PennState

CSE 443: Introduction to Computer Security

Module: Authentication

Prof. Syed Rafiul Hussain
Department of Computer Science and Engineering
The Pennsylvania State University

Acknowledgements: Some of the slides have been adopted from
Trent Jaeger (Penn State), Patrick McDaniel (Penn State), Ninghui Li (Purdue) and William Enck (NCSU)

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

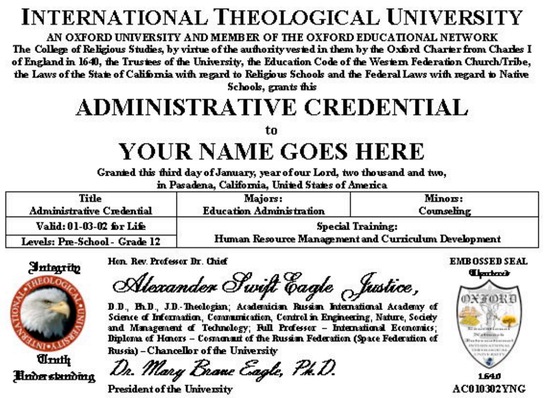
What is Identity?

- 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
- Credentials can be
  - Something I know
  - Something I have
  - Something I am



INTERNATIONAL THEOLOGICAL UNIVERSITY

AN OXFORD UNIVERSITY AND MEMBER OF THE OXFORD EDUCATIONAL NETWORK

The College of Religious Studies, by virtue of the authority vested in them by the Oxford Charter from Charles I of England in 1640, the Trustees of the University, the Education Code of the Western Federation Church/Tribe, the Laws of the State of California with regard to Religious Schools and the Federal Laws with regard to Native Schools, grants this

ADMINISTRATIVE CREDENTIAL

to

YOUR NAME GOES HERE

Granted this third day of January, year of our Lord, two thousand and two, in Pasadena, California, United States of America

Title	Majors:	Minors:
Administrative Credential	Education Administration	Counseling
Valid: 01-03-02 for Life	Special Training:	
Levels: Pre-School - Grade 12	Human Resource Management and Curriculum Development	

Integrity

Truth

Understanding

Hon. Rev. Professor Dr. Chief

Alexander Swift Eagle Justice,

D.D., Th.D., J.D.-Theologian, Academician Russian International Academy of Science of Information, Communication, Control in Engineering, Nature, Society and Management of Technology; Full Professor – International Economics; Diploma of Honors – Cosmonaut of the Russian Federation (Space Federation of Russia) – Chancellor of the University

Dr. Mary Beane Eagle, Ph.D.

President of the University

EMBOSSED SEAL

OXFORD

1640

AC010302YNG

Something you know …

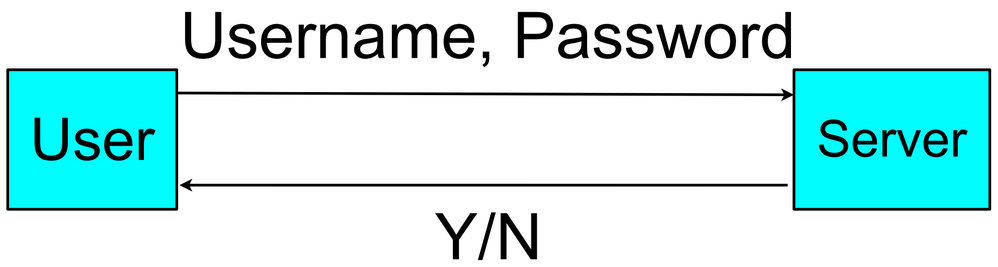
- Passport number, mothers maiden name, last 4 digits of your social security, credit card number
- Passwords and pass-phrases
  - Note: passwords are generally pretty weak
    - University of Michigan: 5% of passwords were goblue
    - Passwords used in more than one place
  - Not just because bad ones 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?

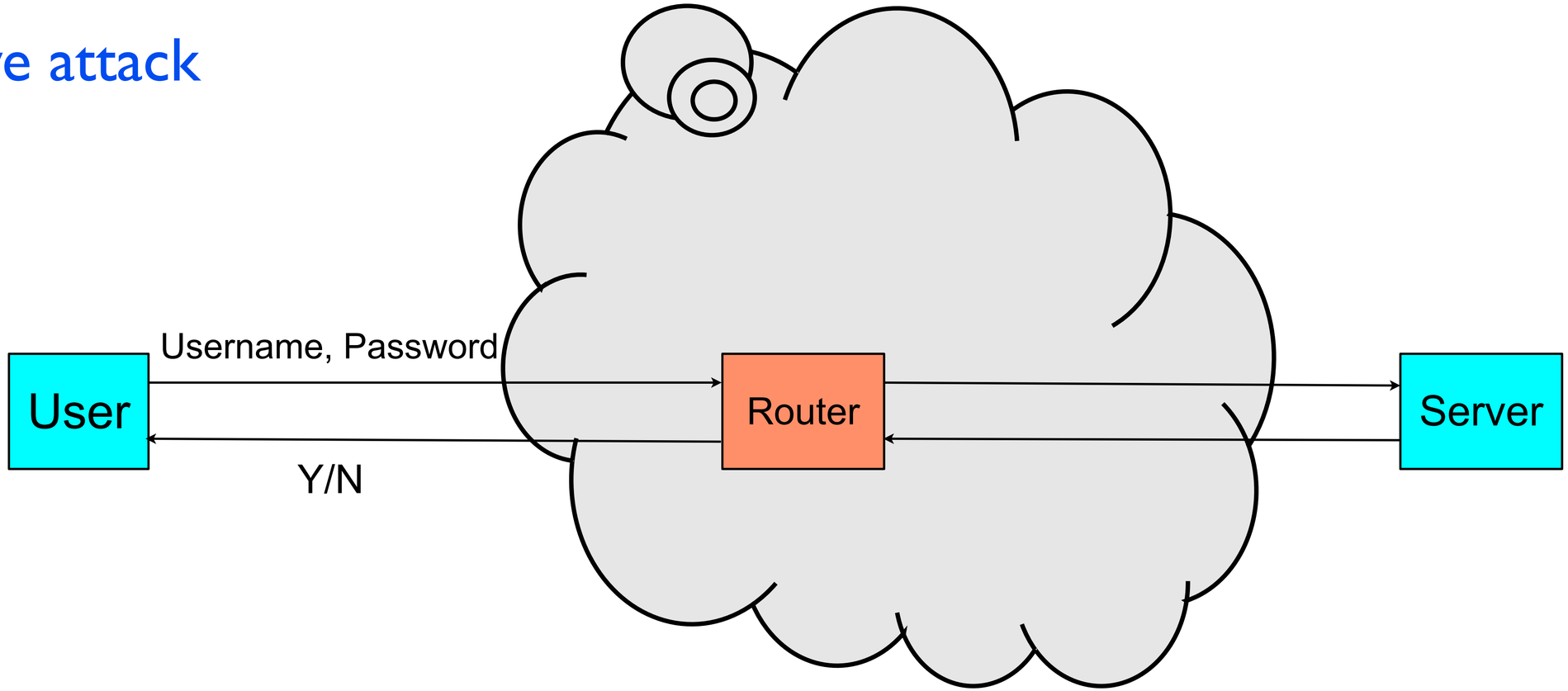
Password Security

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



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

- What properties must hash function satisfy for this purpose?
  - Should hash entries be invertible?
  - Could two passwords result in the same hash value?

Password Storage

PennState

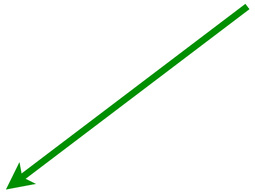
- Store password as a "hash" of its value
  - Originally stored in /etc/passwd file (readable by all)
  - Now in /etc/shadow (readable only be *root*)

- What if an adversary can gain access to a password file?
  - How would you attack this?

“Salt”ing passwords

- Suppose you want to avoid a *offline dictionary attack*
  - bad guy precomputing popular passwords and looking at the password file
- A *salt* is a random number added to the password differentiate passwords when stored in `/etc/shadow`

$$
\begin{array}{l}
salt_1, h(salt_1, pw_1) \\
salt_i, h(salt_2, pw_2) \\
salt_i, h(salt_3, pw_3) \\
\\
\\
salt_n, h(salt_n, pw_n)
\end{array}
$$



- *consequence*: guesses each password independently

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) = 3.3×10^{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

Password Protection

- Access: Change the way passwords are stored
  - /etc/shadow which is only accessible to root
- Length:
  - Increase password length to 12 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 12 char passwords can you remember?
  - Password generation is not well-thought out

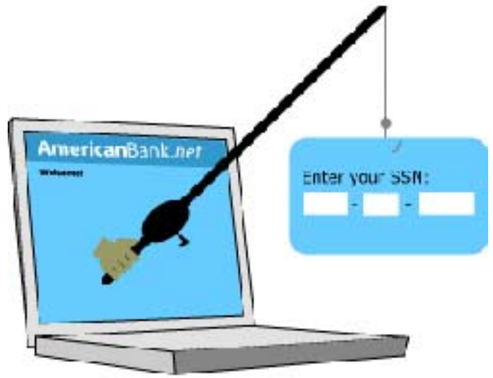
Password Policies

- 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 you have …

- Tokens (transponders, …)
  - Speedpass, EZ-pass
  - SecureID
- Smartcards
  - Unpowered processors
  - Small NV storage
  - Tamper resistant

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

A (simplified) sample token device

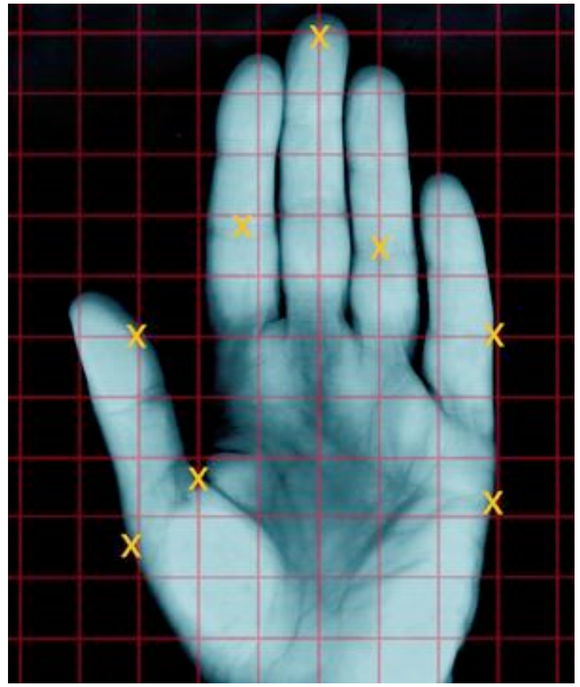
- A one-time password system that essentially uses a *hash chain* as authenticators.
  - For seed (S) and chain length (l)
  - Tamperproof token encodes S in firmware

$$\mathrm{pw}_i = h^{l-i}(S)$$

  - Device display shows password for epoch i
  - Time synchronization allows authentication server to know what i is expected, and authenticate the user.
- *Note*: somebody can see your token display at some time but learn nothing useful for later periods.

Something your are …

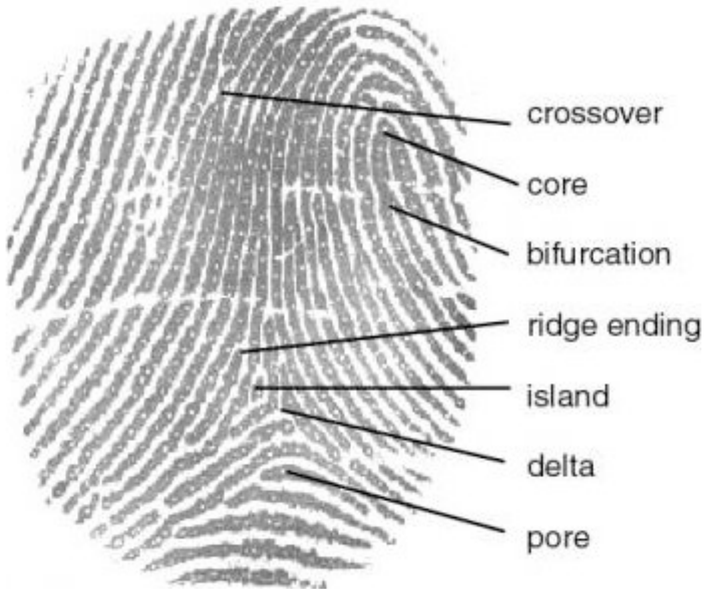
- Biometrics measure some physical characteristic
  - Fingerprint, face recognition, retina scanners, voice, signature, DNA
  - Can be extremely accurate and fast
  - Active biometrics authenticate
  - Passive biometrics recognize



- Issues with biometrics?
  - Revocation – lost fingerprint?
  - "fuzzy" credential, e.g., your face changes based on mood ...
  - Great for physical security, not feasible for on-line systems

Biometrics Example

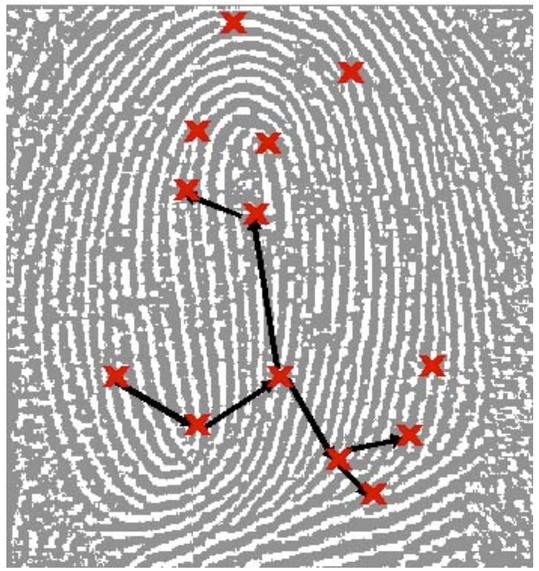
- A fingerprint biometric device (of several)
  - record the conductivity of the surface of your finger to build a "map" of the ridges
  - scanned map converted into a graph by looking for landmarks, e.g., ridges, cores, …



  - A fingerprint is represented in the form of a graph whose nodes correspond to ridges in the print. Edges of the graph connect nodes that represent neighboring or intersecting ridges.

Fingerprint Biometrics (cont.)

- Graph is compared to database of authentic identities
- Graph is same, the person deemed "authentic"
  - This is a variant of the *graph isomorphism* problem
  - Problem: what does it mean to be the "same enough"
    - rotation
    - imperfect contact
    - finger damage



- *Fundamental Problem*: False accept vs. false reject rates?

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