Security building blocks: authentication

Markus Peuhkuri

2005-03-01

Lecture topics

- Authentication
- Different methods to authenticate
- Caveats in authentication

How one authenticates

- What one *knows*
  - passwords, PIN
- What one *has*
  - keys, smartcards
- *What* one *is*
  - biometric identification
- *Where* one *is*
  - terminal restrictions

Risks on authentication

- Masquerade
  - use of victim's resources
- Multiple identities
  - social benefits, voting, law enforcement
- Identity theft
  - victim's identity, attackers authentication

Attacks on authentication

- Trial and error
  - password guessing
  - token authenticator subverting
  - team attack on biometrics

  ⇒limit attack space: number of attempts. However, that may result denial of service.
- Replication of authenticator
- Stealing of authenticator
- Playback attack

Deploying authentication

- Enrolment
  - trusted administrator ⇔ self-enrolment
- Maintenance
  - password aging, update of biometrics
- Revocation
  - lost token, disclosed secret key
- Operational problems
  - re-establishing authenticator

Economics of authentication

- Software
  - for organisation, system
- Hardware
  - for site, user, workstation
- Enrolment costs
  - administration, per user costs
- Usage costs
  - time spent by user to authenticate
- Maintenance
  - time spent to maintain system: for system administration and user time to renew password.
- Problem recovery
  - lost devices, forgotten passwords, flu
- Availability
  - cost of lost access
- Revocation costs
  - removing rights from user, lost authenticators

Passwords

- Prevailing method to authenticate
- No extra hardware needed
- Can be as strong as wanted
  - 8-character password of printable ASCII characters
    ⇒ 52-bit key
  - 20-character ⇒128 bits
- In reality, key space much smaller
- User memory overloading with passwords

Study on password quality [2]

- Students divided into 3 groups

  control group with traditional advice: Your password should be at least seven characters long and contain at least one non-letter.

  random password group with randomly selecting letters from sheet

  passphrase group with mnemonic phrase to aid remembering

	Cracked %		Difficulty	
group	dictionary	+brute-force	1-5	weeks to learn
control	32	3	1.52	0.7
random	8	3	3.15	4.8
phrase	6	3	1.67	0.6
other	33	2		

So, what is a good password policy?

- Promote mnemonic-based passwords
  - easy to remember
  - difficult to guess
- Use long enough passwords[1]
- Advice using non-alphanumeric characters[2]
- Enforce user compliance
  - does a bad password endanger system or other users?[3]
  - random assigned passwords a method to enforce quality

Password storage

- If stored plain, system compromise leads to disclosure
  $\Rightarrow$ possible large-scale compromise
- Using external authentication server
  - is it possible to detect on wire
- Distributed knowledge of right authentication

Using passwords

- Password recovery on web sites
  - new password or link to reset emailed to user
  - possibly verification question
  - all rest on mail password
- Initial passwords
  - often badly chosen
  - opens window of attack before user changes
  - latent accounts

[1] Minimum 8 characters, more if case does not matter.
[2] Note, that those position differs in different keyboards.
[3] Or, should users be protected from themselves.

Authentication tokens

- Smart card with cryptographic processor
  - key is kept on card, only results communicated
  - may be in several forms
- GSM SIM module
- Challenge-response calculators
- Time-based tokens
- Should be tamper-resistant

Using authentication token

- Separates authentication from device
  - revocation costs less
  - class compromise may not be fatal
- Strictly controlled environment
- Less trust on third-party devices
- Less trust on software
- Provides keys for network communications

Multi-factor authentication

- Compromise of single factor does not endanger system
  - password on local terminal
  - ssh key from network (key protected by passphrase)
  - debit card and PIN
- Pluggable Authentication Modules (PAM)
  - possible to have any combination of authentication

Biometrics

- 1997: year of biometrics... and since then
- Method used by humans

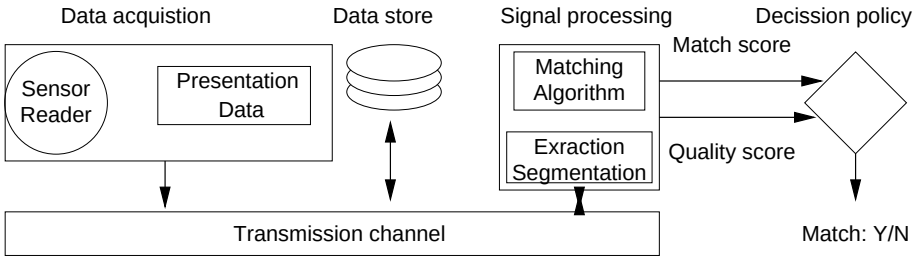
  > *She put the skins of the kids of the goats on his hands, and on the smooth of his neck. ... Jacob went near to Isaac his father. He felt him, and said, "The voice is Jacob's voice, but the hands are the hands of Esau." (Genesis 27:16)*

- Why to use biometrics
  - convenient: authenticator is always with you
  - need for strong authentication: difficult to steal or lose.
  - decreased cost of devices
  - government and industry adoption

Trusted path

- How a user knows she is talking to trojan
  - attention key
  - small, external device
- How a system knows there is a human
- Can someone record and replay authentication tokens

Components of biometric system [1, p. 29]



[1]

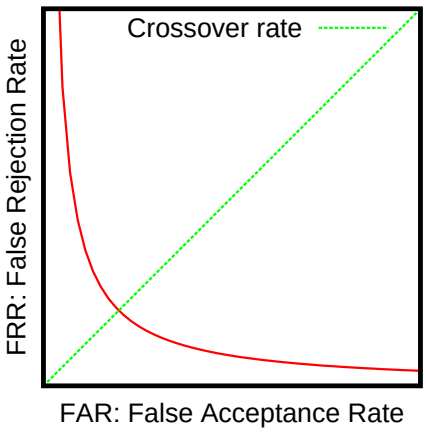
$$FAR = \frac{False\ acceptance\ count}{total\ number\ of\ samples} \quad \text{(Type II error)} \tag{1}$$

$$FRR = \frac{False\ rejections\ count}{total\ number\ of\ samples} \quad \text{(Type I error)} \tag{2}$$

- failure rate
- insult rate

Identification $\Leftrightarrow$ authentication

- Sheep $\Leftrightarrow$ goats



- Identification
  - who is this person?
  - selecting one from a large group
    $\Rightarrow$ high error rate
  - birthday paradox
- Authentication
  - is this person N.N.?
  - checking if person matches to one's records

Biometric characteristics based on

- Genetics
- Phenotype
- Behavioural
- Liveness testing important part

Biometrics

- Fingerprint
  - used for thousands of years, crime 1870s
  - 256 – 1200 B
  - degeneration of fingerprints
  - 1 – 3 % of population has problems
- Hand geometry
  - hand and finger length, width
  - 9 B
  - injury
  - 1.5 % error rate
- Facial
  - works best with “mug shots”
  - 80 – 2000 B
  - environmental factors
  - typical 10 – 25 % error rate
- Voice
  - 70 – 80 B/sec
  - illness, noise, communications
  - 2 % error rate
- Signature
  - 500 – 1000 B
  - lots of variable factors
- Keystroke dynamics
  - continuous monitoring
  - high FRR
- Iris
  - 256 – 512 B
  - glasses, positioning
  - 10 s authentication time
  - very low error rate
- Retina
  - 96 B
  - illness
  - awkward method, difficult to record without user knowledge
  - very low error rate

Experimental biometrics

- Vein patterns back of hand
- Facial thermography
- DNA
- Sweat pores
- Hand grip
- Fingernail bed
- Body odour
- Ear shape
- Gait: body motion
- Skin luminance
- Brain wave pattern
- Footprint, foot dynamics

Location security

- Physical security well understood
  - radio waves does not stop on walls
- Many problems solved with human monitoring
  - voting
  - biometrics
- Restricts possibility for an attacker
  - administrator password can be entered from connected console
- Use of GPS or other positioning method
- Enforcing communication delay limits

Summary

- Password is still good
- If it is man-made, a man can break it
- Selecting right compromise between FAR — FRR
- Beware denial of service

References

[1] Jr. John D. Woodward, Nicholas M. Orlans, and Peter T. Higgins. *Biometrics*. McGraw-Hill/Osborne, 2003.

[2] J. Yan, A. Blackwell, R. Anderson, and A. Grant. Password memorability and security: empirical results. *IEEE Security & Privacy Magazine*, 2(5):25–31, September 2004.