle name
    • Bronk then turned to the email account providers
    • Using the same technique as Kernell, Bronk pretended
      to have forgotten his (her) password
    • Sometimes succeeded at answering the security
      questions necessary to recover a forgotten password
    • Same technique to obtain access to FB accounts.
Identification & Authentication

• Sidebar 2-2
  – How?
    • After he had the women’s passwords, he perused their sent mail folders for embarrassing photographs
    • He sometimes mailed those to a victim’s contacts or posted them on her Facebook page
    • He carried out his activities from Dec 2009 to Oct 2010
    • Police found 3200 Internet contacts and 172 email files containing explicit photographs
    • Police sent mail to all the contacts to ask if they had been victimized, and 46 replied that they had

Identification & Authentication

• Vulnerability?
  – Faulty/weak or incomplete authentication
  – Already mentioned the password issues

• Countermeasures?
  – Strong authentication
Identification & Authentication

• Strong authentication
  – Knowledge: Something You Know
  – Biometrics: Something You Are
  – Tokens: Something You Have
  – Multifactor Authentication
  – Secure Authentication

Identification & Authentication

• Knowledge: Something You Know
  – Passwords
  – Password security:
    • Use characters other than just a–z
    • Choose long passwords
    • Avoid actual names or words
    • Choose an unlikely password
    • Change the password regularly (Not my opinion!)
    • Don’t write it down
    • Don’t tell anyone else
Identification & Authentication

• Password vulnerabilities
  – Loss
    • If the user loses the password, a new one must be assigned – cannot find "lost" one.
  – Use
    • Supplying a password for each access to an object can be inconvenient/time consuming.
  – Disclosure
    • To an unauthorized individual
  – Revocation
    • To revoke access, someone must change password

Identification & Authentication

• 12 steps to hack p/wss (increasing difficulty)
  – no password
  – the same as the user ID
  – is, or is derived from, the user’s name
  – common word list/names/patterns
  – contained in a short college dictionary
  – contained in a complete English word list
  – contained in common non-English language dictionaries
Identification & Authentication

• 12 steps to hack p/w s (increasing difficulty)
  – contained in a short college dictionary with capitalizations (PaSSWoRD) or substitutions (0 for letter O)
  – contained in a complete English dictionary with capitalizations or substitutions
  – contained in common non-English dictionaries with capitalization or substitutions
  – by brute force, trying all possible combinations from a specified character set
  – obtained by brute force, trying all possible combinations from the full character set

FIGURE 2-1 Distribution of Password Types

From Analyzing Computer Security by Charles P. Pfleeger and Shari Lawrence Pfleeger (ISBN: 0132789469) Copyright © 2012 Pearson Education, Inc. All rights reserved.
Identification & Authentication

• Knowledge: Something You Know
  – Sidebar 2-4: Usability in the Small versus Usability in the Large
    • Usability in the small
      – managing one password or token for an application – easy
    • Usability in the large
      – managing many passwords or tokens at once – daunting task
  • Remembering one password VS many
  – Sidebar 2-5: Using Personal Patterns for Auth.
    • GrlDSure
    • ImageShield
Identification & Authentication

• Knowledge: Something You Know
  – Sidebar 2-5: Using Personal Patterns for Auth.
    • ImageShield

One time passwords & Smart cards

• Authentication using a credit card type device that generates a password.
• Password generation software using seed
• Benefits
  – Auto generated passwords means not needing to remember
  – No password maintenance
  – Used in conjunction with authentication and authorisation tools
  – Useless to thieves
• Remote access servers
Identification & Authentication

• Strong authentication
  – Biometrics: Something You Are

Access based on physiology

Biometrics

Characteristics:
- Accuracy
- Speed and Throughput
- Reliability
- Data Storage & Processing
- Enrollment Procedures
- Uniqueness
- Counterfeiting
- User Acceptance

Combinations provide deeper rigour

Based on what a person is:
- Voice recognition
- Iris Scans
- Fingerprints

Something a user knows
• Has
• is
Identification & Authentication

- Strong authentication
  - Tokens: Something You Have
Identification & Authentication

• Strong authentication
  – Multifactor Authentication
    • Combination of some or all of the above
Identification & Authentication

• Strong authentication
  – Secure Authentication
    • Simply using any or all of the above mechanisms is no guarantee that an authentication approach is secure
    • To achieve true security, we need to think carefully about the problem we are trying to solve and the tools we have
    • We also need to think about blocking possible attacks and attackers
      – Certain access times
      – Access only on certain devices
  • Above might be inconvenient, but security could outweigh

Conclusion

<table>
<thead>
<tr>
<th>Threat</th>
<th>Consequence</th>
<th>Severity</th>
<th>Ease of Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Impersonation</td>
<td>Access by unauthorized party</td>
<td>Extremely high</td>
<td>Easy to moderate</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Exploitability</th>
<th>Prevalence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faulty, weak, or nonexistent authentication</td>
<td>Easy</td>
<td>Frequent</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Countermeasure</th>
<th>Addresses Which Issue</th>
<th>Mitigation Type</th>
<th>Mitigation Effect</th>
<th>Effort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong authentication: knowledge</td>
<td>Faulty, weak, or nonexistent authentication</td>
<td>Preventive</td>
<td>High</td>
<td>Easy</td>
</tr>
<tr>
<td>Strong authentication: biometrics</td>
<td>Faulty, weak, or nonexistent authentication</td>
<td>Preventive</td>
<td>High</td>
<td>Easy</td>
</tr>
<tr>
<td>Strong authentication: token</td>
<td>Faulty, weak, or nonexistent authentication</td>
<td>Preventive</td>
<td>High</td>
<td>Easy</td>
</tr>
</tbody>
</table>
FIGURE 2-7 Threat–Vulnerability–Countermeasure Analysis