Lecture 3 - Passwords and Authentication

CSE497b - Spring 2007
Introduction Computer and Network Security
Professor Jaeger
www.cse.psu.edu/~tjaeger/cse497b-s06/
What is authentication?

• Reliably verifying the identity of someone
• **Q**: How do you do this in practice today?
• **A**: A human scale protocol?

1. A and B ask for credentials (implicitly or explicitly)
2. B provides credential to A who verifies it
3. A provides credential to B who verifies it

• Both parties are authenticated: mutual authentication
• The question is, what credentials do you use?
  – The answer is *context specific*, where the kinds of credentials and the level of *due diligence* is related to the tasks for which the entity is being authenticated
What is Identity?

• That which gives you access … which is largely determined by context
  – We all have lots of identities
  – Pseudo-identities

• Really, determined by who is evaluating credential
  – Driver’s License, Passport, SSN prove …
  – Credit cards prove …
  – Signature proves …
  – Password proves …
  – Voice proves …

• Exercise: Give an example of bad mapping between a credential and the purpose for which it was used.
Credentials

... are evidence used to prove identity

- Something I am
- Something I have
- Something I know
Something you know …

- Passport number, mother's maiden name, last 4 digits of your social security, credit card number
- Passwords and pass-phrases
  - Note: passwords are generally pretty weak
    - University of Michigan: 5% of passwords were goblue
    - Passwords used in more than one place
  - Not just because bad ones selected: If you can remember it, then a computer can guess it
    - Computers can often guess very quickly
    - Easy to mount off-line attacks
    - Easy countermeasures for on-line attacks
Passwords (cont.)

• Entropy vs. memorability
  – The more complex a password the harder it is to guess ...
  – ... and the harder it is to remember.
  – Thus, we write them down.

• Preventing online attacks
  – Tracking bad guesses and “locking” account
  – Slowing after each guess
  – Problems here?

• Preventing offline attacks
  – Hashing, salting passwords
  – Protected Storage

• Q: *password policies*: setting standards helpful?
Password Security

• Who is an adversary?
• What are the threats?
• What are the vulnerabilities?

![Diagram showing the exchange of Username, Password between User and Server with Y/N response.]
Attack

• How does the attack work?
• Passive attack
Not my system

• Did systems really work this way?
  – A slew of them
  – rlogin, telnet, ftp, etc.

• Solutions
  – Secure communication of passwords
    • Cryptographic protocols: SSL, SSH

• What about other places where the password is available?
  – on computer
  – on paper
Password Storage

• Store password as a “hash” of its value
  – Originally stored in /etc/passwd file
  – Not in the clear

• Hash function: cryptographic
  – Like a checksum
  – One-way function: Using output H(x) cannot find x
  – Collision-free function: Highly unlikely that H(x)=H(y) if x not equal y

• Problems
  – Think about threats and vulnerabilities?
Password Cracking

• Attacker can access the hashed password
  – Can guess and test passwords offline
• Called “password cracking”
• Lots of help
  – John the Ripper
• How well do these work?
Password Cracking

• We ran John the Ripper on CSE authentications
  – 3500 in all

• In first hour, 25% were recovered
  – About half of these due to dictionary attacks
  – But, half using other heuristics and brute force

• Over 5 days, 35% were recovered
  – Steady state recovery due to brute force

• What happens when search get faster?
  – 95 characters and a 8 char password (/2) = $3.3 \times 10^{15}$
  – Sounds like a long time, but...
    • Parallelism: E.g., botnets, multiple cores
    • Botnet of 100,000 could crack in a day by next year
    • 1,000 Bots in a month by 2009
Password Protection

• Access: Change the way passwords are stored
  – /etc/shadow which is only accessible to root

• Length:
  – Increase password length to 15 characters

• Use Entropy:
  – Still need random passwords

• Problems:
  – A common network protocol still sends password material that could be collected and cracked
    • That is what we used, not /etc/shadow
  – How many 15 char passwords can you remember?
  – Password generation is not well-thought out
Password Policies

• One PSU student’s opinion

• “First of all why regulate student’s password security? It should be up to the student to change his or her password if he or she chooses to do so. Of someone wishes to share his or her password with someone else, let them. It’s obvious that the whole ordeal is meant to show the administration’s depth of control over the student population.”
Other Password Problems

• Often social factors are more of a problem

• Social Engineering
  – Share passwords
  – “shoulder surfing”
  – Post-its

• Internet
  – How many different passwords can you have?
  – Same one for every server?

• Phishing sites
  – Trick you into revealing your password
Something your have …

- Tokens (transponders, …)
  - Speedpass, EZ-pass
- Smartcards

- Digital Certificates (used by Websites to authenticate themselves to customers)
  - More on this later …
Two-Factor Authentication

• Combine what you know (e.g., passwords) with what you have

• Example
  – Grade entry
  – Requires password
  – And RSA SecurID value

• Smartcard and PIN
Biometrics measure some physical characteristic
- Fingerprint, face recognition, retina scanners, voice, signature, DNA
- Can be extremely accurate and fast
- Active biometrics authenticate
- Passive biometrics recognize

What is the fundamental problem?
- Revocation – lost fingerprint?
- Great for physical security, generally not feasible for online systems

Definitely will need a second factor
Take Away

• Authentication is a fundamental security mechanism
• Practical methods are in broad use
  – Have limited effectiveness
• Need support of cryptography
  – What we’ll discuss next week