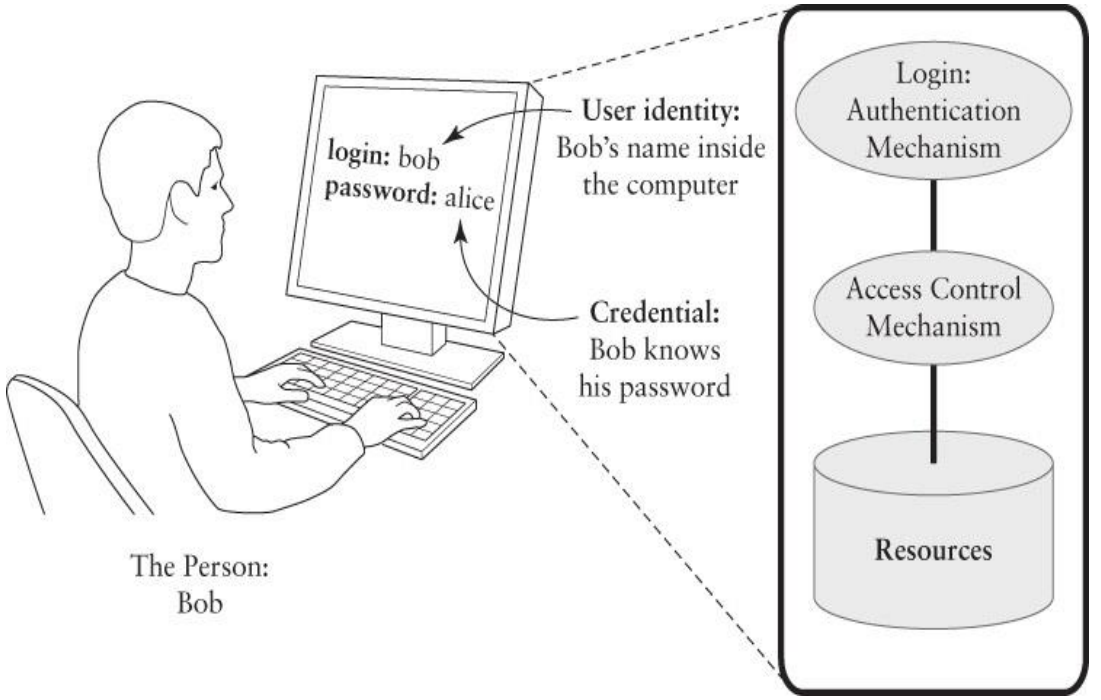
Authenticating Users

Today's Plan

- **Elements of Authentication (Chapter 6, Elementary Information Security)**
- Lab 5: Managing users and groups in Linux.
- Lab(s) Python: Passwords and Biometrics.

Elements of Authentications

- An authentication system makes it as hard as possible for one user to masquerade as another by forging a credential.



Authentication Factors

- Something you know
  - Password, pin
- Something you have
  - Key, token
- Something you are
  - Biometric measure, personal trait

Others authentication factors?

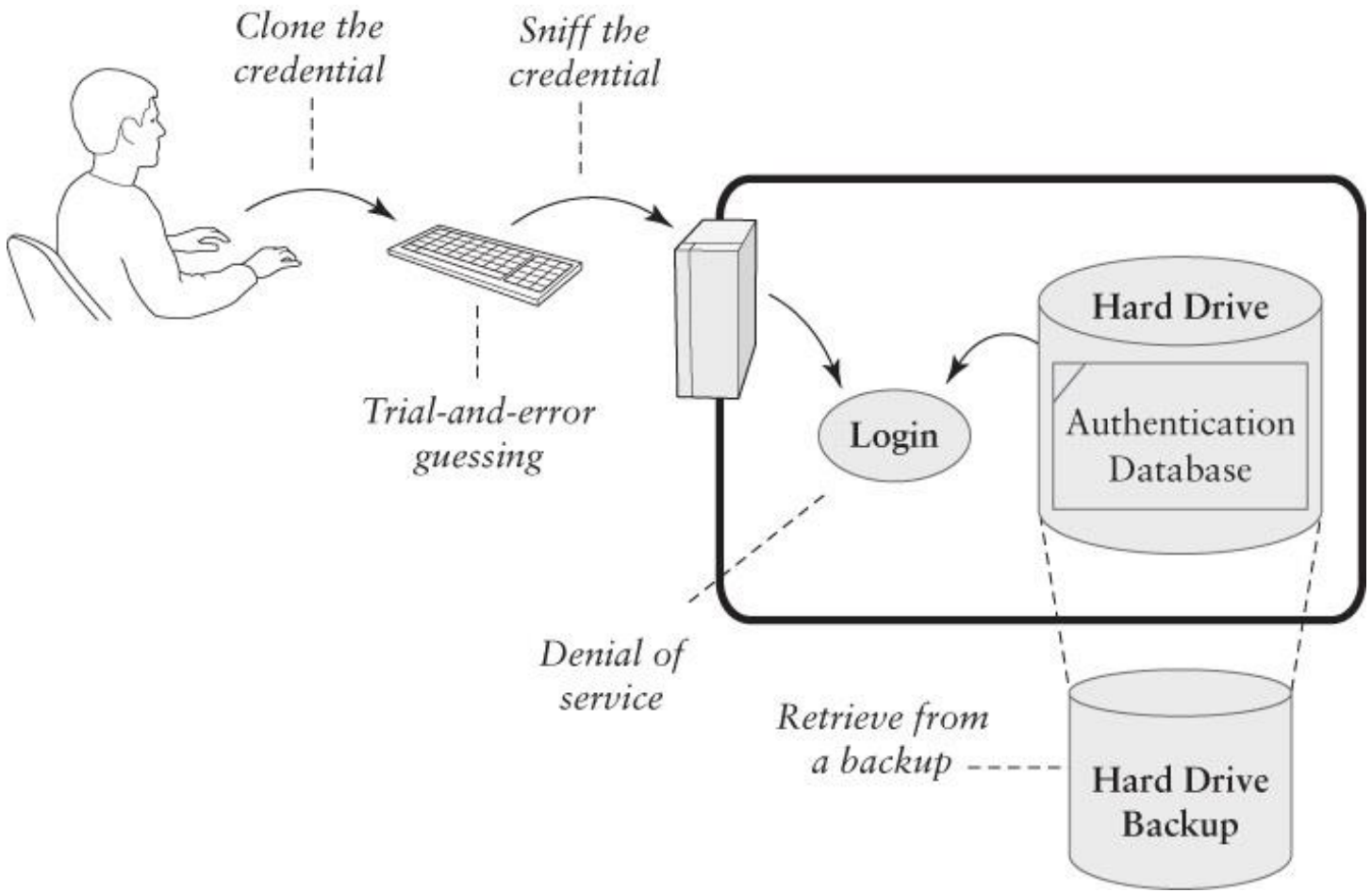
- **Something you can do**, e.g. accurately reproducing a signature or speak.
- **Something you exhibit**, e.g. a particular personality trait, or even neurological behaviour that could be read by an fMRI. These are not strictly "are" features, as they're more fluid.
- **Somewhere you are** (or have access to), e.g. locking a session to an IP, or sending a confirmation pin to your address. This one is a bit tenuous in terms of being called an *authentication* factor, but it's still useful to note.

Adding more really helps?

Multi-Factor Authentication

- Using different factors, not multiple instances of the same factor
- Follows the **defence-in-depth** best practice principle:
  - Checkpoints are added for authentication and authorisation.
- Examples: ATM, Biometric laptops, Biometric cards.

Attacks on Authentication



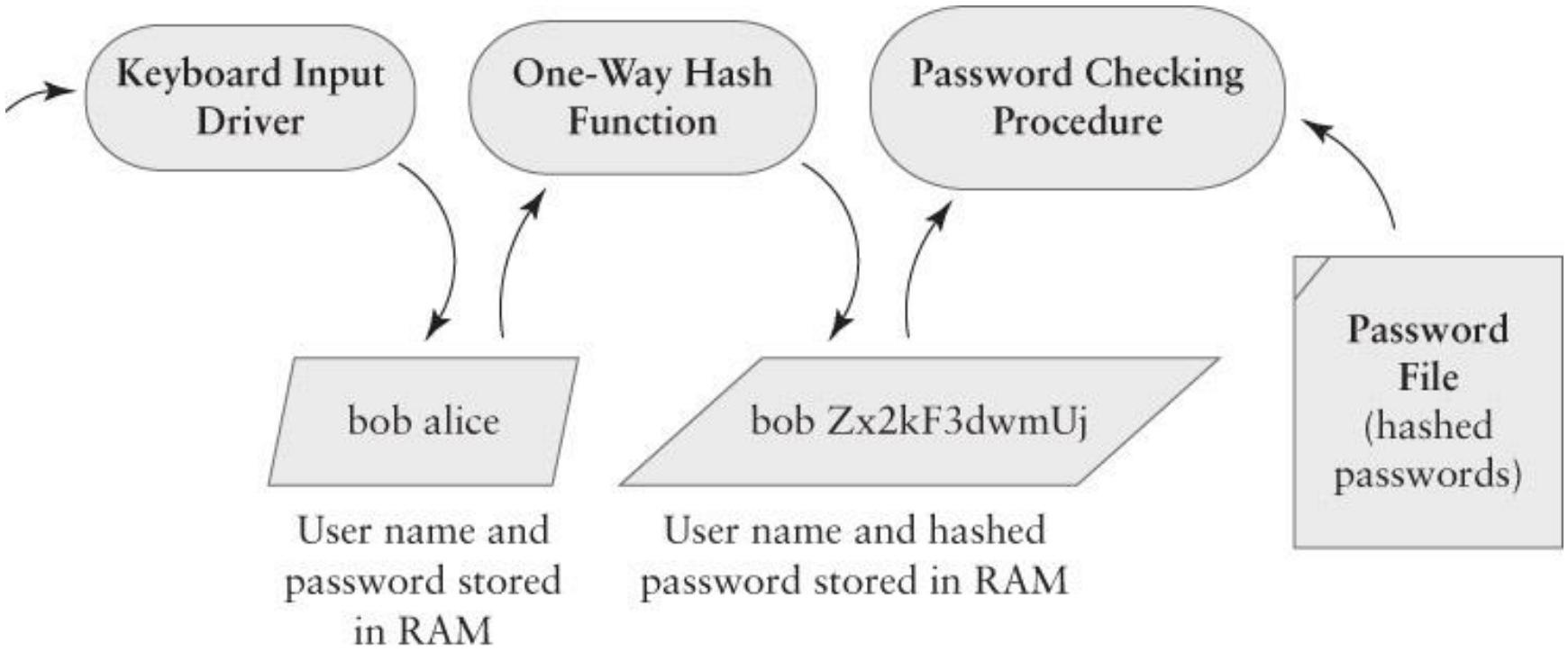
Passwords

Something you know

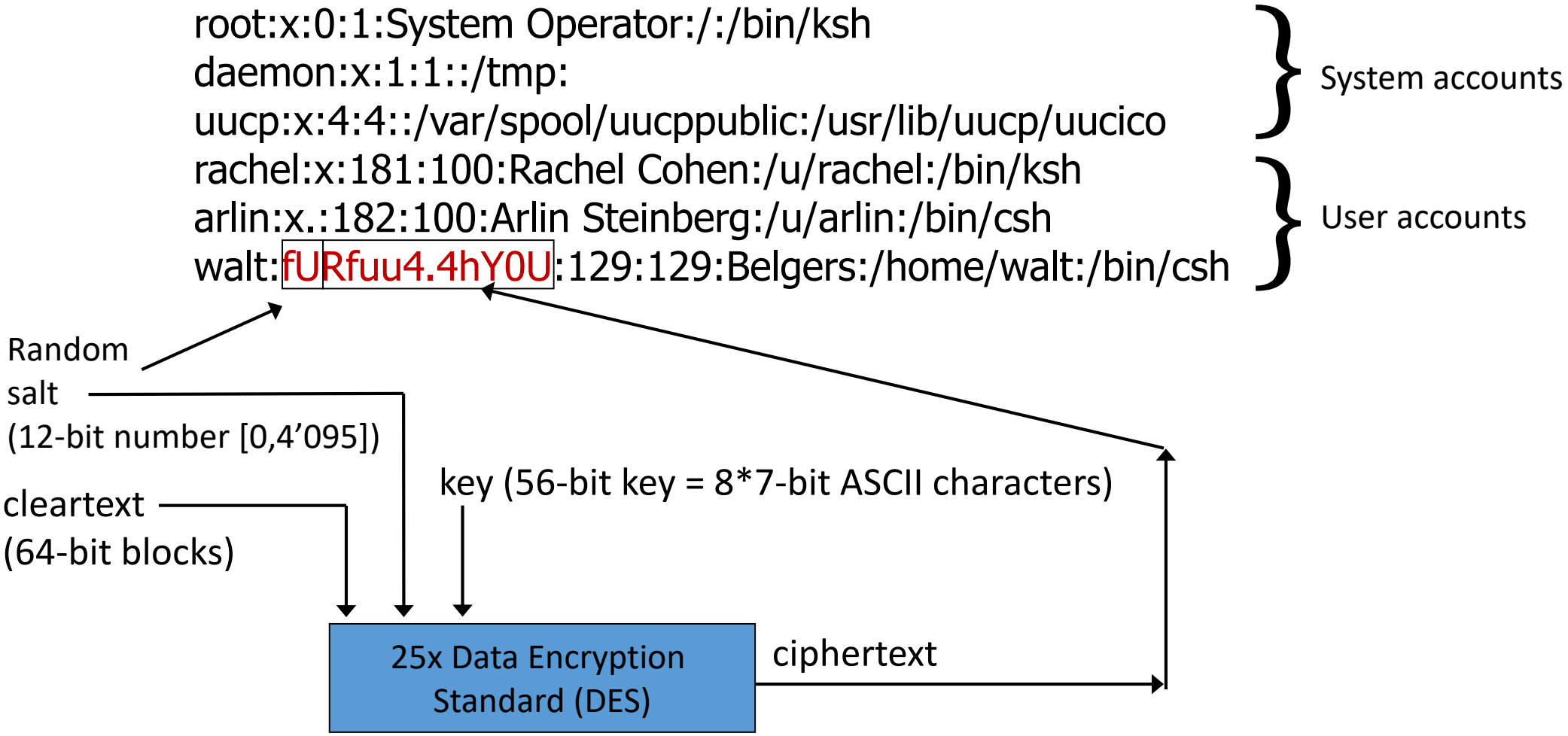
Password Authentication

- Each User ID is associated with a secret:
  - User presents the secret when logging in.
  - System checks the secret against the authentication database.
  - Access granted if the secret matches.
- Risks:
  - Shoulder surfing at the keyboard.
  - Reading the password off of printer paper.
  - Sniffing the password in transit or in RAM.
  - Retrieving the authentication database.

Password Hashing



The crypt() algorithm



Examples of “salted” passwords

Password	Salt	Encrypted password
nutmeg	Mi	MiqkFWCm1fNJI
ellen1	ri	ri79KNd7V6.Sk
Sharon	./	./2aN7ysff3qM
norahs	am	amfIADT2iqjAf
norahs	7a	7azfT5tIdyh0I

Pros and Cons of Classical Salt

- The same password can be encrypted in 4,096 different ways.
- This makes it much harder for an attacker to build a reverse dictionary for translated encrypted passwords back into her unencrypted form:
  - To build a reverse dictionary of 100,000 words, an attacker would need to have 409,600,000 entries.
  - With 8-character passwords and 13-character encrypted passwords, 409,600,000 entries fit in roughly 8 GBs of storage.
- Error in implementation:
  - Many systems selected salt based on the time of day, which made some salts more likely than others.

Solutions

- Adopting other encryption methods (i.e. Blowfish, MD5, SHA).
  - Add more characters for passwords and more salt variety.
- crytpt16(): Increase DES rounds.
- Modular Crypt Format (MCF): Extensible scheme for formatting encrypted passwords.
  - 1EqkVUoQ2$4VLpJuZ.Q2wm6TAiyYt75.
  - 5rounds=535000$h84dK.$eTIcudqFuA7bfMQza61WMQ73WtvkLmjbfsdOnKaSRj/

Sniffing Passwords

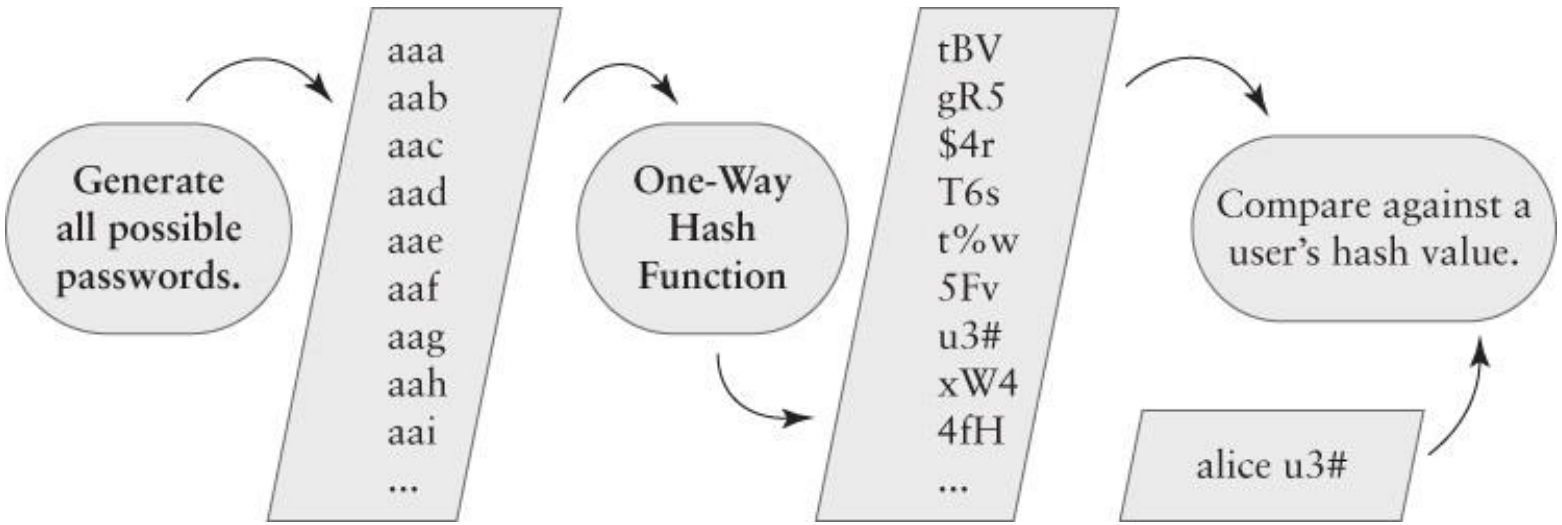
- Goal: intercept the password before it is hashed.

- Keystroke loggers
  - In Hardware: devices that connect to a keyboard's USB cable.
  - In Software: procedures that eavesdrop on keyboard input buffers.

Password Guessing

- DoD Password Guideline (1985) required a minimum 1 in a million chance of successful guessing.
  - This was designed to defeat interactive password guessing: a person or machine made numerous guesses.
- Some guessing succeeds based on social and personal knowledge of the targeted victim.
- Modern network-based guessing can try tens of thousands of alternatives very quickly.
- Examples: John the Ripper, hydra, medusa, ophcrack, rainbowcrack, ssh bruteforce, etc…

Offline Password Cracking



How fast it is?

- It depends on the size of the search space.
  - How many valid or likely passwords are there?

- Valid passwords are limited to specific sets of characters, typically from the ASCII set.
    - Two letter passwords = 26^2
    - Three letter passwords = 26^3
    - Password with L letters = 26^L

Increasing the search space

- Two options:
  - Increase length of password L.
  - Increase the character set A.

- Search space for fixed length password $S = A^L$

- Search space S for range of lengths from 1 to L : $S = \frac{(A^{L+1}-1)}{(A-1)}$

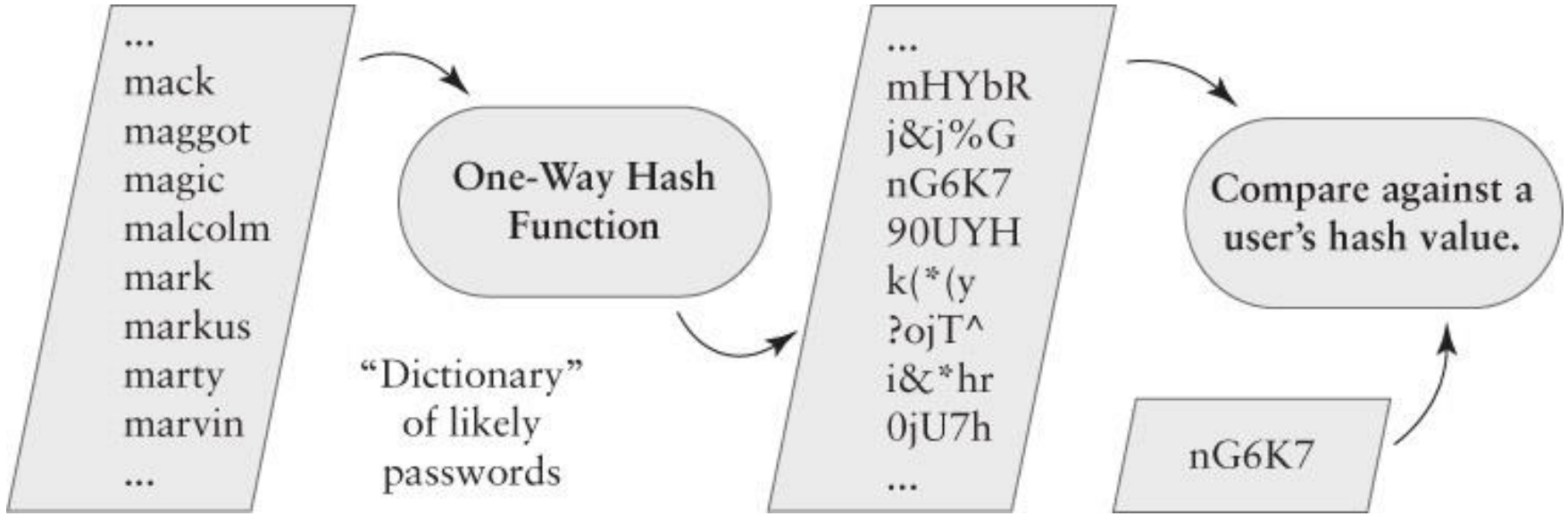
Reducing the search space

- Attacker does not try every possible password!

- Restricts the search space to likely passwords:
  - **Morris worm successfully used this attack.**

- A dictionary attack
  - Uses a list of likely passwords as the password space.
  - There are far fewer likely passwords than possible passwords.

Dictionary Attack



How fast is it?

- An estimate of the likelihood that a trial-and-error attack will succeed:
  - Construct a dictionary of passwords that people are likely to use.
  - Estimate the likelihood that people choose those passwords.

FIXED LENGTH

$$V = \frac{S}{l} = \frac{A^L}{l}$$

RANGE OF LENGTHS 1 TO L

$$V = \frac{S}{l} = \frac{\frac{(A^{L+1}-1)}{(A-1)}}{l} = \frac{A^{L+1}-1}{l(A-1)}$$

- *S* = Size of the search space (dictionary).
- l = Likelihood that users choose from dictionary.
- *V* = # of trials for success (i.e. for a 50% chance, $l = 2$).

Tokens

Something you have

Pro’s and Con’s

Benefits

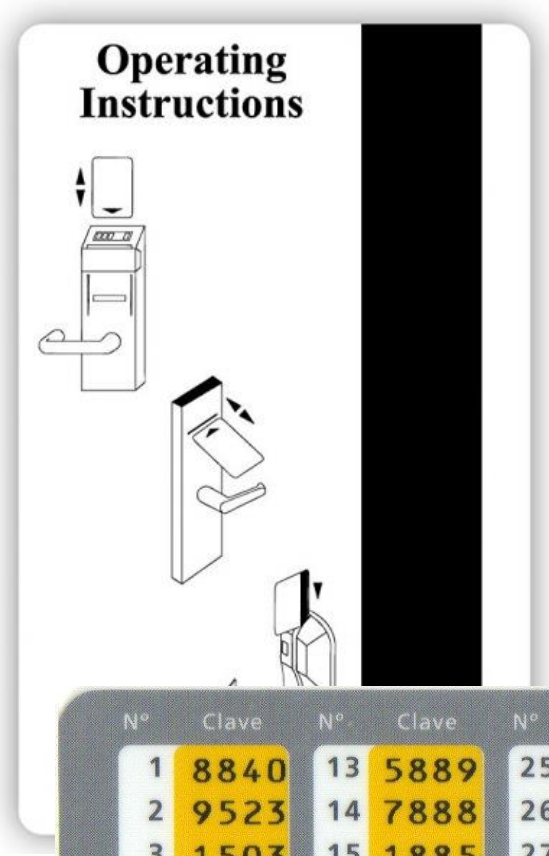
- Hard to attack - uses a stronger secret than you get in a typical password.
- Hard to forge - must hack the hardware.
- Hard to share – secret stored in hardware.

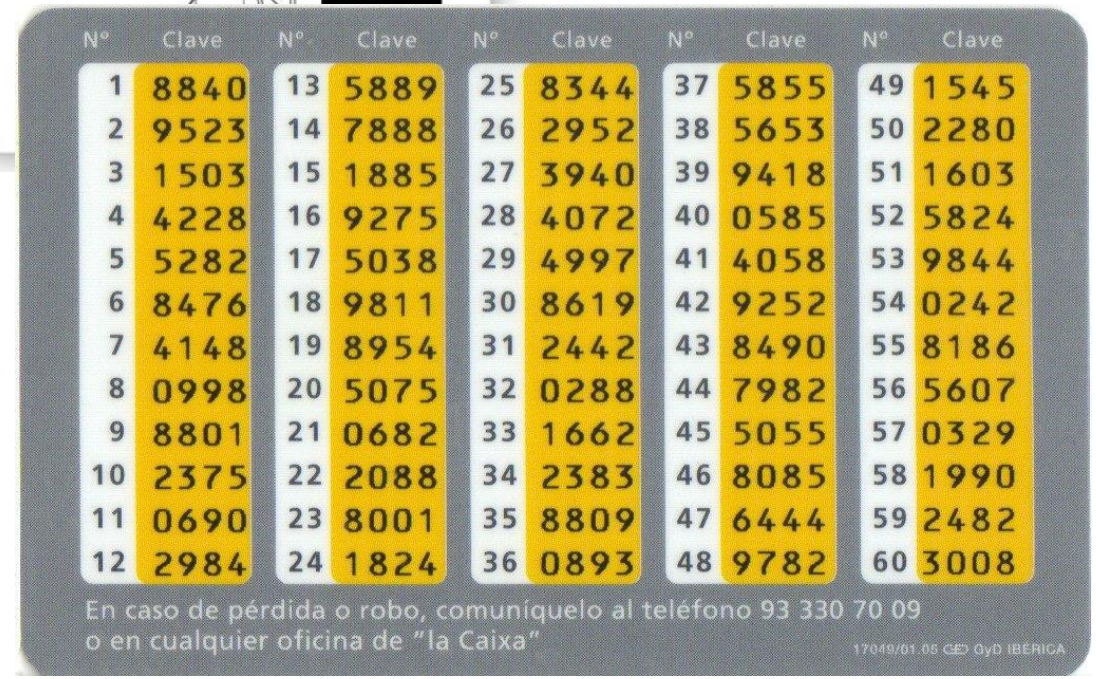
Problems

- “Expensive”.
- Can be lost or stolen.
- Risk of hardware failure.
- Risk of battery loss.

Types of Tokens

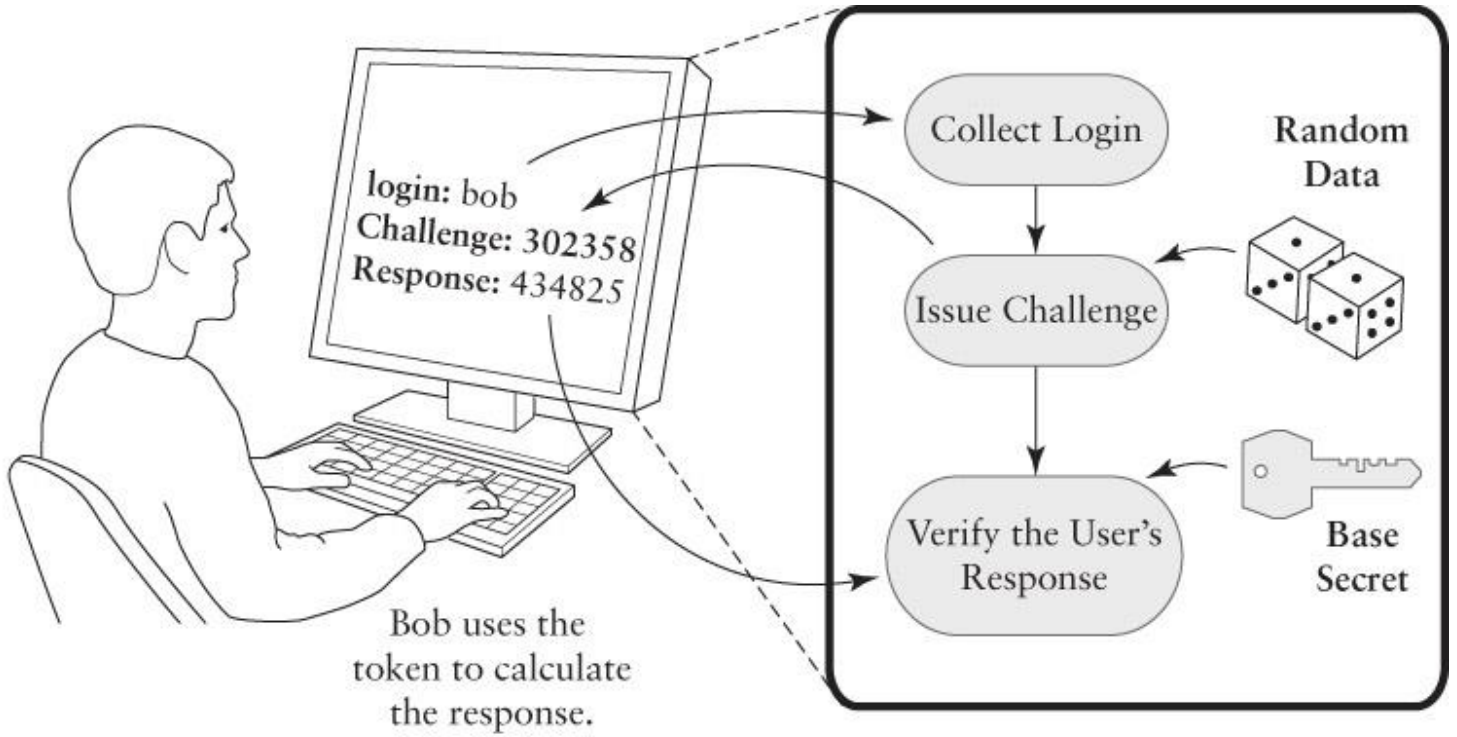
- Passive Tokens
  - Stores an unchanging credential.
  - Example: card keys for hotel rooms.
- Active Tokens
  - Stores a secret that generates a different credential for each login
  - Example: one-time password tokens.





N°	Clave	N°	Clave	N°	Clave	N°	Clave	N°	Clave
1	8840	13	5889	25	8344	37	5855	49	1545
2	9523	14	7888	26	2952	38	5653	50	2280
3	1503	15	1885	27	3940	39	9418	51	1603
4	4228	16	9275	28	4072	40	0585	52	5824
5	5282	17	5038	29	4997	41	4058	53	9844
6	8476	18	9811	30	8619	42	9252	54	0242
7	4148	19	8954	31	2442	43	8490	55	8186
8	0998	20	5075	32	0288	44	7982	56	5607
9	8801	21	0682	33	1662	45	5055	57	0329
10	2375	22	2088	34	2383	46	8085	58	1990
11	0690	23	8001	35	8809	47	6444	59	2482
12	2984	24	1824	36	0893	48	9782	60	3008

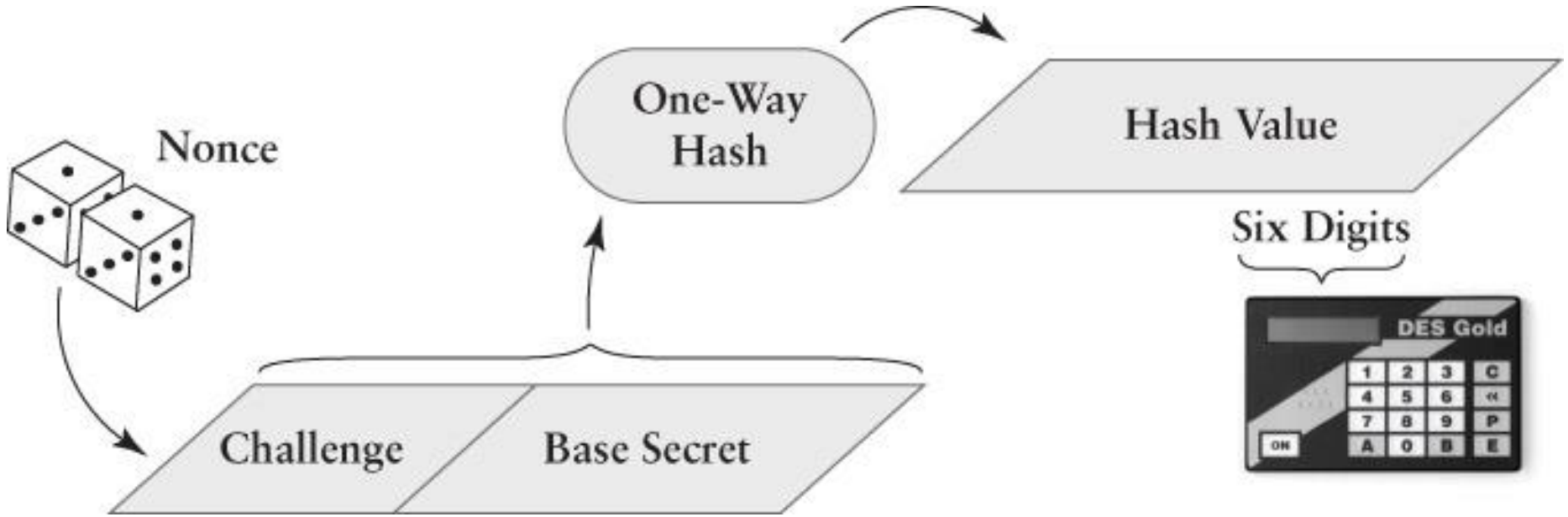
Challenge Response Authentication



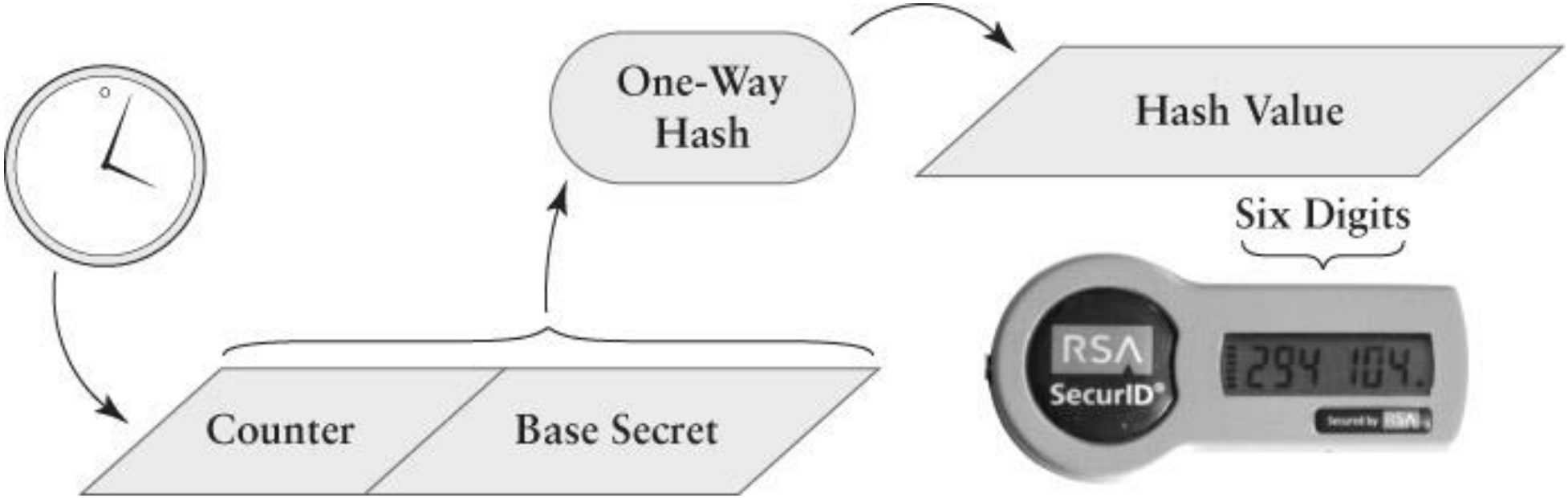
Challenge Response Authentication

- Challenge Response Authentication is a protocol.
  - An exchange of data to yield a shared result.
- Four steps:
  - Bob says, “Authenticate me”.
  - Alice says, “The challenge is 56923”.
  - Bob calculates the response and says, “The response is 17390”.
  - Alice checks Bob’s response against what she expected, using the same calculation.
- Calculation relies on a shared secret.

Challenge Response Authentication



One-time Password Token



Biometrics

Something you are

Bertillion System of Criminal Identification


RELEVÉ
DU
SIGNALEMENT ANTHROPOMÉTRIQUE

1. Taille. — 2. Envergure. — 3. Buste. — 4. Longueur de la tête. — 5. Largeur de la tête. — 6. Oreille droite. — 7. Pied gauche. — 8. Médius gauche. — 9. Coudée gauche.


DEPARTMENT OF POLICE SERVICE — NEW HAVEN, CONN.

Name Edward Blasco. Aliases Wm. Breen. Color Wh.

Crime Trespass on R.R. Cars. Date of Arrest Nov. 23d, 1933.

Disposition City Court, Nov. 24, 1933, Judgment suspended.

BERTILLON MEASUREMENTS

Height	1 m	Head length		L. Foot	Color of left eye	Circle 4.	Age 17 Born in
Stretch		Head Width		L. Mid. F.		Periph Z.	Apparent Age 17.
Trunk	1 m	Cheek Width		L. Lit. F.			Nativity ?
Eng. Height	6.1.	R. Ear		L. Fore A.		Pecul.	Occupation None.

Remarks incident to Measurement: Height in shoes.

DESCRIPTIVE

Right index finger to be impressed IMMEDIATELY after Signature is written

Forehead: Inclin. / Height / Width / Pecul.

Nose: Profile: Ridge / Base / Root. DIMENSIONS: Length / Projection / Breadth. Pecul.

R. Ear

Teeth Up. ft., are bad.

Chin

Beard

Hair Dk. ch.

Complexion Med. dk.

Weight 137.

Build Slim.

Measured at Police Headquarters New Haven, Conn. Date Nov. 23d, 1933. 19

Prisoner's Signature Edward Blasco.

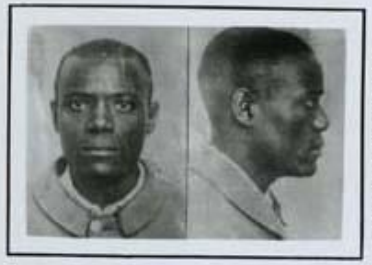
Remarks Lucky, Thing he and two others were arrested at Cedar Hill RR yard, If they had reached where the electric wires are, would have been killed

When bertillionage failed

FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
J. Edgar Hoover, Director

History of the "West Brothers" Identification..

Bertillon Measurements are not always a Reliable Means of Identification



In 1903, one WILL WEST was committed to the U. S. Penitentiary at Leavenworth, Kansas, a few days thereafter being brought to the office of the record clerk to be measured and photographed. He denied having been in the penitentiary before, but the clerk doubting the statement, ran his measuring instruments over him, and from the Bertillon measurements obtained went to his files, returning with the card the measurements called for properly filled out, accompanied with the photograph and bearing the name WILLIAM WEST. Will West, the new prisoner, continued to deny that the card was his, whereupon the record clerk turned it over and read that William West was already a prisoner in that institution, having been committed to a life sentence on September 9, 1901, for murder.

The Bertillon measurements of these, given below, are nearly identical whereas the fingerprint classifications given are decidedly different.

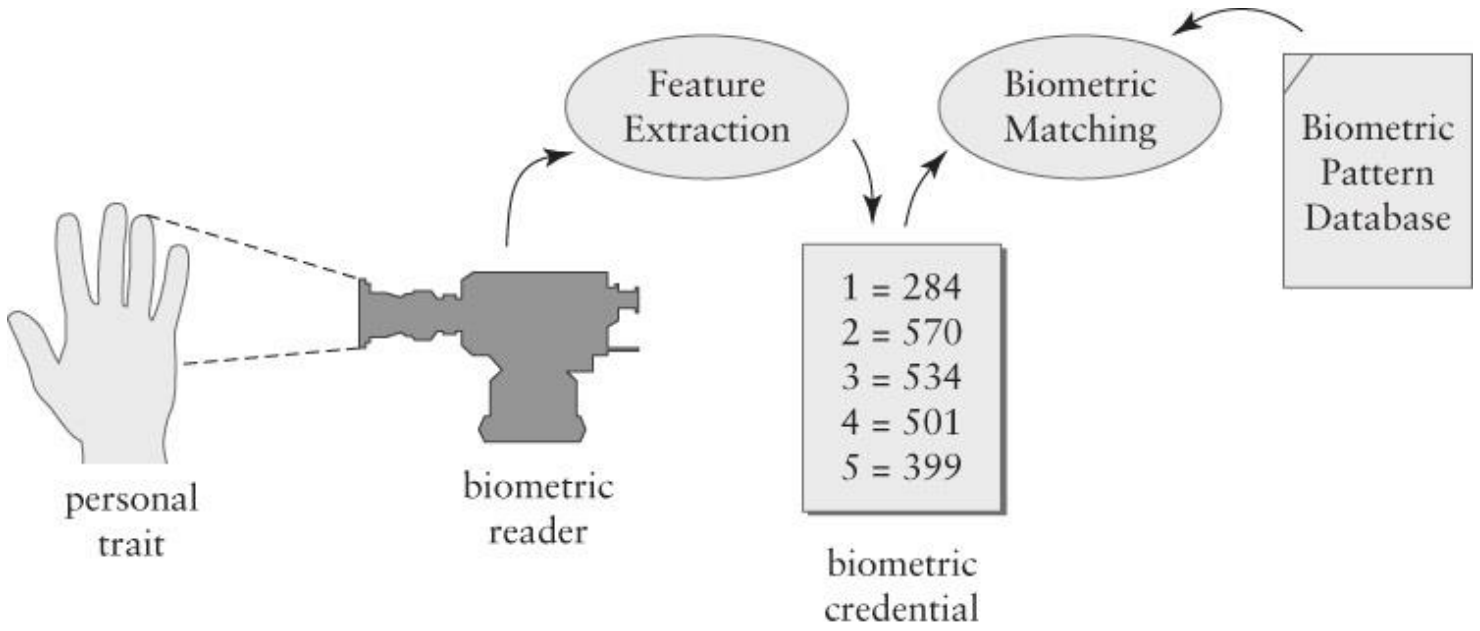
The case is particularly interesting as indicating the fallacies in the Bertillon system, which necessitated the adoption of the fingerprint system as a medium of identification. It is not even definitely known that these two Wests were related despite their remarkable resemblance.

Their Bertillon measurements and fingerprint classifications are set out separately below:

177.5; 188.0; 91.3; 19.8; 15.9; 14.8; 6.5; 27.5; 12.2; 9.6; 50.3
15- 30 W OM 13 Ref: 30 W OM 13
28 W I 26 U OO

178.5; 187.0; 91.2; 19.7; 15.8; 14.8; 6.6; 28.2; 12.3; 9.7; 50.2
10- 13 U O O Ref: 13 U O 17
32 W I 18 28 W I 18

Biometrics 101



Accuracy

- Two types of errors:
  - False acceptance: Incorrectly detects a match with a credential and the database.
  - False rejection: Fails to detect a match between a credential and the database.
- False Acceptance Rate (FAR)
  - Likelihood of incorrectly authenticating someone as an authorised user.
    - $V = \frac{1}{2 * A_{FAR}}$
- False Rejection Rate (FRR)
  - Denial of service.
  - Calculated as number of rejections / total attempts.

Calculation of V in biometrics

- What would “99%” or “99.9%” accuracy would mean in terms of FAR and V?

$$Acc = 99\%$$
$$FAR = 1\%$$
$$A_{FAR} = 0.01$$
$$V = \frac{1}{2 * A_{FAR}} = \frac{1}{0.02} = 50$$

One in 50 attacks will be successful.

$$Acc = 99.9\%$$
$$FAR = 0.1\%$$
$$A_{FAR} = 0.001$$
$$V = \frac{1}{2 * A_{FAR}} = \frac{1}{0.002} = 500$$

One in 500 attacks will be successful.

Authentication Requirements

- Constructing a policy for an isolated computer.
- Answer these questions:
  - Is the computer used at home, at work, or both?
  - For each environment, are there threats?
  - Are these weak, strong or extreme threats?
- Weak threat: Might make an opportunistic attack on a vulnerable computer.
- Strong threat: Will spend time and effort on an attack, if unlikely to be detected and/or caught.
- Extreme threat: Will take whatever is needed even with the risk of being caught.

Threats and Motivations

Level of Threat	Level of Motivation	Level of Motivation Related to Authentication
Weak Threat	No Motivation	The agent is not motivated to try to trick the authentication system.
	Scant Motivation	The agent has limited skills and a mild motivation to overcome the authentication system. For example, an agent might exploit a written-down password or carelessly stored key.
Strong Threat	Stealth Motivation	The agent has the skills and motivation to attack the authentication system, but is not motivated to cause significant, visible damage.
	Low Motivation	The agent has the skills and motivation to attack the authentication system and cause visible though limited damage.
Extreme Threat	Moderate Motivation	The agent has the skills and motivation to attack the authentication system and cause significant damage, possibly including bodily injuries.
	High Motivation	The agent has the skills and motivation to attack the authentication system and cause severe damage, possibly including loss of life.

Weak Threat Environments

- At Home
  - Do not write down passwords that are at risk of being lost or stolen.
- At Work
  - Avoid shoulder surfing.
  - Passwords may be written down as long as the user keeps physical possession of the list.
  - Authentication tokens shall be used.
- Passwords should be hard to guess and easy to remember.

Strong Threat Environment

- Using Passwords
  - System should track failed password guesses to try to detect guessing attacks.
  - Protect against keyboard sniffers.
  - Pick passwords that resist offline attacks.
  - The system should provide “secure attention”.
- Other options:
  - Multi-factor authentication.

Final note


NORTH KOREA
Military Demarcation Line
SEOUL
Incheon
Suwon
Wonju
Gangneung
Ulleungdo
Liancourt Rocks
Sea of Japan
Yellow Sea
Daejeon
Daegu
Pohang
Jeonju
Changwon
Ulsan
Gwangju
Busan
Mokpo
Yeosu
Korea Strait
Jeju-do
Hallasan
0 50 100 km
0 50 100 mi

Lab 5: Creating Users in Linux

ADDITIONAL PRACTICE

- After lab 5, try the jupyter notebooks on passwords and biometrics using Python.