Managing Enterprise Cybersecurity MIS 4596

Unit #12

Agenda

- Identity and Authentication – a historic problem
- Identity and Authentication for controlling access to IT Assets
- Identification
- Authentication
    - Something you know
    - Something you have
    - Something you are
- Multi-factor Authentication

Learning more about RSA

An online tool for checking your work:

https://www.cryptool.org/en/cto/rsa-step-by-step

Part 2. Calculating RSA keys

Note: To help you answer the following questions, view this "RSA Algorithm" video. Also, you can review the RSA wikipedia page example.

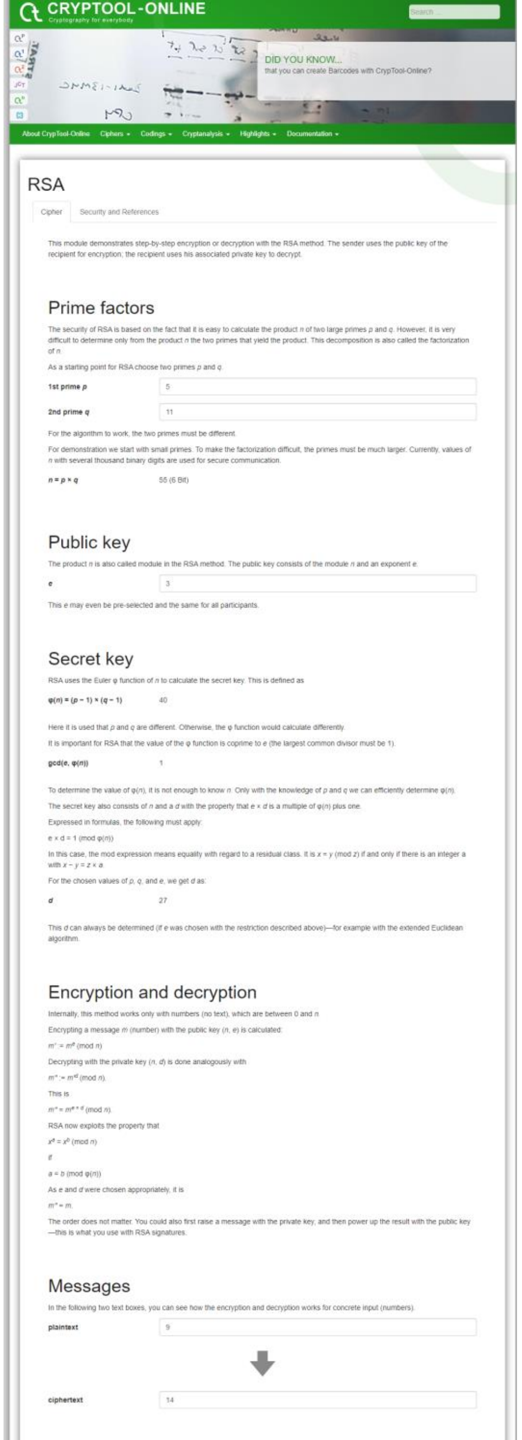
1. Complete encryption and decryption using the RSA algorithm, for the following data (show all work): `p = 5, q = 11, e = 3, M = 9`. Also:

   Question: What is the ciphertext when performing RSA encryption with p=5, q=11, e=3, M=9?

   Question: Show all work for encryption **and** decryption

2. You are Eve. In a public-key system using RSA, you intercept the ciphertext, `C=10`, sent to a user whose public key is `e=5, n=35`.

   Question: What is the plaintext `M`?



RSA

This module demonstrates step-by-step encryption or decryption with the RSA method. The sender uses the public key of the recipient for encryption; the recipient uses his associated private key to decrypt.

Prime factors

The security of RSA is based on the fact that it is easy to calculate the product n of two large primes p and q. However, it is very difficult to determine only from the product n the two primes that yield the product. This decomposition is also called the factorization of n.

As a starting point for RSA choose two primes p and q.

1st prime p 5

2nd prime q 11

For the algorithm to work, the two primes must be different.

For demonstration we start with small primes. To make the factorization difficult, the primes must be much larger. Currently, values of n with several thousand binary digits are used for secure communication.

$n = p \times q$ 55 (6 Bit)

Public key

The product n is also called module in the RSA method. The public key consists of the module n and an exponent e.

e 3

This e may even be pre-selected and the same for all participants.

Secret key

RSA uses the Euler φ function of n to calculate the secret key. This is defined as

$\varphi(n) = (p - 1) \times (q - 1)$ 40

Here it is used that p and q are different. Otherwise, the φ function would calculate differently.

It is important for RSA that the value of the φ function is coprime to e (the largest common divisor must be 1).

$\gcd(e, \varphi(n))$ 1

To determine the value of $\varphi(n)$, it is not enough to know n. Only with the knowledge of p and q we can efficiently determine $\varphi(n)$.

The secret key also consists of n and a d with the property that $e \times d$ is a multiple of $\varphi(n)$ plus one.

Expressed in formulas, the following must apply:

$e \times d = 1 \pmod{\varphi(n)}$

In this case, the mod expression means equality with regard to a residual class. It is $x = y \pmod{z}$ if and only if there is an integer a with $x - y = z \times a$.

For the chosen values of p, q, and e, we get d as:

d 27

This d can always be determined (if e was chosen with the restriction described above)—for example with the extended Euclidean algorithm.

Encryption and decryption

Internally, this method works only with numbers (no text), which are between 0 and n.

Encrypting a message m (number) with the public key (n, e) is calculated:

$m' := m^e \pmod{n}$

Decrypting with the private key (n, d) is done analogously with

$m'' := m'^d \pmod{n}$.

This is

$m'' = m^{e \times d} \pmod{n}$.

RSA now exploits the property that

$x^a = x^b \pmod{n}$

if

$a = b \pmod{\varphi(n)}$

As e and d were chosen appropriately, it is

$m'' = m$.

The order does not matter. You could also first raise a message with the private key, and then power up the result with the public key—this is what you use with RSA signatures.

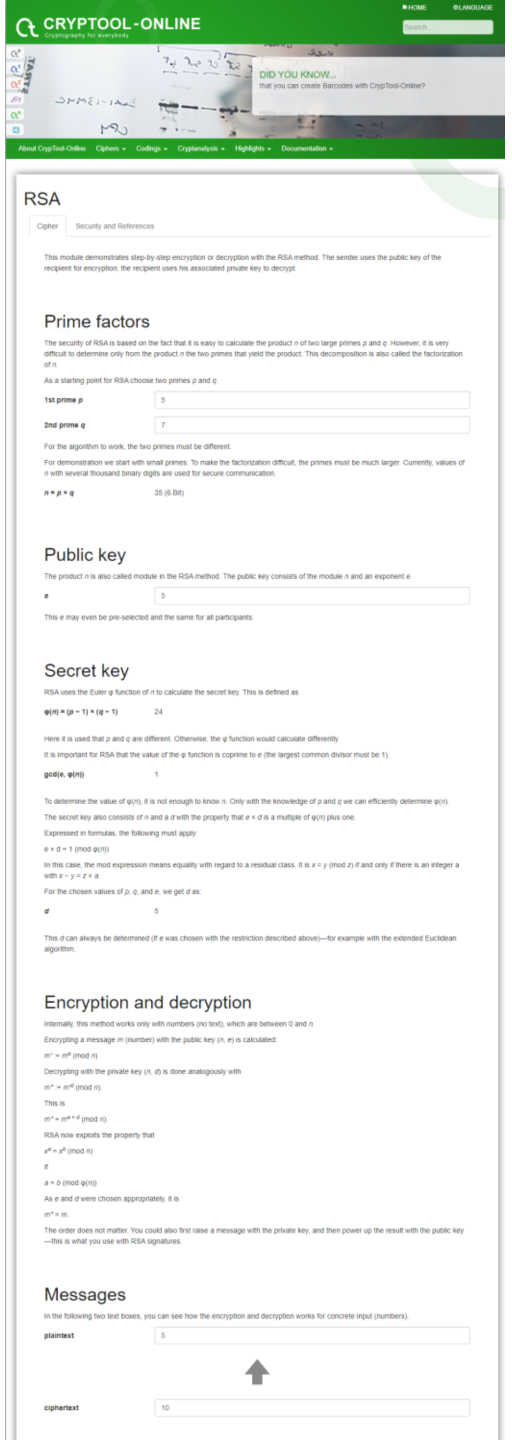
Messages

In the following two text boxes, you can see how the encryption and decryption works for concrete input (numbers).

plaintext 9

↓

ciphertext 14



RSA

This module demonstrates step-by-step encryption or decryption with the RSA method. The sender uses the public key of the recipient for encryption; the recipient uses his associated private key to decrypt.

Prime factors

The security of RSA is based on the fact that it is easy to calculate the product n of two large primes p and q. However, it is very difficult to determine only from the product n the two primes that yield the product. This decomposition is also called the factorization of n.

As a starting point for RSA choose two primes p and q.

1st prime p 5

2nd prime q 7

For the algorithm to work, the two primes must be different.

For demonstration we start with small primes. To make the factorization difficult, the primes must be much larger. Currently, values of n with several thousand binary digits are used for secure communication.

$n = p \times q$ 35 (6 Bit)

Public key

The product n is also called module in the RSA method. The public key consists of the module n and an exponent e.

e 5

This e may even be pre-selected and the same for all participants.

Secret key

RSA uses the Euler φ function of n to calculate the secret key. This is defined as

$\varphi(n) = (p - 1) \times (q - 1)$ 24

Here it is used that p and q are different. Otherwise, the φ function would calculate differently.

It is important for RSA that the value of the φ function is coprime to e (the largest common divisor must be 1).

$\gcd(e, \varphi(n))$ 1

To determine the value of $\varphi(n)$, it is not enough to know n. Only with the knowledge of p and q we can efficiently determine $\varphi(n)$.

The secret key also consists of n and a d with the property that $e \times d$ is a multiple of $\varphi(n)$ plus one.

Expressed in formulas, the following must apply:

$e \times d = 1 \pmod{\varphi(n)}$

In this case, the mod expression means equality with regard to a residual class. It is $x = y \pmod{z}$ if and only if there is an integer a with $x - y = z \times a$.

For the chosen values of p, q, and e, we get d as:

d 5

This d can always be determined (if e was chosen with the restriction described above)—for example with the extended Euclidean algorithm.

Encryption and decryption

Internally, this method works only with numbers (no text), which are between 0 and n.

Encrypting a message m (number) with the public key (n, e) is calculated:

$m' := m^e \pmod{n}$

Decrypting with the private key (n, d) is done analogously with

$m'' := m'^d \pmod{n}$.

This is

$m'' = m^{e \times d} \pmod{n}$.

RSA now exploits the property that

$x^a = x^b \pmod{n}$

if

$a = b \pmod{\varphi(n)}$

As e and d were chosen appropriately, it is

$m'' = m$.

The order does not matter. You could also first raise a message with the private key, and then power up the result with the public key—this is what you use with RSA signatures.

Messages

In the following two text boxes, you can see how the encryption and decryption works for concrete input (numbers).

plaintext 5

↑

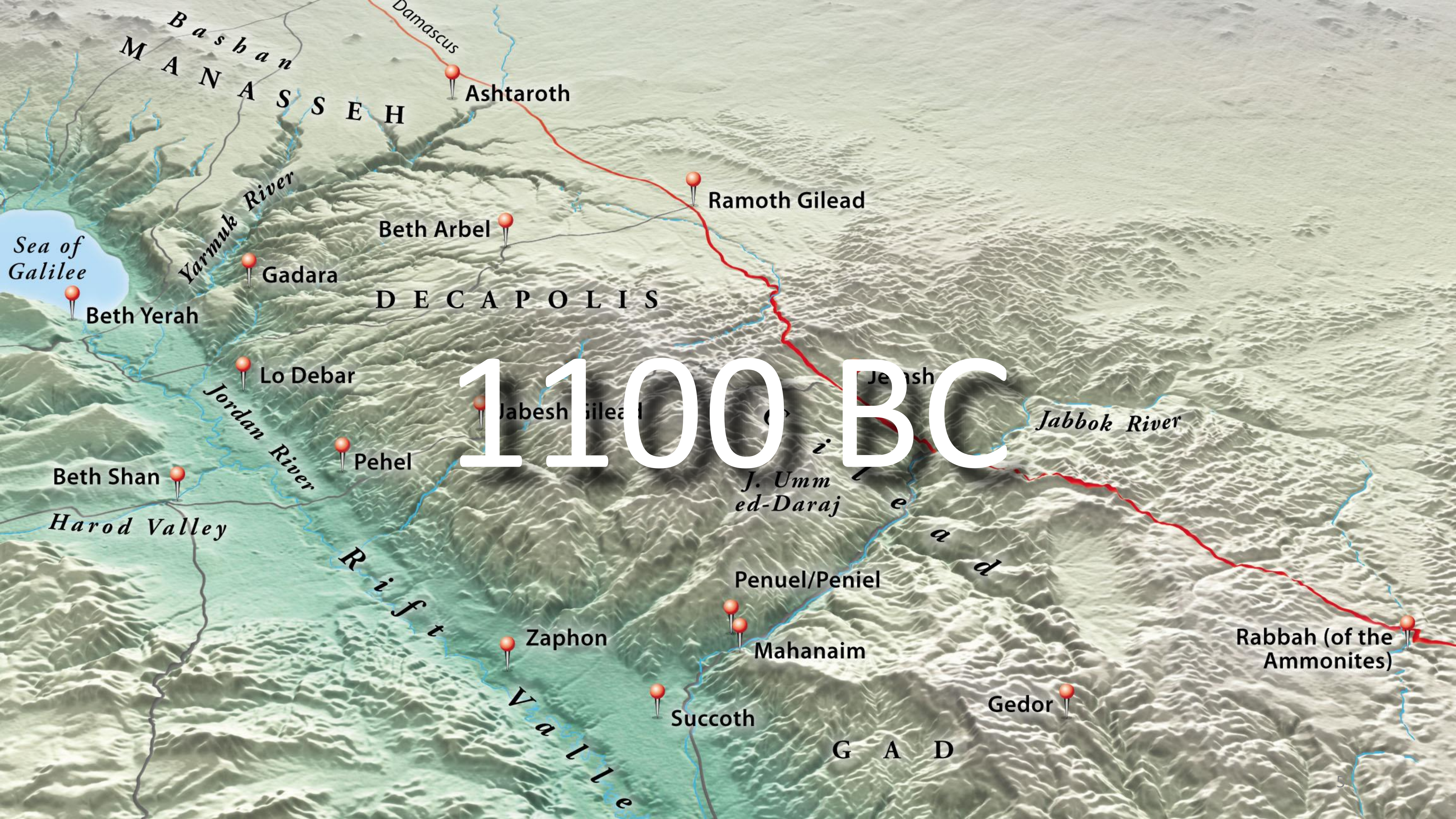
ciphertext 10

Identity and Authentication

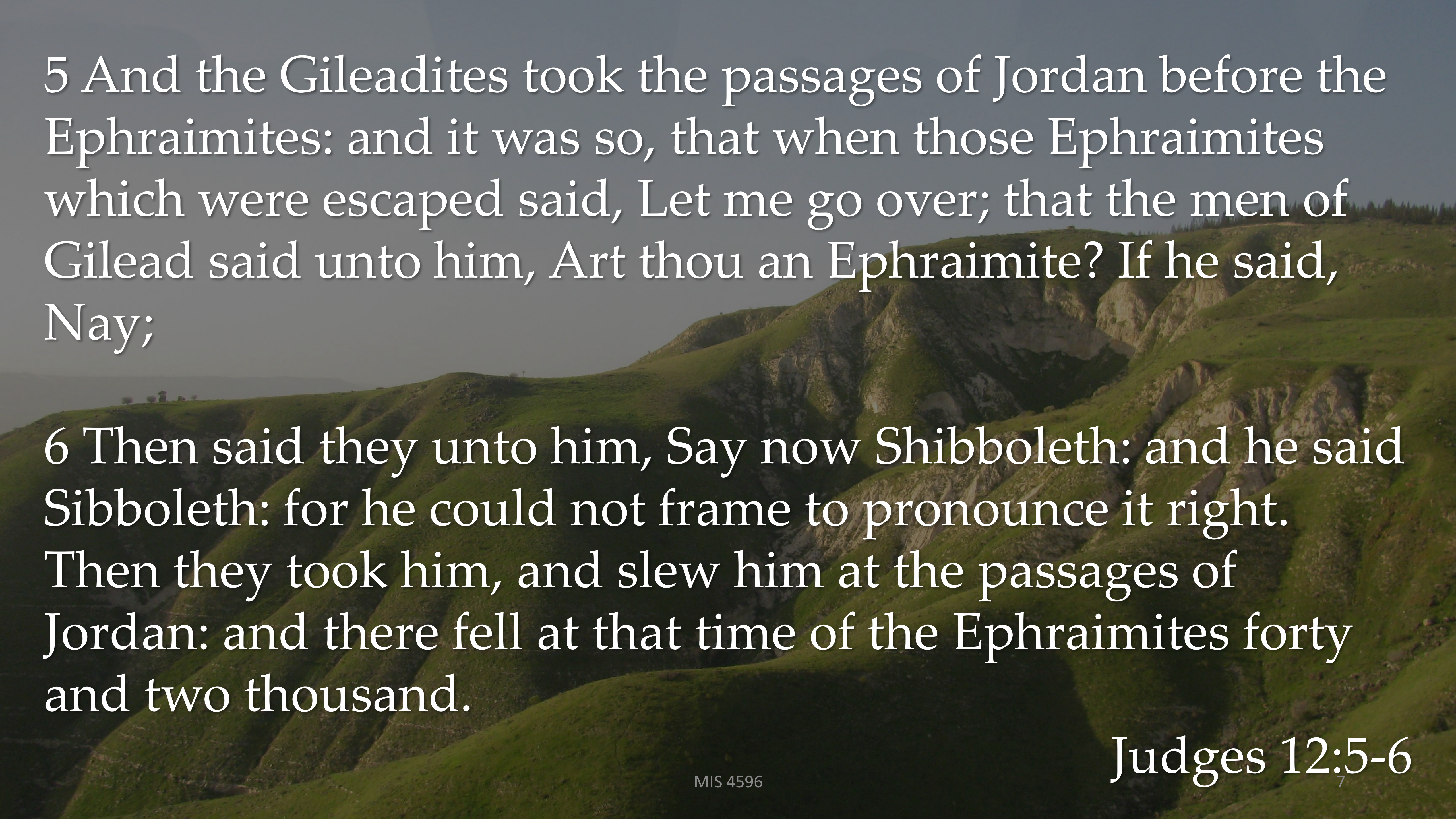
"…is about the continuity of relationships, knowing who to trust and who not to trust, making sense of a complex world"

(Schneier, *Secrets and Lies*, p. 68-69)

- Are ancient problems, a Bible example, from approximately 1100 BC talks about the Gileadites who captured the water crossings of the Jordan river leading to Ephraim…,


Damascus
Bashan
MANASSEH
Ashtaroth
Ramoth Gilead
Yarmuk River
Beth Arbel
Sea of Galilee
Gadara
Beth Yerah
DECAPOLIS
Lo Debar
Jerash
Jabesh Gilead
Jabbok River
Jordan River
Pehel
Beth Shan
J. Umm ed-Daraj
Gilead
Harod Valley
Rift Valle
Penuel/Peniel
Zaphon
Mahanaim
Rabbah (of the Ammonites)
Succoth
Gedor
GAD

1100 BC



5 And the Gileadites took the passages of Jordan before the Ephraimites: and it was so, that when those Ephraimites which were escaped said, Let me go over; that the men of Gilead said unto him, Art thou an Ephraimite? If he said, Nay;

6 Then said they unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right. Then they took him, and slew him at the passages of Jordan: and there fell at that time of the Ephraimites forty and two thousand.

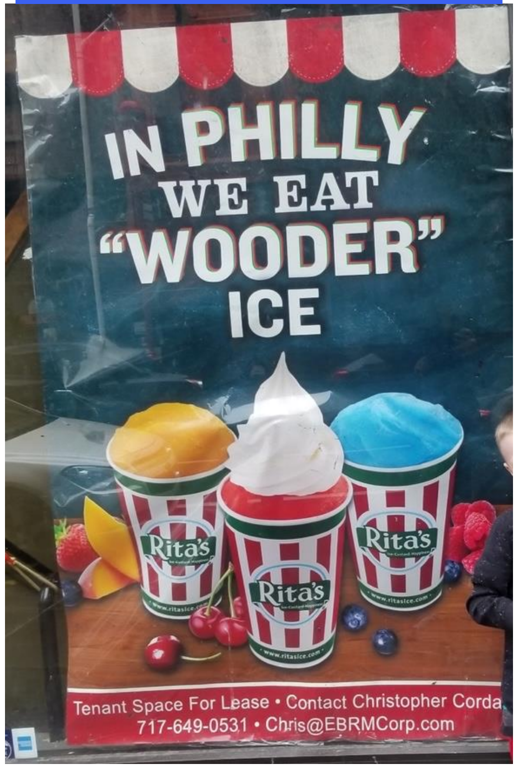
Judges 12:5-6

shibboleth

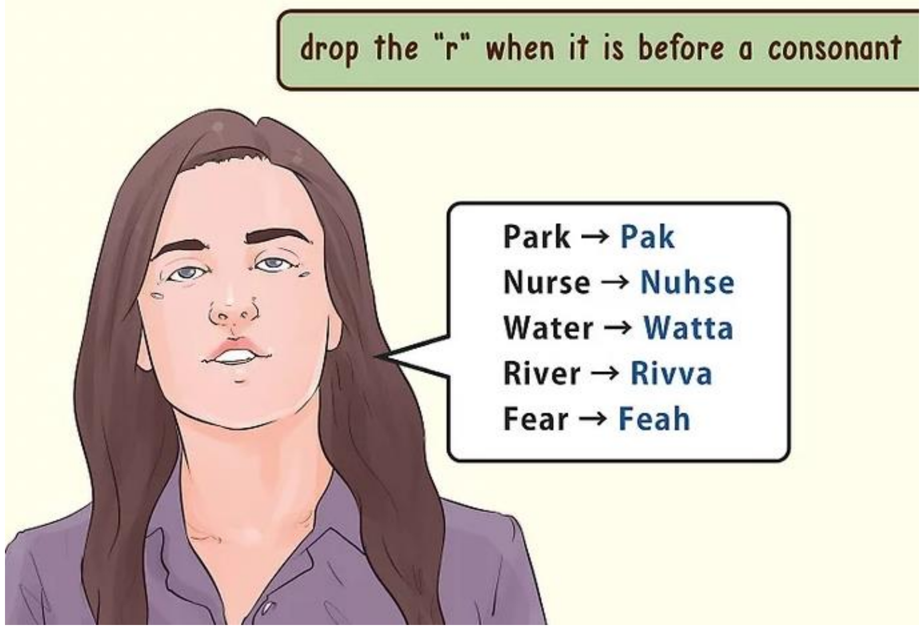
More recently, the word “Shibboleth” has been incorporated into the English language to mean something that distinguishes or identifies someone:

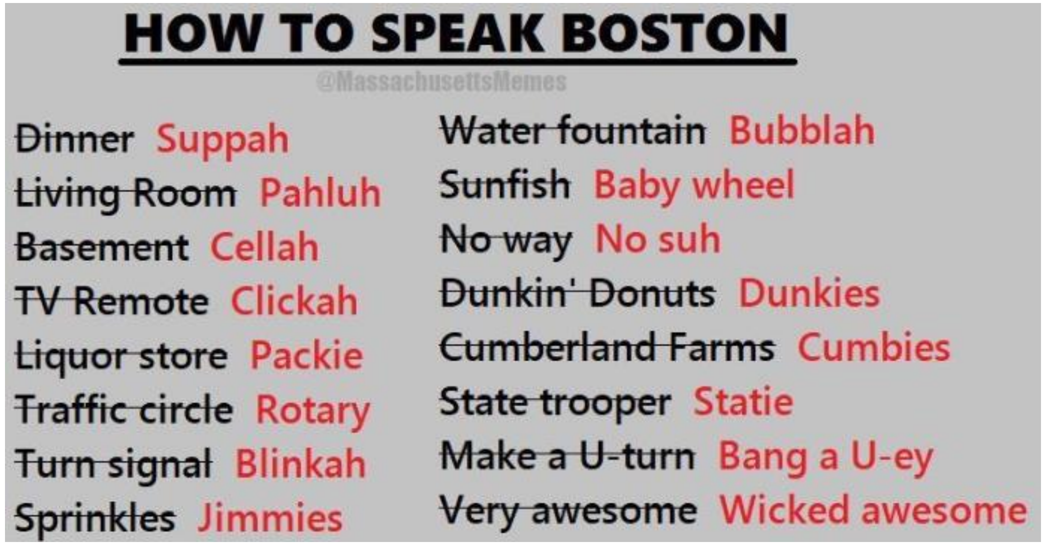
- a peculiarity of pronunciation, behavior, mode of dress, etc., that distinguishes a particular class or set of persons

You drink "wooder" not "water"


IN PHILLY
WE EAT
“WOODER”
ICE
Rita's
Rita's
Rita's
Tenant Space For Lease • Contact Christopher Corda
717-649-0531 • Chris@EBRMCorp.com

Talking like a stereotypical New Yorker





HOW TO SPEAK BOSTON

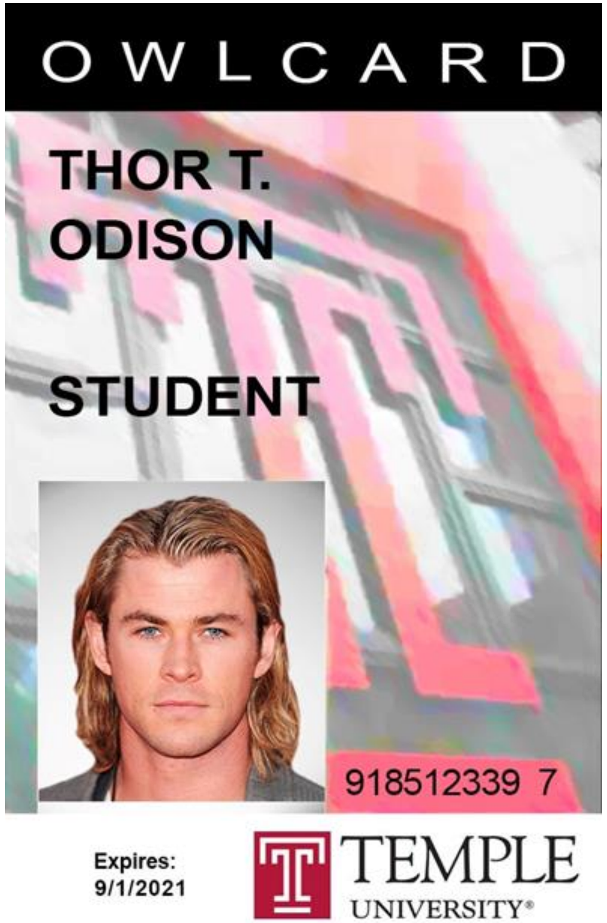
@MassachusettsMemes

~~Dinner~~	Suppah	~~Water fountain~~	Bubblah
~~Living Room~~	Pahluh	~~Sunfish~~	Baby wheel
~~Basement~~	Cellah	~~No way~~	No suh
~~TV Remote~~	Clickah	~~Dunkin' Donuts~~	Dunkies
~~Liquor store~~	Packie	~~Cumberland Farms~~	Cumbies
~~Traffic circle~~	Rotary	~~State trooper~~	Statie
~~Turn signal~~	Blinkah	~~Make a U-turn~~	Bang a U-ey
~~Sprinkles~~	Jimmies	~~Very awesome~~	Wicked awesome

Question:

When you enter Speakman or Alter Hall and show/swipe your Temple ID, what is happening?

- *Identification ?*
- *Authentication ?*
- *Authorization ?*



OWLCARD

THOR T.
ODISON

STUDENT

918512339 7

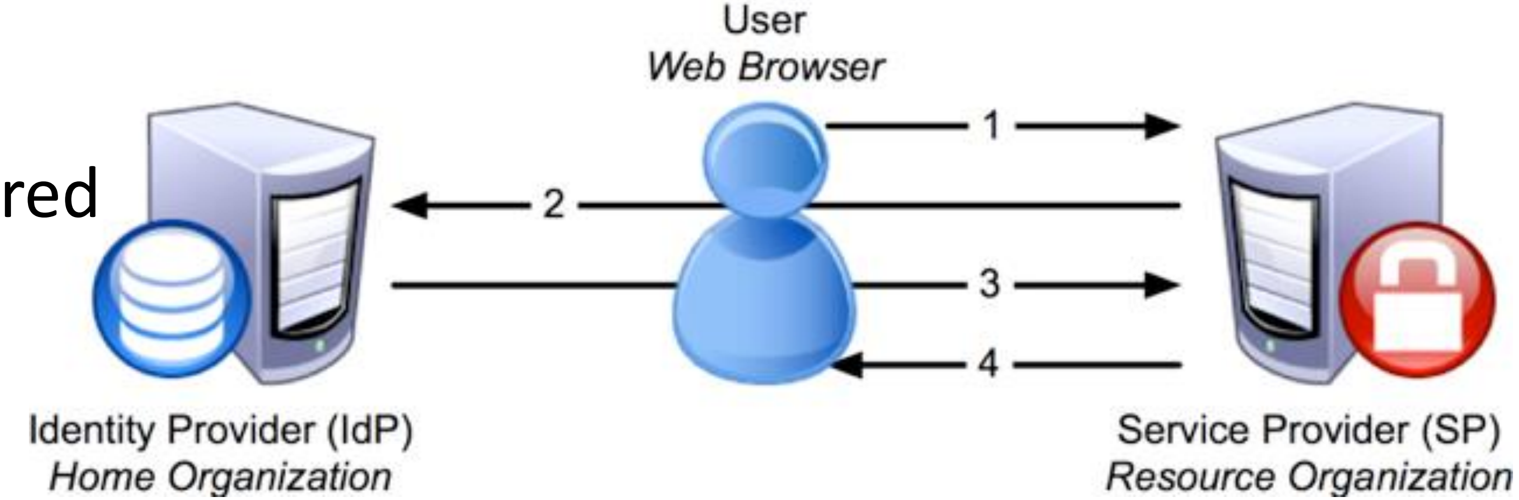
Expires:
9/1/2021

TEMPLE
UNIVERSITY®

shibboleth

In today’s information technology a shibboleth is a single shared community-wide password that enables members of that community to access an online resource without revealing their individual identities

We no longer believe a shared password is safe



Controlling Access to IT Assets

- A central theme of information system security
- Many different security controls work together to provide access control
  - Identity, Authentication, Authorization, Auditing…
- IT Asset includes:
  - Information
  - Systems
  - Devices
  - Facilities
  - Personnel

Identity Management

Identification and Authentication are distinct functions

Identification: Who you say you are

Authentication: Confirmation that you are who you say you are

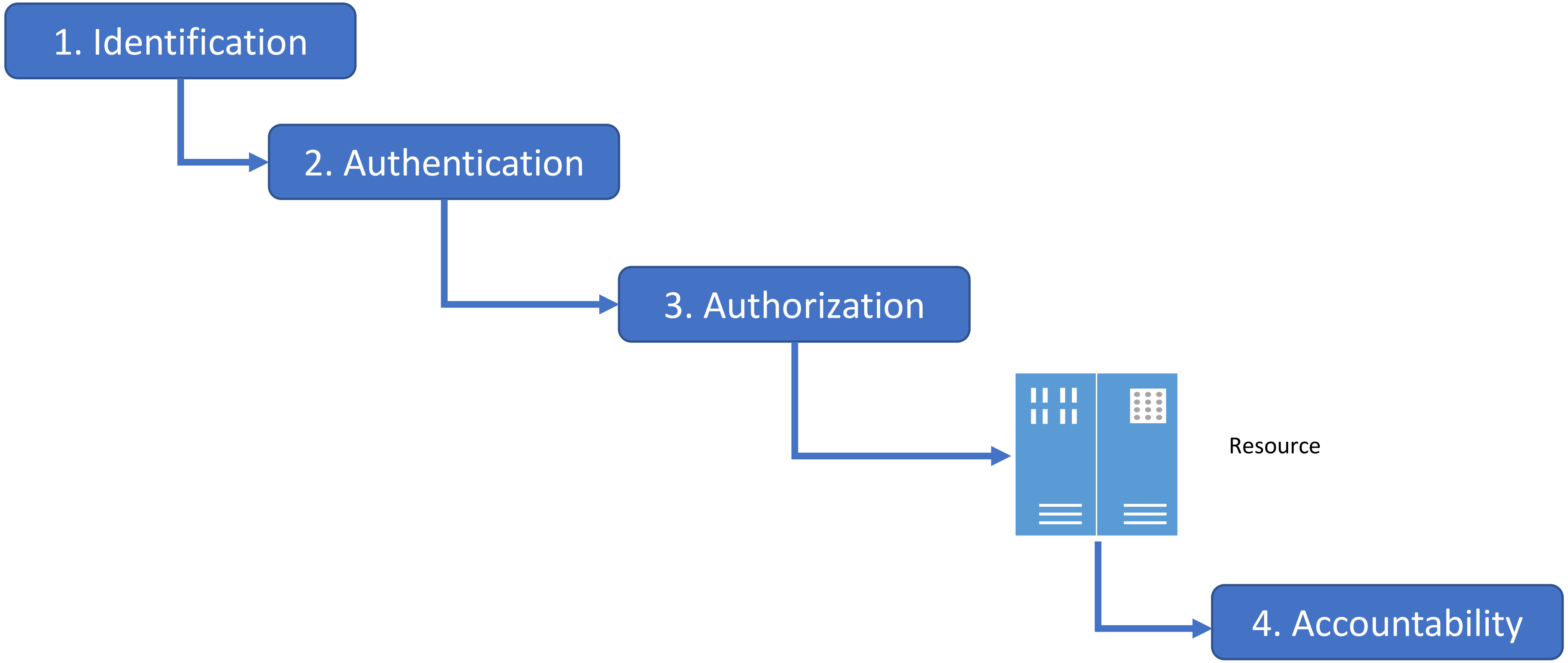
Identity and Authentication

First line of defense in battling unauthorized access to network resources and systems

- Broad term covering several types of mechanisms that control access to features of networks, computers and information stored and flowing within them

Identification, Authentication, Authorization, and Accountability ("AAA")

To access an information system resource, a user must pass through the following logical steps:



1. Identification

2. Authentication

3. Authorization

4. Accountability

Authorization: Access to information…

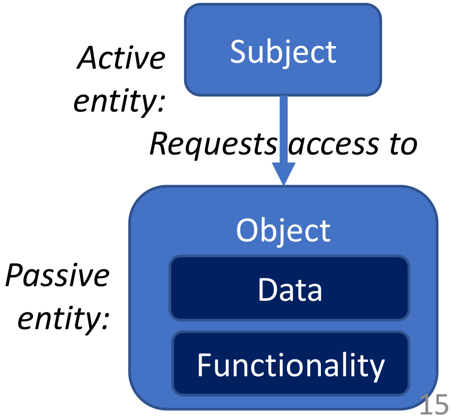
Access is the ability to create a flow of information between user and system

The flow of information between a <u>subject</u> and an <u>object</u>

- Subject
  - Always the active entity - requesting access to an object or data within the object
  - Can be users, programs, processes, services, computers…
  - When authorized, subjects can modify objects
- Object
  - Always the passive object - providing information to active subjects
  - Can be data files, databases, computers, programs, processes, services, storage media…

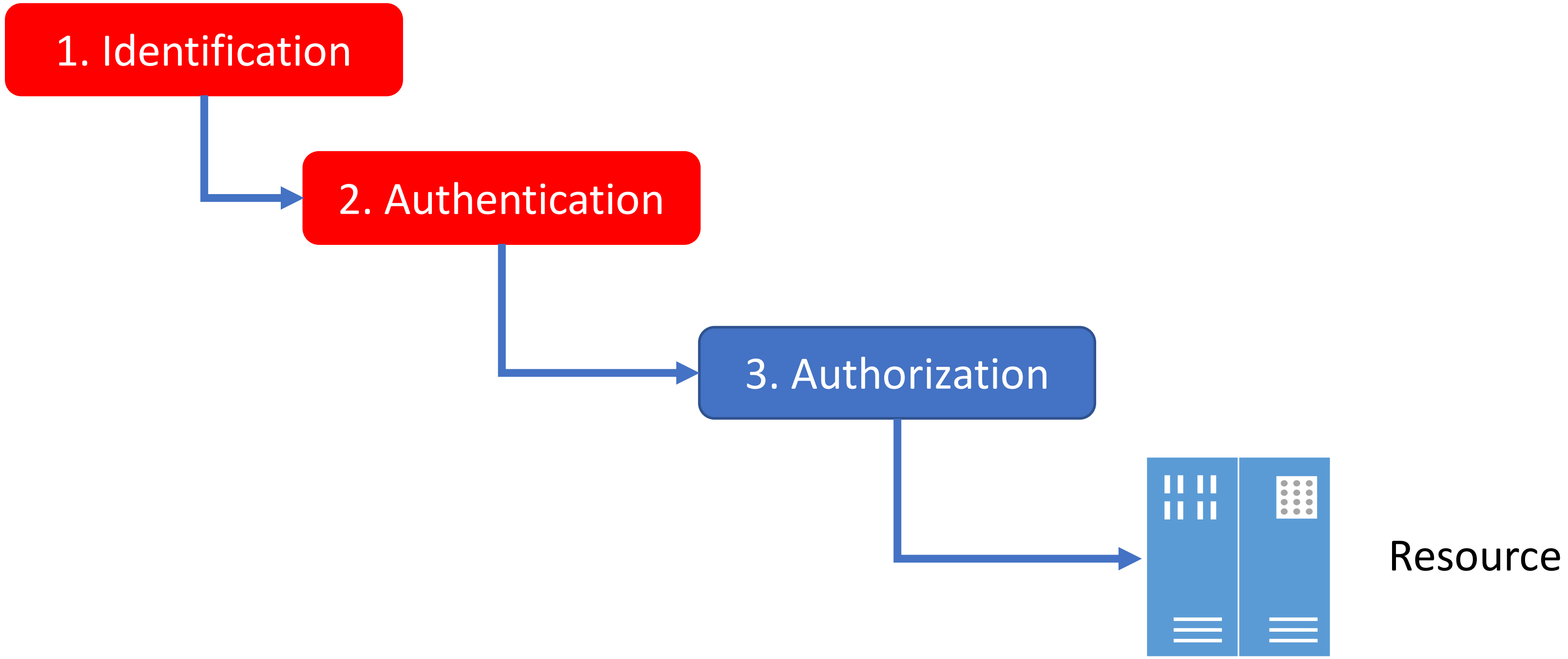
E.g. “***A user (subject) accesses an object (data file)***”

Note: *Roles of subject and object can switch during interactions – e.g. a computer program can be both a data requester and a data provider, switching back and forth*



To access a network's resource, a user must:

Prove their identity (i.e. has the necessary credentials)



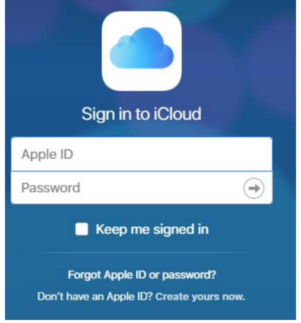
Identification and Authentication

Usually involves a two-step process:

1. **Identification:** Entering public information
    - Method by which a subject (user, program or process) claims to have a specific identity
        - *Username, employee number, account number, or email address*

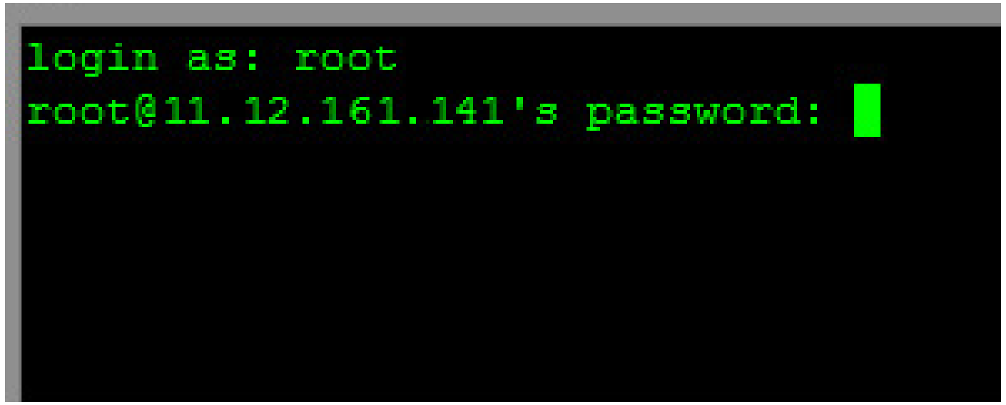
2. **Authentication:** Entering private information
    - Individual's identify must be verified during authentication process
    - Method by which subject proves it is who it says it is
        - *Static password, smart token, one-time password, or PIN*

Identification


Sign in to iCloud
Apple ID
Password
Keep me signed in
Forgot Apple ID or password?
Don't have an Apple ID? Create yours now.

Method of establishing the subject's identity

- *Subject can be a human user, program or process*
- **Identity** – A set of attributes that uniquely describe a person within a given context
- Typically a user name, email address or other public information



```
login as: root
root@11.12.161.141's password: 
```

Identification

USER ID

means

User Identification

Entering public information

- Method by which a subject (user, program or process) supplies identifying information to claim they have a specific identity
  - *Username, employee number, account number, or email address*

Creating secure identities involves 3 key aspects:

1. **Uniqueness** – every user, program or process must be identified with an identifier (i.e. unique ID) that is specific to the individual for accountability
2. **Non-descriptive** – Identifier should not indicate the purpose of the account nor the user’s position nor tasks done with the account
3. **Issuance** – provided by an authority as a formal/official means of proving identity

Authentication

The process of establishing confidence in the identity of users or information systems

Multi factor authentication
Something you have
Something you are
Something you know

Method of proving identity is something a person:

1. **Knows** – a secret password
2. **Has** – a public key certificate, Computer Access Card, …
3. **Is or does** – biometrics

Authentication – Classic 3 factor paradigm

…for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

1. Something the subject knows (“authentication by knowledge”) – Type 1 factor

- Examples: password, PIN, combination to a lock…
- Usually least expensive method to implement
- Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. Something the subject has (“authentication by ownership”) – Type 2 factor

- Examples: Key, swipe card, access card, badge…
- Common for accessing facilities, sensitive areas, and authenticate holder
- Vulnerability: Can be lost or stolen and result in unauthorized access

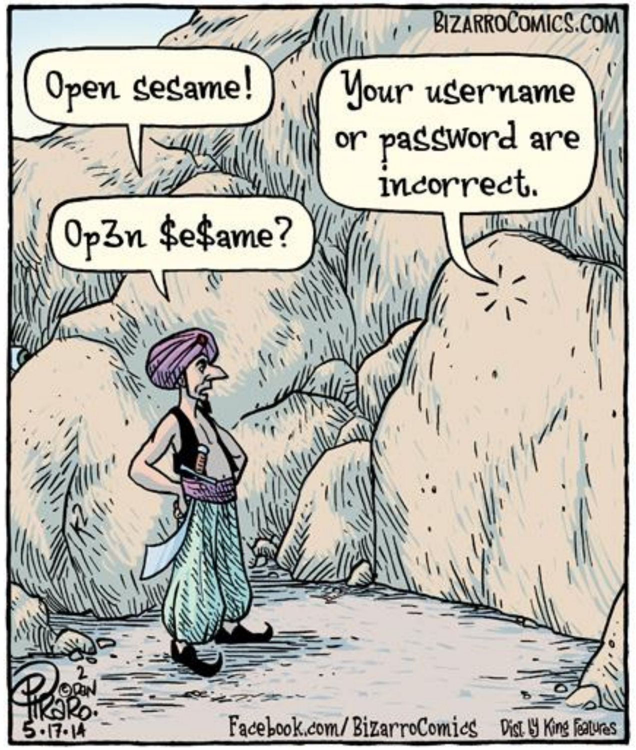
3. Something the subject is (“authentication by characteristic”) – Type 3 factor

- Examples: Fingerprint, palm scan, retina scan…
- Based on biometrics – a way to identify the subject by a unique physical attribute
- Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection

Authentication – Something you know

Use of secret words to authenticate humans dates at least as far back as the military of ancient Rome (Polybius, 118 BC), which developed a careful procedure for using daily “watchwords” to prevent infiltration

Also appears in the folk tale of Ali Baba and the forty thieves (translated into English in 1785) who used the phrase “open sesame” to access a magic cave



Authentication – something you know

Passwords

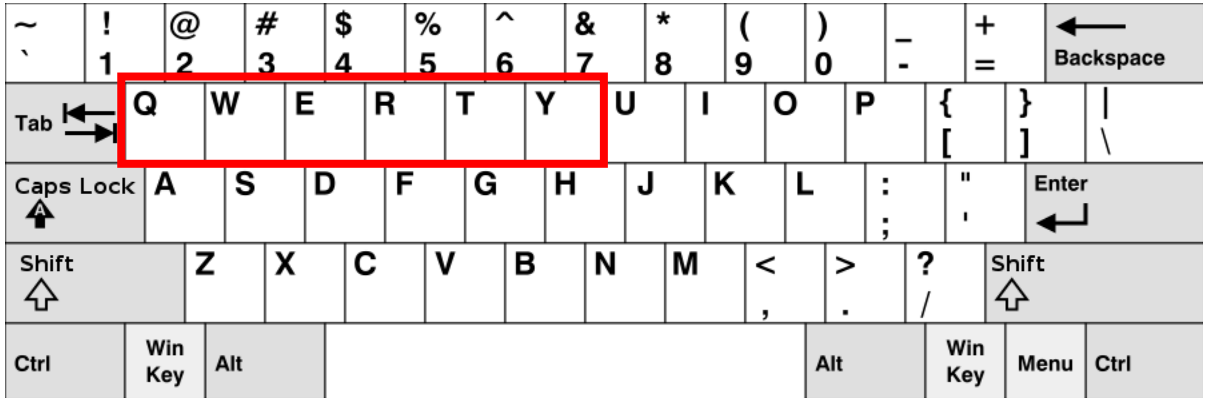
- A secret shared between user authentication system
- User name + password most common identification, authentication scheme
  - *A weak security mechanism – requiring implementation of strong password protections*

Authentication - Passwords

How many unique characters can be produced by the standard QWERTY keyboard?

Standard US Qwerty keyboards have 101, 104 or 107 keys which can produce 96 unique characters

- *26 lower case letters*
- *26 upper case letters*
- *10 numbers*
- *32 visible symbols*
- *2 Windows and Menu keys*



~ ` ! 1 @ 2 # 3 $ 4 % 5 ^ 6 & 7 * 8 (9) 0 _ - + = Backspace
Tab Q W E R T Y U I O P { [}] | \
Caps Lock A S D F G H J K L : ; " ' Enter
Shift Z X C V B N M < , > . ? / Shift
Ctrl Win Key Alt Alt Win Key Menu Ctrl

"The name comes from the order of the first six keys on the top left letter row of the keyboard (Q W E R T Y). The QWERTY design is based on a layout created for the Sholes and Glidden typewriter and sold to E. Remington and Sons in 1873. It became popular with the success of the Remington No. 2 of 1878, and remains in widespread use."

Wikipedia

Authentication – Classic 3 factor paradigm

…for authentication systems

Subject provides information to prove it is who it says it is and authentication system verifies the identification information

1. Something the subject knows (“authentication by knowledge”) – Type 1 factor

- Examples: password, PIN, combination to a lock…
- Usually least expensive method to implement
- Vulnerability: Someone else may acquire this knowledge and gain unauthorized access to a resource

2. Something the subject has (“authentication by ownership”) – Type 2 factor

- Examples: Key, swipe card, access card, badge…
- Common for accessing facilities, sensitive areas, and authenticate holder
- Vulnerability: Can be lost or stolen and result in unauthorized access

3. Something the subject is (“authentication by characteristic”) – Type 3 factor

- Examples: Fingerprint, palm scan, retina scan…
- Based on biometrics – a way to identify the subject by a unique physical attribute
- Vulnerability: Can be expensive, cumbersome/troubling to users and associated with false acceptance or rejection

Authentication - Passwords

How to create a password that is hard to crack:

- The longer the password, the harder it is to crack
- Always use a combination of characters, numbers and special characters
- Variety in passwords on different apps and systems…

https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref

- 1 character password: 96 tries to crack
- 2 characters: 96 *96 = 9,216
- 3 characters: 96 * 96 * 96 = 884,736
- 4 characters 96^4 = 84,934,656
- …
- 8 characters 96^8 = 7,213,895,789,838,336

LAST
WEEK
TONIGHT
WITH JOHN OLIVER

Authentication: Passphrase

This is a relatively complex password: cCs,.ebj7L}c

But it is difficult to remember

Passphrase

- Is a sequence of characters that is longer than a password
- Takes the place of a password
- Can be more secure than a password because it is more complex

This passphrase is easier to remember:

I like to eat chocolate chip cookies.

Use of random words in passphrase is better:

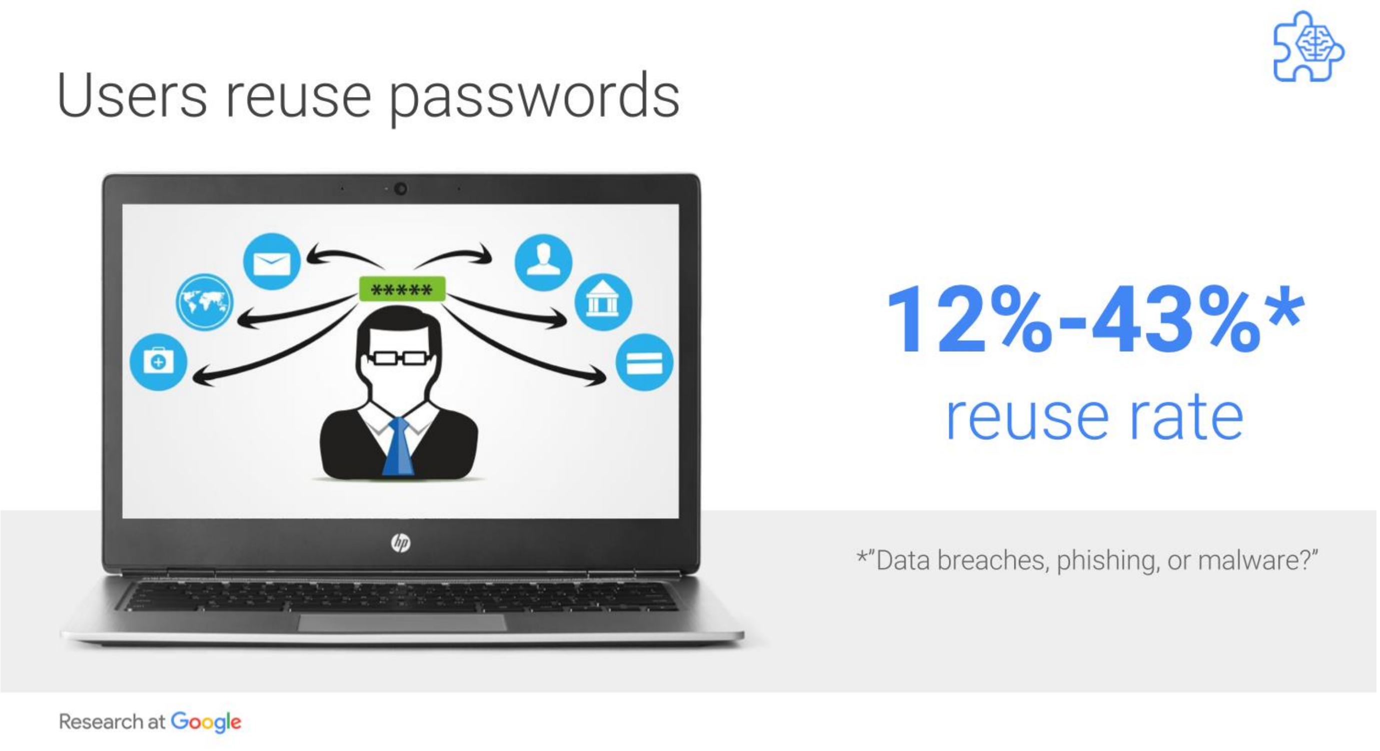
Correct horse battery staple

“The reuse of passwords is the #1 cause of harm on the internet”

https://www.cnet.com/news/facebook-chief-security-officer-alex-stamos-web-summit-lisbon-hackers/

According to a study of 29 million people, 38% reused their passwords

https://arxiv.org/pdf/1706.01939.pdf



Users reuse passwords

12%-43%*
reuse rate

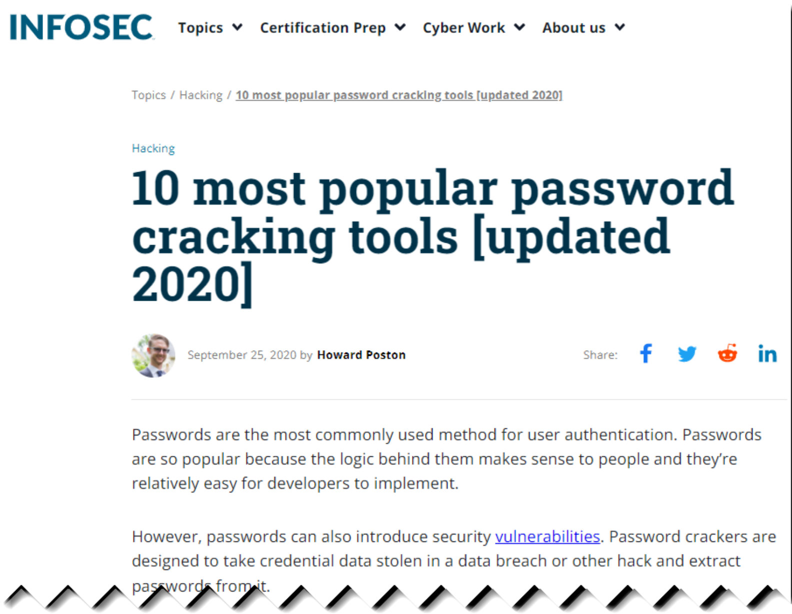
*"Data breaches, phishing, or malware?"

Research at Google

https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf

Techniques to attack passwords

- Guessing
- Social engineering
- Dictionary attacks
- Electronic monitoring
- Access the password file
- Brute force attacks
- Rainbow tables



Topics / Hacking / 10 most popular password cracking tools [updated 2020]

Hacking

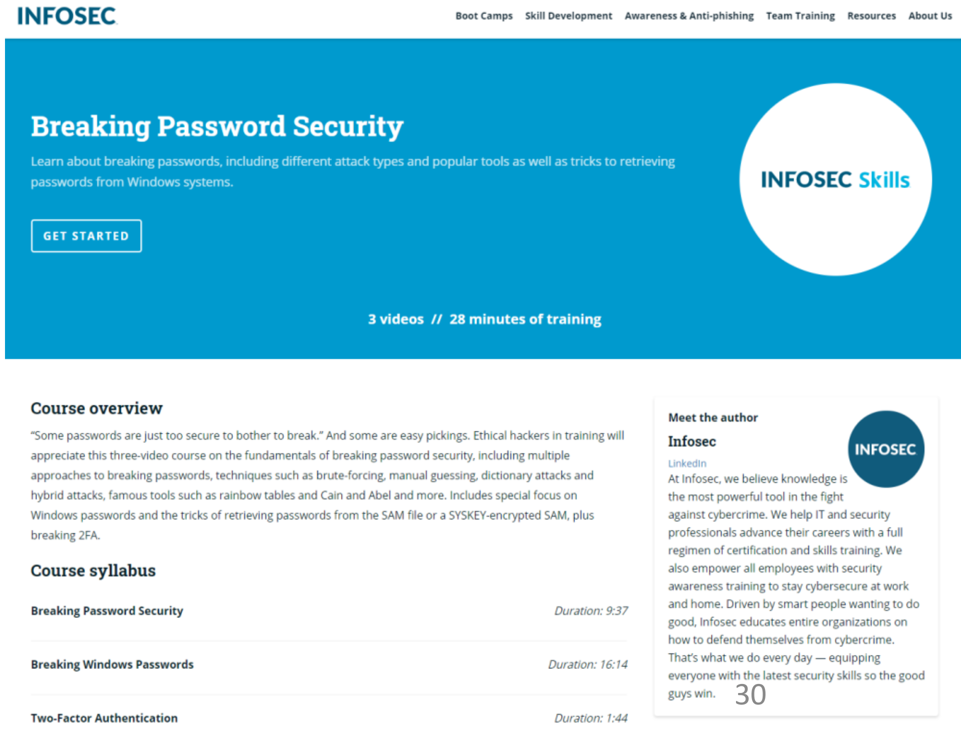
10 most popular password cracking tools [updated 2020]

September 25, 2020 by **Howard Poston**

Passwords are the most commonly used method for user authentication. Passwords are so popular because the logic behind them makes sense to people and they're relatively easy for developers to implement.

However, passwords can also introduce security vulnerabilities. Password crackers are designed to take credential data stolen in a data breach or other hack and extract passwords from it.

https://resources.infosecinstitute.com/10-popular-password-cracking-tools/#gref



Breaking Password Security

Learn about breaking passwords, including different attack types and popular tools as well as tricks to retrieving passwords from Windows systems.

3 videos // 28 minutes of training

Course overview

"Some passwords are just too secure to bother to break." And some are easy pickings. Ethical hackers in training will appreciate this three-video course on the fundamentals of breaking password security, including multiple approaches to breaking passwords, techniques such as brute-forcing, manual guessing, dictionary attacks and hybrid attacks, famous tools such as rainbow tables and Cain and Abel and more. Includes special focus on Windows passwords and the tricks of retrieving passwords from the SAM file or a SYSKEY-encrypted SAM, plus breaking 2FA.

Course syllabus

Breaking Password Security	*Duration: 9:37*
Breaking Windows Passwords	*Duration: 16:14*
Two-Factor Authentication	*Duration: 1:44*

Meet the author

Infosec

LinkedIn

At Infosec, we believe knowledge is the most powerful tool in the fight against cybercrime. We help IT and security professionals advance their careers with a full regimen of certification and skills training. We also empower all employees with security awareness training to stay cybersecure at work and home. Driven by smart people wanting to do good, Infosec educates entire organizations on how to defend themselves from cybercrime. That's what we do every day — equipping everyone with the latest security skills so the good guys win.

Authentication: Passwords with Password Managers

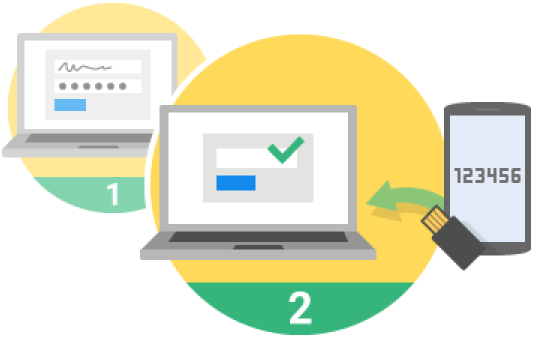
Keeping all of your passwords in a password manager is a good idea

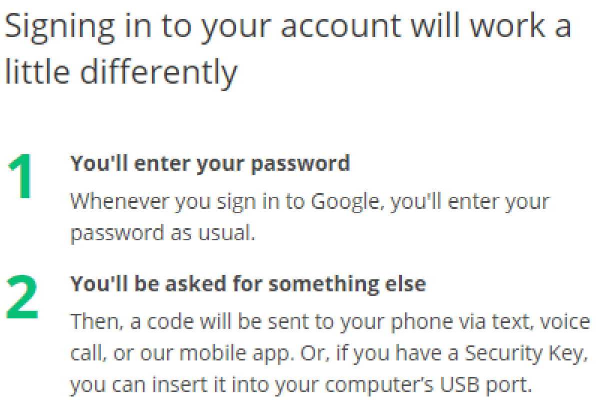
- https://en.wikipedia.org/wiki/1Password
- https://en.wikipedia.org/wiki/LastPass
- https://fossbytes.com/best-free-password-manager-software/
- https://www.techradar.com/best/password-manager

Authentication - something you have

e.g.

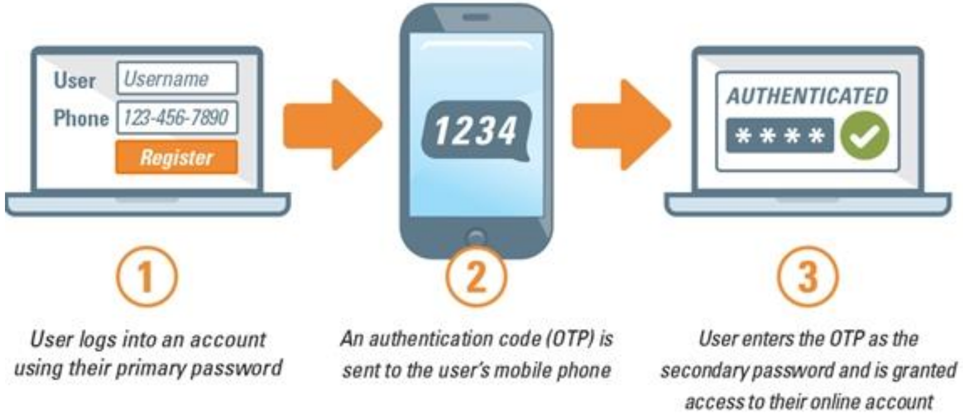
- Your phone
- ID Card
- Synchronous token
  - Time Based
  - Counter Synchronization




Signing in to your account will work a little differently

1 **You'll enter your password**
Whenever you sign in to Google, you'll enter your password as usual.

2 **You'll be asked for something else**
Then, a code will be sent to your phone via text, voice call, or our mobile app. Or, if you have a Security Key, you can insert it into your computer's USB port.



1. User logs into an account using their primary password
2. An authentication code (OTP) is sent to the user's mobile phone
3. User enters the OTP as the secondary password and is granted access to their online account

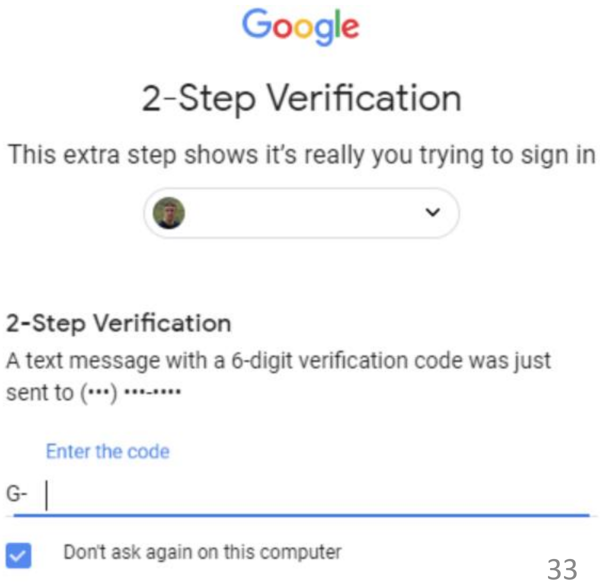
…something you have: Cell phone

The number one thing most people can do to protect themselves online is to enable any type of two-factor authentication for their important accounts

2-factor authentication requires you to have 2 things to get into your account, often it consists of:

1. Something you know (your password)
2. Something you have
    1. Your mobile device with security code

- SMS stands for Short Message Service, the most widely used type of text messaging
- When you enable SMS-based 2-factor authentication, the service will send your mobile phone number a text message containing a one-time code whenever you sign in from a new device
- If someone has your username and password for the related account, they cannot sign into your account without access to your text messages



Google

2-Step Verification

This extra step shows it's really you trying to sign in

2-Step Verification

A text message with a 6-digit verification code was just sent to (•••) •••-••••

Enter the code

G-

☑ Don't ask again on this computer

Something you have: Cell phone

SMS-based 2-factor authentication is better than nothing, but still not ideal because someone could steal your phone number or intercept your text messages

For example,

An attacker could impersonate you and move your phone number to a new phone

- In a “Port-out scam” a criminal pretends to be you and moves your current phone number to another cellular carrier
- In “SIM hijacking”, an attacker moves your phone number from your current SIM card to the attacker’s SIM card

This is a big problem!

- Many online accounts, including bank accounts, use your phone number as a two-factor authentication method. They won’t let you sign in without sending a code to your phone first.

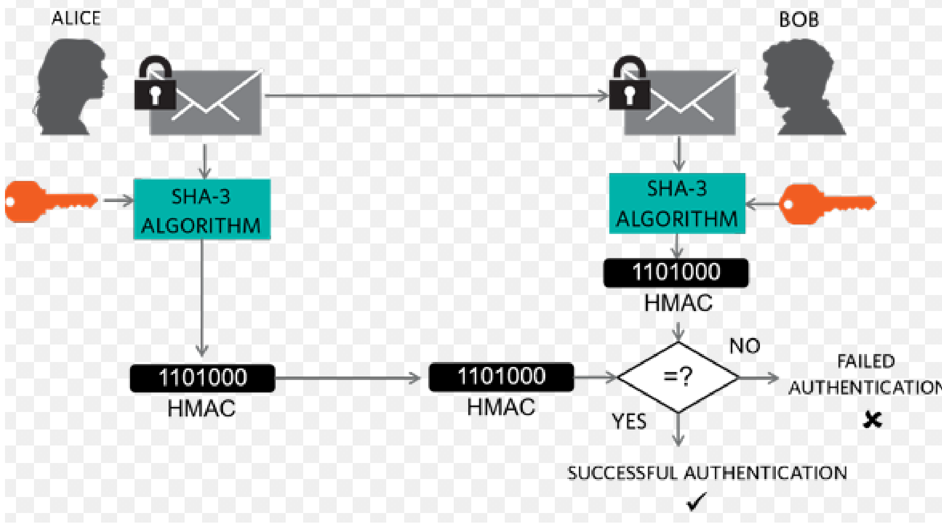
But, after the porting scam or SIM hijacking has taken place, the attacker will receive that security code on their phone. They can use it to gain access to your financial accounts and other sensitive services.

Something you have: Cell phone

- SMS-based 2-factor authentication is not ideal because someone could steal your phone number or intercept your text messages
  - It’s one of the weaker things that you can have to authenticate, because your phone number is actually “something you lease” from the phone company, you don’t actually own or control it
- For example, in the most likely attack
  - An attacker could impersonate you and move your phone number to a new phone in a phone number porting scam
- Alternatively, an attacker could intercept SMS messages intended for you
  - For example, they could spoof a cell tower near you, or a government could use its access to the cellular network to forward and capture your messages

Something you have: Cell phone with one-time codes

- Hash (HMAC)-based one-time password (HOTP), https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm



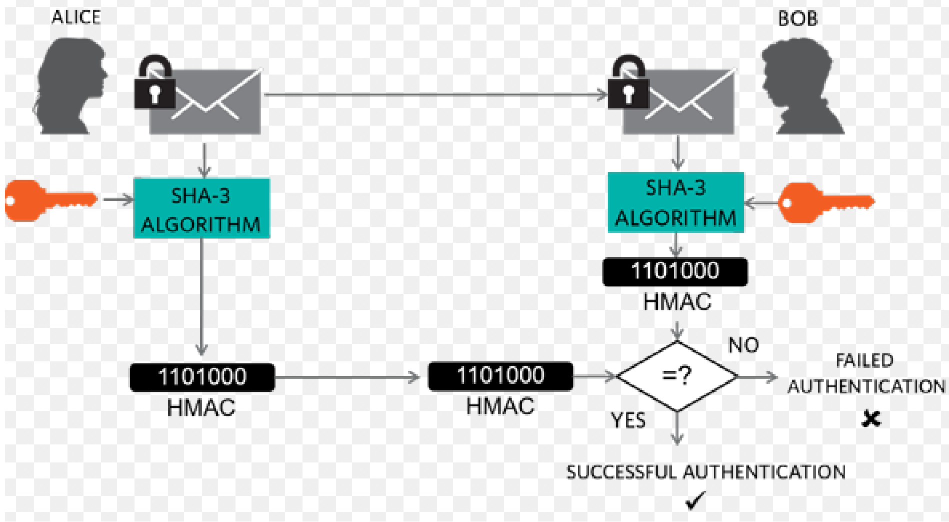
HMAC = Hash Message Authentication Code

1. Message is concatenated with a symmetric key (not encrypted)
2. The combination is hashed resulting in a HMAC
3. The HMAC is appended to the message and sent to the receiver
4. The receiver concatenates the message with the symmetric key
5. The receiver hashes the combination and compares it to the HMAC received with the message, if the HMACs match the message is authenticated

Note: Authenticity and Integrity are achieved, but confidentiality is not

Something you have: Cell phone with one-time codes

- Hash (HMAC)-based one-time password (HOTP), https://en.wikipedia.org/wiki/HMAC-based_One-time_Password_algorithm



- Time-based one-time password (TOTP), https://en.wikipedia.org/wiki/Time-based_One-time_Password_algorithm

- Drawback is that these can be phished, intercepted, and man-in-the-middle attacked

Something you have: Universal Second Factor (U2F) security keys

- U2F security keys turn web authentication on its head
  - *Instead of the user having to authenticate to the website, U2F requires websites to authenticate to the U2F token*
- It takes people out of the authentication equation, making phishing impossible
- Google eliminates phishing of its employees requiring all employees to use U2F

https://en.wikipedia.org/wiki/Universal_2nd_Factor

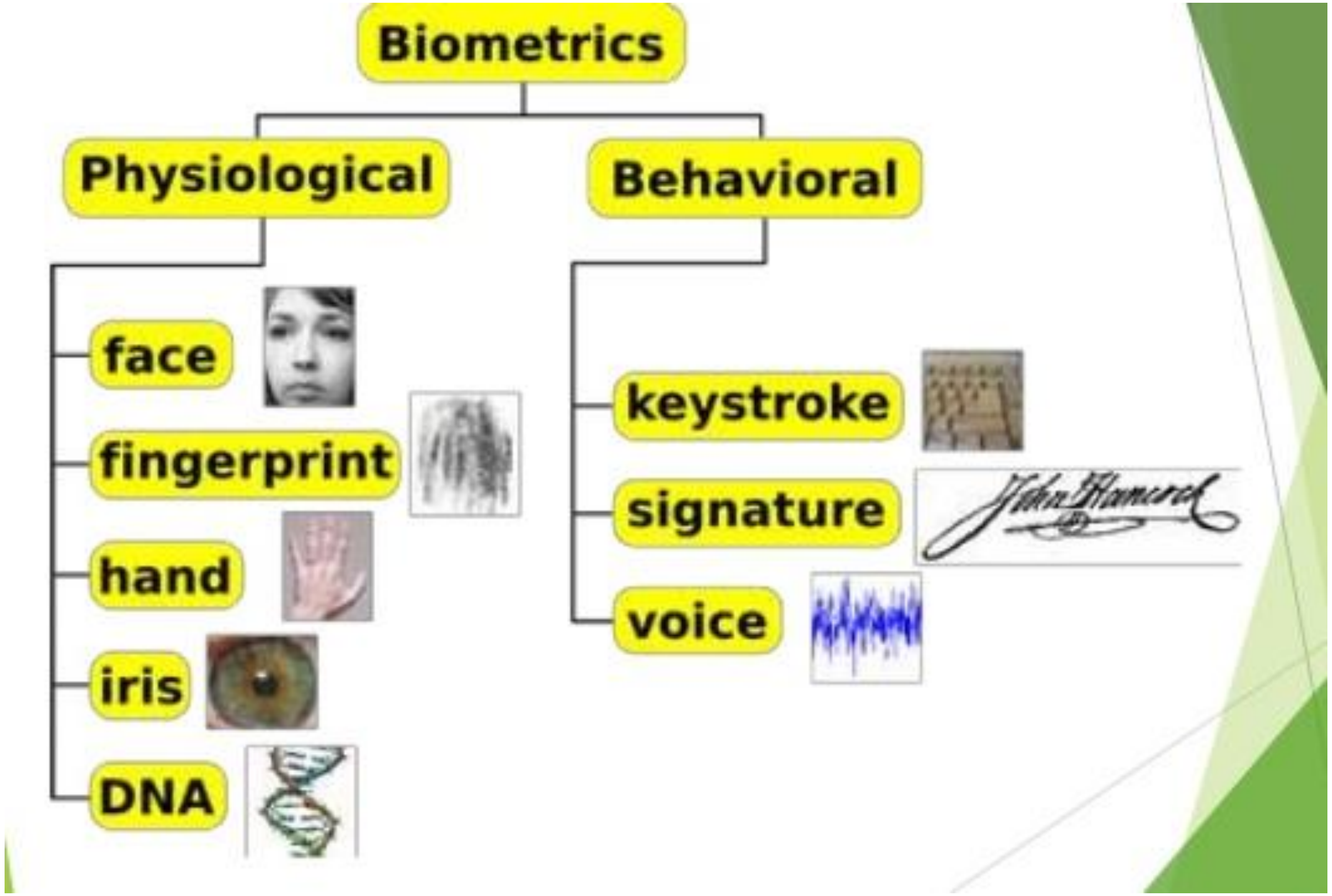
- Sites that let you use U2F: https://www.dongleauth.info

Authentication – something you are or do ("Biometrics")

- Verifies an identity by analyzing a unique person attribute or behavior
- Most expensive way to prove identity, also has difficulties with user acceptance
- Many different types of biometric systems

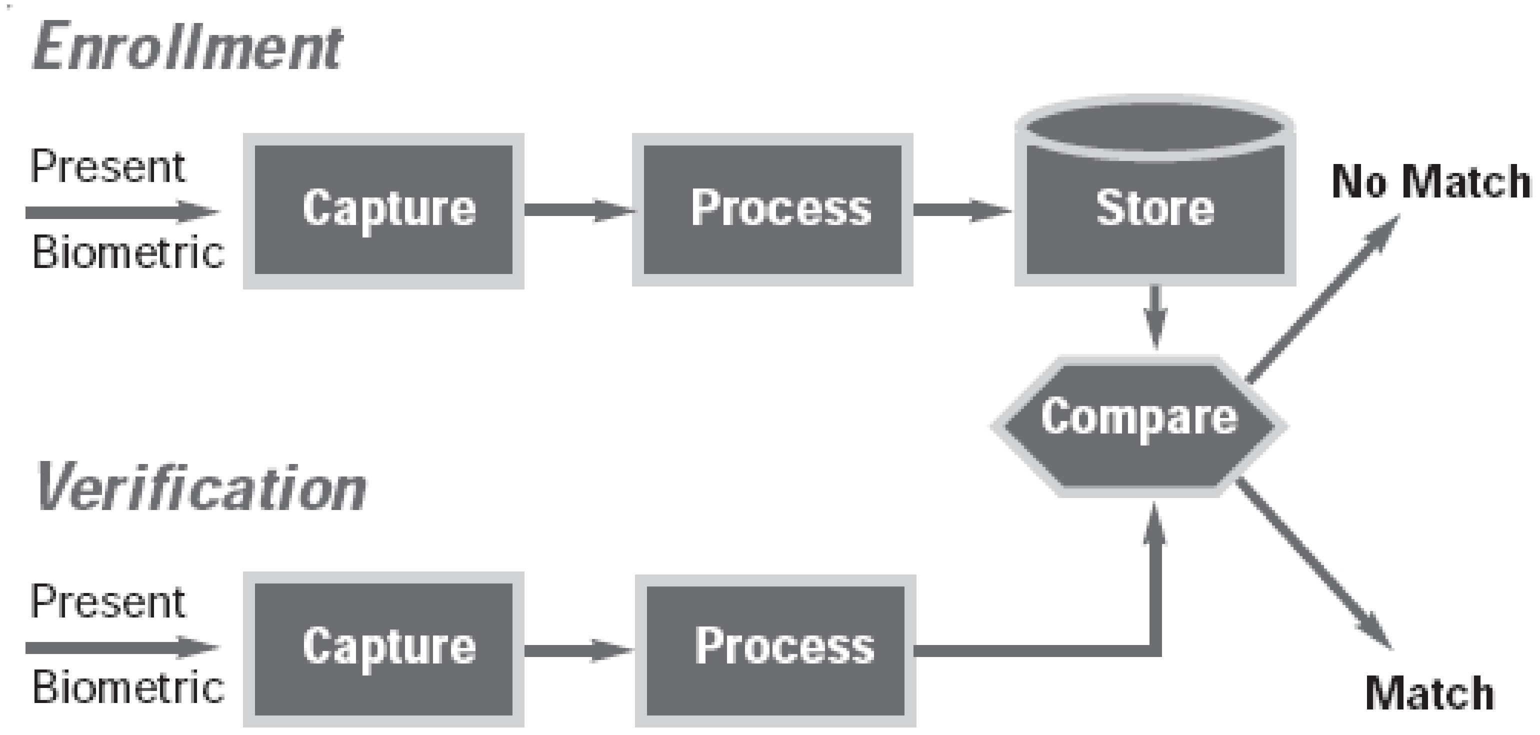
Authentication

Most common biometric systems:



Authentication – Biometric Systems

During identity verification (i.e. authentication) the biometric system scans personal’s physiological attribute or behavioral trait and compares the captured data to a record created in an earlier enrollment process



Scanning fingerprint from display

Bkav®
Bkav

Authentication: Multi-factor

Multi-factor authentication refers to use of >1 factor:

Something the subject knows ("authentication by knowledge")

+

Something the subject has ("authentication by ownership")

+

Something the subject is ("authentication by characteristic")

Authentication system strength determined by the number of factors incorporated into the systems

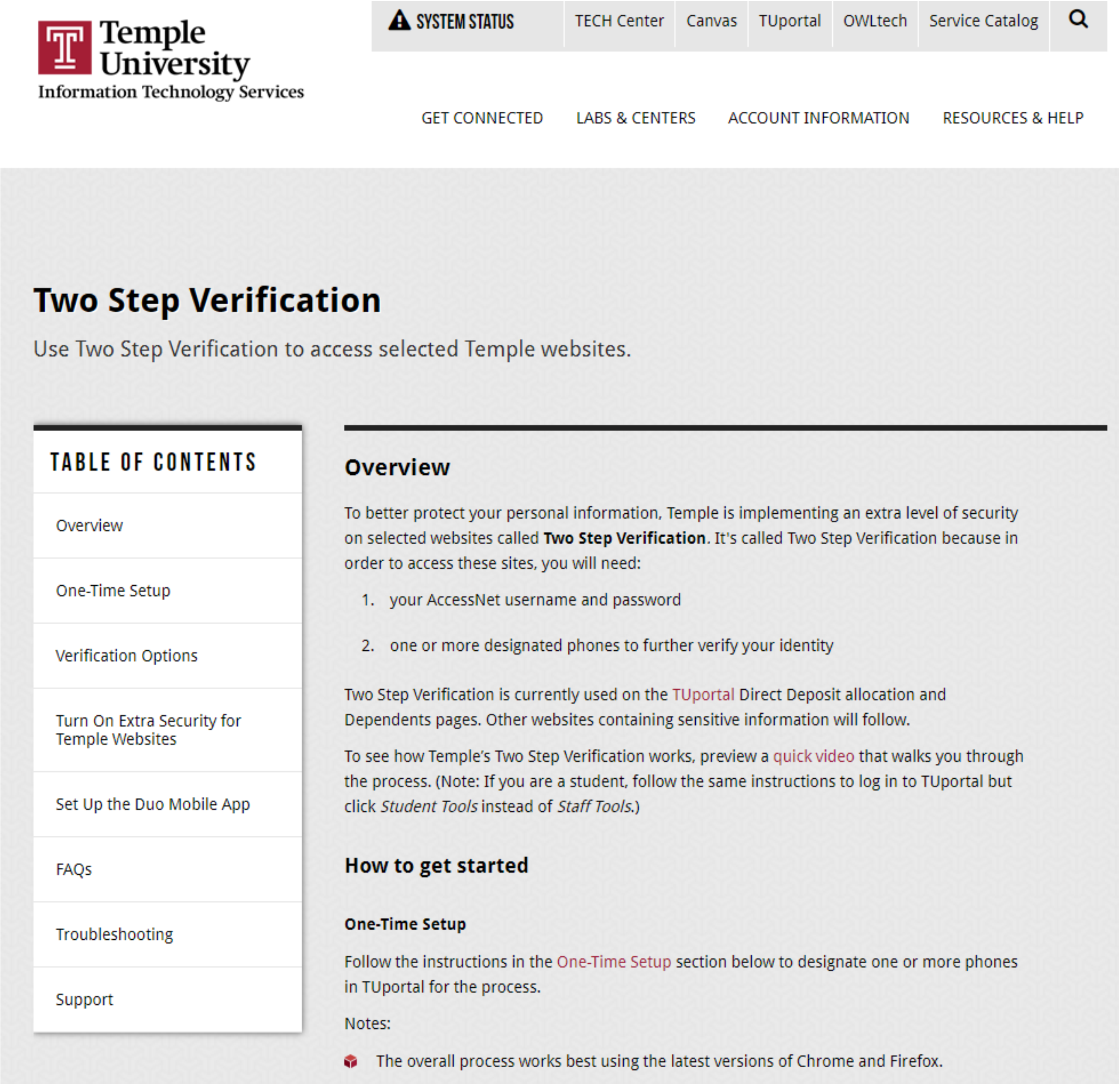
- Implementations that use 2 factors are considered stronger than those that only use 1 factor
- Systems that incorporate all 3 factors are stronger than systems that incorporate 2 factors

Example: An ATM machine requires both something you have (the ATM card) and something you know (the PIN)

- *Both the card and pin on their own are weak*
- *Together they are strong!*

Authentication: Multi-factor

https://its.temple.edu/two-step-verification#128831



Two Step Verification

Use Two Step Verification to access selected Temple websites.

TABLE OF CONTENTS

Overview

To better protect your personal information, Temple is implementing an extra level of security on selected websites called **Two Step Verification**. It's called Two Step Verification because in order to access these sites, you will need:

1. your AccessNet username and password
2. one or more designated phones to further verify your identity

Two Step Verification is currently used on the TUportal Direct Deposit allocation and Dependents pages. Other websites containing sensitive information will follow.

To see how Temple's Two Step Verification works, preview a quick video that walks you through the process. (Note: If you are a student, follow the same instructions to log in to TUportal but click *Student Tools* instead of *Staff Tools*.)

How to get started

One-Time Setup

Follow the instructions in the One-Time Setup section below to designate one or more phones in TUportal for the process.

Notes:

- The overall process works best using the latest versions of Chrome and Firefox.

Agenda

- ✓RSA Asymmetric Encryption Lab
- ✓Identity and Authentication – a historic problem
- ✓Identity and Authentication for controlling access to IT Assets
- ✓Identification
- ✓Authentication
  - ✓Something you know
  - ✓Something you have
  - ✓Something you are
- ✓Multi-factor Authentication