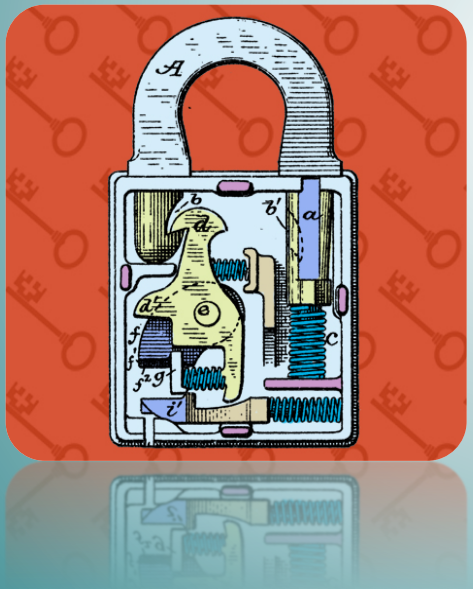
Garantía y Seguridad en Sistemas y Redes

Tema 3. User Authentication



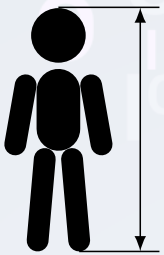
Esteban Stafford

Departamento de Ingeniería Informática y Electrónica

Contents

Means of Authentication

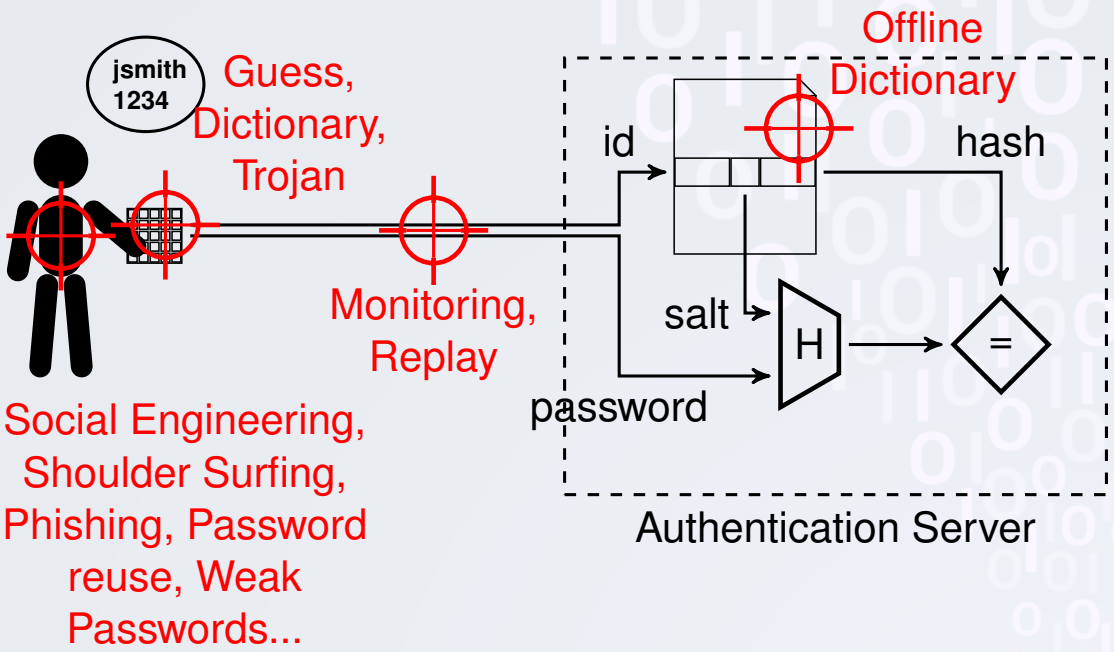
- The user's identity can authenticated with something he/she...

Knows	Has	Is	Can
			
Passwords, PIN, Prearranged Questions	Keys, keycards, code generators	Fingerprint, retina, face	Voice, handwriting, typing

Multifactor Authentication

- Single means of authentication might not be enough.
- Combine two or more authentication factors.
- Typical
  - Token + PIN
  - Password + Email
  - Password + Mobile phone (SMS one-time-password)
  - ...

Password-Based Authentication



Reducing password vulnerabilities

- **Offline Dictionary**: Protect authentication server. Make hash function slow.
- **Monitoring**: Improve protocol. Encrypt network traffic.
- **Replay**: Improve protocol. Encrypt network traffic.
- **Dictionary**: Limit amount of unsuccessful attempts per endpoint and time period.
- **User**
  - Education!!!
  - Force periodic password change.
  - Proactive Password Checker: Enforce password length and complexity at choosing time.

Dictionary attacks

Experiment: Open `ssh` port to the Internet.

Time	Attempts
20:00	154
21:00	0
22:00	160
23:00	206
00:00	0
01:00	0
02:00	0
03:00	324
04:00	140
05:00	371
06:00	243
07:00	176

IP Address	Attempts	Time (min)
117.27.158.98	132	4.91
122.225.103.97	206	5.03
122.225.109.105	176	4.75
122.225.109.120	210	5.01
122.225.109.219	160	4.15
144.0.0.26	510	34.53
218.2.0.129	243	4.83
61.174.51.215	155	5.08

User Name	Attempts
root	1618
admin	174

Token-Based Authentication

- Longer strong computer generated codes.
- Sophisticated authentication algorithms.

- Hardware requirements.
- Possibility of token loss or theft (PIN).
- User inconvenience.

Protocols

- **Static**: Like passwords, only longer.
- **Dynamic Password Generators**: Passwords are changed after time (Time-synchronized passwords) or number of uses (Mathematical-algorithm-generated passwords).
- **Challenge-response**: Authentication server sends data to token, which responds in a unique way to it.

Token-Based Authentication

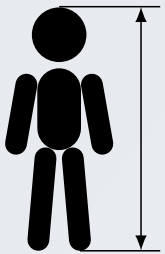
Interface

- **Screen**: User reads and types password.
- **Electronic**: Token interacts directly with authentication server (Contacts, USB, Bluetooth)

Examples

- Memory cards
- Chip (Smart) cards
- RFID Keys
- Security hardware tokens
- Mobile telephones

Biometric Authentication

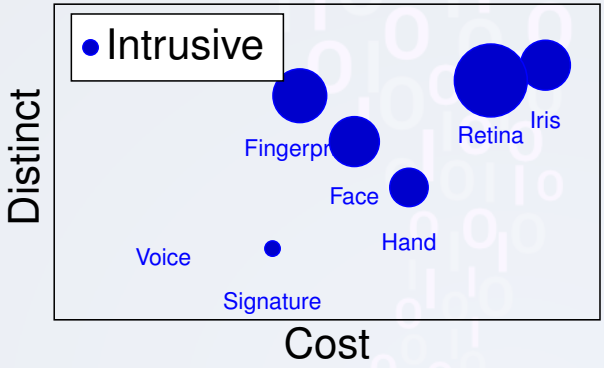


- Fingerprints
- Facial Features
- Hand geometry
- Retinal pattern
- Iris

- Signature
- Voice
- Typing timing

About

- Physical measurements converted to bits.
- Data is checked against Authentication Server.
- Dynamic Biometric are good for challenge protocols.

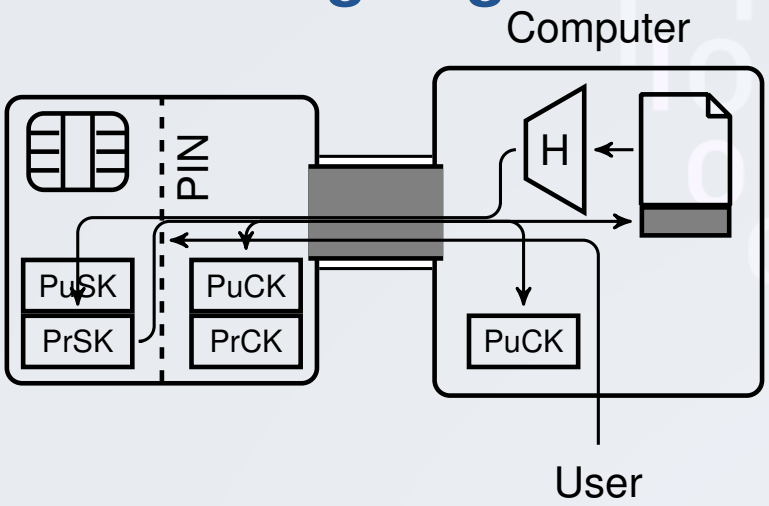


Dto. Nacional de Identidad Electrónico

- Document that authenticates the user's identity and signature in the physical world.
- Since 2006, it uses Integrated Circuit Card ISO-7816-1.
- Chip allows the user to sign and authenticate digitally.

Public	PIN Protected	Secured
■ CA Certificate	■ Authentication Cert	■ User Info.
■ Diffie-Hellman keys	■ Signing Cert	■ Photo
■ Component Cert	■ X509v3 2048bit key with RSA enc.	■ Signature
		■ Fingerprints

Document signing with DNIe



- **Firma electrónica avanzada**: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios bajo el exclusivo control del firmante.
- **Firma electrónica reconocida**: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Authentication/SSL with DNIe