CHEAT SHEETS

IAM Bootcamp 2024

1. Importance of IAM

1.1 Zero Trust

- Every time someone wants to access data or perform a particular operation, regardless of whether they are internal or external, this person will have to authenticate and be authorized before they can continue.
- Zero-trust is based on **two key factors**: **authentication and encryption**. Although this model is not easily implemented in traditional network setups, it has gained more and more traction as it fits cloud-driven environments quite well.

- The first principle of Zero Trust is to assume threats will always come from the outside or within your environment and that your network will always be a hostile area.
- Nowadays, the perimeter is highly extended with the integration of the cloud, third parties, remote teleworkers, and data centers.
- This leads to the following principle: **every user, device, and network connection must prove that it is allowed to get access before it is given access.**
- You must assume that your network is hostile, all traffic should be logged and inspected.
- One of the first principles of zero trust was that the network is hostile, and you cannot trust things just because they are inside the network.
- A way to implement this is to authenticate and encrypt all traffic, end to end. This ensures that unknown devices cannot connect to the assets you control.

- Zero Trust typically focuses on several principles. The **National Institute of Technology (NIST)** has released a standard that includes defining a model based on:

  - Identity: role and privileges of a specific account.
  - Credentials: authentication principles such as passwords and keys.
  - Access management: policy to control who has access from where.
  - Operations: how to monitor and maintain zero trust architectures and what approval flows are required.
  - Endpoints: the distinction between the trust level of different systems.
  - Hosting: this could be your private data center or a public cloud environment.
  - Connectivity: how connections are made between devices and if that connection is trusted by default.

- Let's see how this works with a web server that has standard TLS implemented. You deploy a server certificate on the server. This is to ensure users that they connect to a valid server. This is different for the server as it cannot verify whether the connection is from a legitimate or malicious user.
- Fortunately, TLS supports mutual authentication. The client and server will verify each other before establishing a connection. A rogue device will no longer be able to connect to the server. As a result, in this scenario, you already have one condition: to establish a trusting relationship between these components.

2. Some Definitions

Digital Identity is the online person of a subject. A single subject can have multiple digital identities for different services.

Identification is the process of claiming to be a specific individual. Typing in a user ID is a form of identification

Authentication is a process in which a subject proves they possess one or more valid authenticators associated with an identity.

YOU KNOW → **Something you know**

By remembering a piece of information and presenting it, you can prove that you are who you say you are. The best example of something you know is a password.

YOU HAVE → **Something you have**

By possessing something, you can prove that you are a specific entity. Token-based schemes, in which you carry a token that generates a new password, are examples of something you have.

YOU ARE → **Something you are**

By presenting a unique attribute tied to your physical makeup. This is often called biometrics. Hand scans, thumbprints, and retina scans are all examples of biometrics.

2.1 Identity Governance

"Identity Governance and Administration (IGA), also known as identity security, is at the center of IT operations, enabling and securing digital identities for all users, applications, and data. It allows businesses to provide automated access to an ever-growing number of technology assets while managing potential security and compliance risks." [3]

2.2 Identity Access Management

"Identity management is the organizational process for identifying, authenticating and authorizing individuals or groups of people to have access to applications, systems or networks by associating user rights and restrictions with established identities." [4]

[3] What is Identity Governance and Administration (IGA)? | SailPoint
[4]https://searchsecurity.techtarget.com/definition/identity-management-ID-management

Authorization is the process of determining what a subject is allowed to do or access after authentication. **Authorizations should be based on the principle of least privilege, where an entity is given only the minimal access needed to do the job.**

Accountability is the process of identifying who did what on the system and when they did it.

Zero Standing Privileges (ZSP) [2] is a security principle that advocates removing all persistent user privileges within an enterprise's estate. Practically Zero Standing Privileges are a progression from the concept of just-in-time access. This control reduces risk by preventing a user from accessing the system by removing all entitlements until temporary access is authorized and granted.

Just In Time Access (JIT Access) [1]
JIT Access helps organizations provision access so that users only have the privileges to access privileged accounts and resources **when they need it and not otherwise at any other time**. Instead of granting always-on (or standing) access (or standing access), **JIT Access limit access to a specific resource in a particular timeframe.** This granular approach mitigates the risk of privileged account abuse by significantly reducing the time a cyber attacker or malicious insider has to gain access to privileged accounts before moving laterally through a system and gaining unauthorized access to sensitive data.

JIT Access can be seen as a way used to enforce the principle of least privilege to ensure users and non-human identities are given the minimum level of privileges. JIT Access can also ensure that privileged activities are conducted by an organization's Identity Access Management (IAM), IT Service Management (ITSM), and Privileged Access Management (PAM) policies, along with its entitlements and workflows.

[1] https://www.cyberark.com/what-is/just-in-time-access/
[2] https://www.cyberark.com/what-is/zero-standing-privileges/

3. Authentication

Authentication is a process in which a subject proves they possess one or more valid authenticators associated with a subscribed identity. During authentication, the subject is referred to as the claimant. The verifier checks the validity of the authenticator.

3.1 Authenticator Assurance Levels (AAL)

Depending on the sensitivity of the resource being accessed and the context of the access request, the user can be asked to provide a different level of user authentication. NIST outlines three different Authenticator Assurance Levels (AAL) with varying degrees of proofing requirements.

AAL1

Requires either single-factor or multifactor authentication using a wide range of available authentication technologies.

AAL2

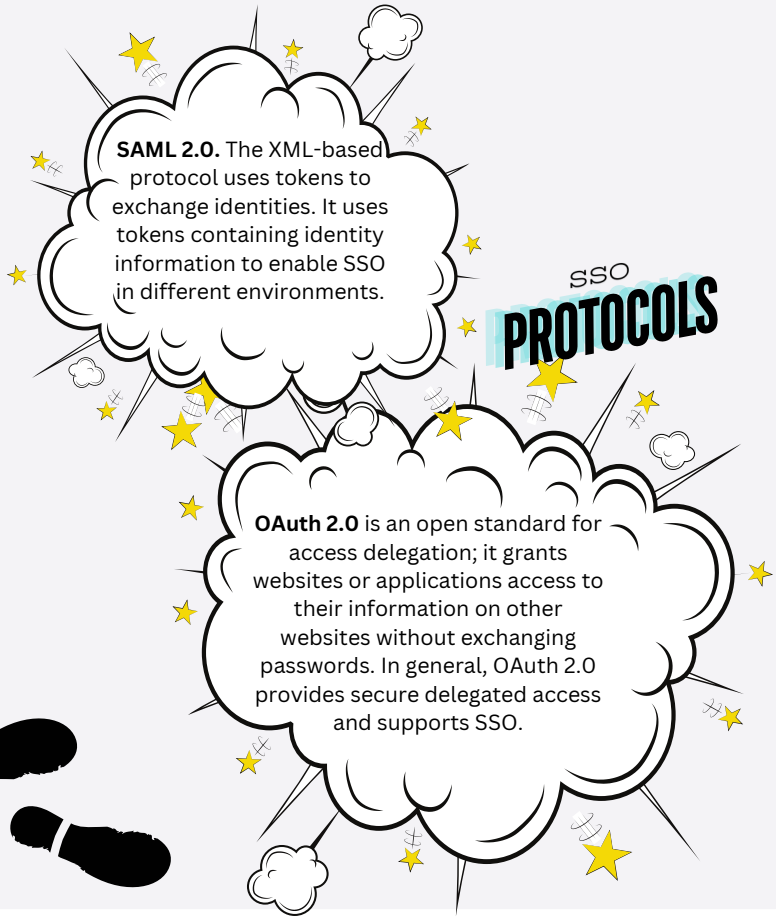
Proof of possession and control of two different authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are needed at AAL2 and above.

AAL3

Requires (1) a hardware-based authenticator and (2) an authenticator that provides verifier impersonation resistance; the same device may fulfill both these requirements.

3.2 Single Sign On (SSO)

Allows a user to log on once with one set of credentials and use those credentials to access different resources. It can be implemented using a central directory service (LDAP or Microsoft Active Directory) or tickets where credentials are stored (Kerberos).



4. Authentication Types

The authentication process requires the claimant to provide one or more of these types of authenticators, also known as authentication factors.

4.1 Authentication Factors

SOMETHING YOU **KNOW**

A Memorized Secret authenticator, commonly referred to as a password or, if numeric, a PIN, is a secret value intended to be chosen and memorized by the user.

CSP
Credential Service Provider
A trusted entity that registers subscriber authenticators and issues electronic credentials to subscribers. A CSP may be an independent third party.

SOMETHING YOU **HAVE**

An authenticator can be any object only the authorized party possesses and can prove it is in their possession, as outlined in the NIST Digital Identity Guidelines:

- **Look-Up Secrets :** It is a physical or electronic record that stores a set of secrets shared between the claimant and the **CSP** [5]." An example of a look-up secret would be a printed card with a table of authentication codes.
- **Out-of-Band Devices:** It is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel.“ An example of an out-of-band device is a mobile phone receiving a text message with a secret code.

SOMETHING YOU **ARE**

This category includes any provable characteristic that is unique to the authorized party, such as a fingerprint. Biometrics are gradually finding their way into our lives more and more these days. The most common types are fingerprint scans and facial recognition (e.g., on your mobile phone), retina scans, and voice recognition. Often, a biometric authentication system builds in some degree of error margin, as a given biometric reading is never identical to the ones performed prior. Therefore, it is not recommended to use a biometric authenticator as a main authentication mechanism; rather, it should be a second factor on of another authenticator (something you know or something you have).

One-Time Password (OTP) Tokens

- **Single Factor OTP:** A single-factor OTP device generates OTPs. This category includes hardware devices and software-based OTP generators installed on mobile phones. These devices have an embedded secret used as the seed for generating OTPs and do not require activation through a second factor. The OTP is displayed on the device and manually input for transmission to the verifier, thereby proving possession and control of the device".
- **Multi-Factor OTP:** A multi-factor OTP device generates OTPs for authentication after activation through an additional authentication factor. This includes hardware devices and software-based OTP generators installed on mobile phones. An example of a multi-factor OTP token is a multi-factor authentication app on your mobile phone.

Cryptographic Devices

- **Single-factor cryptographic devices.** A single-factor cryptographic device is a hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second authentication factor. Authentication is accomplished by proving possession of the device via the authentication protocol (i.e. YubiKey).
- **Multi-factor software cryptographic authenticator.** A multi-factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second authentication factor. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message.

[5] https://www.exabeam.com/explainers/insider--threat/howthreat/how--mfamfa--fatiguefatigue--attacksattacks--

4.2 Multifactor Authentication

- Multi-factor authentication is a method in which access is only granted after being presented with more than one authenticator.
- Often, MFA combines a shared secret (something you know) with an OTP token (something you have) or biometrics (something you are).

4.3 Adaptative Authentication

- Adaptative authentication is the general term for using the context of a request to determine the required authentication level. In an adaptative authentication mechanism, the party requesting access must provide one or more authenticators, depending on the context of their request and the sensitivity of the resource they are attempting to access.
- To do this, the verifier can derive the IALs (Identity Assurance Levels) and AALs (Authenticator Assurance Levels) as defined earlier and apply different pre-assigned policies to each level.
- Many different factors can be used to determine the IAL or AAL required to access a particular resource, of which a few (location, behavior, timing, etc.) have been listed in the slide above. Please note that this list is non-exhaustive, and each verifier should decide which factors to base a specific access requirement.

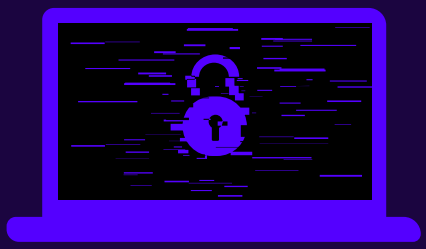
5. Authentication Attacks

5.1 MFA Fatigue Attack

Multi-factor authentication (MFA) fatigue attack, also known as MFA bombing or MFA spamming, is a type of social engineering cyberattack where the attacker repeatedly sends MFA requests to the victim's email, phone, or other registered devices. This attack aims to coerce the victim into confirming their identity via notification, which would authenticate the attacker's attempt to access the victim's account or device. [5]

5.2 Cookie Hijacking

Method by which webmasters break into other websites to steal cookies. This allows them to watch the victim's browsing activity, log their keystrokes, gain access to credit card information and passwords, and more. Cookie hijacking attacks mainly involve injecting JavaScript code into a website by embedding it in the HTML of an otherwise authentic-looking email or advertisement. This malicious code is then executed by the browser when you visit the infected site; it will display an endless series of popups that may be used for phishing purposes to steal your login credentials or other sensitive information. [6]



[6] https://www.exabeam.com/explainers/insider-threat/how-mfa-fatigue-attacks-work-6-ways-to-defend-against-them/
[7] https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack

6. Access Control

It is the broader concept of controlling access to resources and managing this access. Additionally, constant monitoring is needed to ensure access is revoked when it is no longer needed.

Controlling Access. A proper restriction of access rights is enabled by the combination of:

- Least Privilege. Give someone the least amount of access they need to do their job.
- Need to know. Restrict access to only the information required for their job, and no more.

What happens when minimal access is granted and is still too risky?

In those cases, separation of duties needs to be implemented. A given task is split between two individuals such that no single individual can execute a specific action, either by error or with ill intentions.

Separation of duties works; however, the more people work together, the greater the chance they will conspire to accomplish fraudulent actions. To minimize the chance of this occurring, rotation of duties is also an option to consider. This is where people are rotated out of specific jobs at set intervals, so the chance of two people colluding is minimized.

6.1 Access Control Techniques

DAC
Discretionary Access Control

Consists of something the user can manage, such as a username or password. For example, a user might give a document password to someone without notifying the administrator.

MAC
Mandatory Access Control

It Is a type of access control that controls access to all resources via system-enforced credentials that are nontransferable by the authorized party. MAC requires all system users to be assigned a clearance and all data to be assigned a classification level. Users cannot give their clearance to another person.

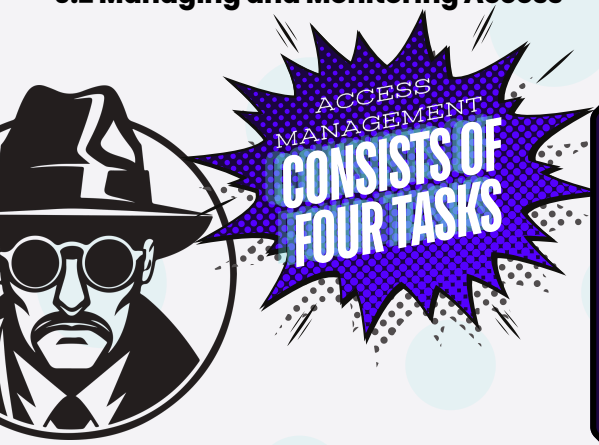
RBAC
Role Based Access Control

It is discretionary or mandatory access control that assigns users to roles or groups based on their organizational functions. Groups are assigned authorization to perform tasks on specific data.

LBAC
Lattice-Based Access Control

It is a mandatory access control that defines access restrictions on the interactions between subjects and objects. A subject is only allowed to access an object if the security level of said subject is greater than or equal to that of the object.

6.2 Managing and Monitoring Access



Privileged Access is access to a computer system with elevated access rights, such as root or administrator access or access to service accounts.

As organizations grow, their number of privileged accounts grows with them. Often, the number of accounts to be managed is enormous, which makes it challenging to keep a good overview of who has access to what. Their proliferation poses other problems, such as using identical passwords or generic user IDs, sharing user accounts, and other harmful practices that weaken the resilience of such accounts to attacks. This, combined with the fact that these privileged accounts are very tempting targets for an adversary, means that proper management of these credentials is vital to ensure the security of the organization's IT infrastructure.

1

Account Administration is a set of processes and controls. The account administrator enrolls a user, assigns authenticators, and assigns authorizations. In practice, this can be performed by multiple teams—for example, where HR does enrollment, authenticators are provided by the team managing the Active Directory, and the application management team assigns authorizations. The process should embed communication of good practices to the user.

2

Maintenance is the process of reviewing account data and spot-checking for inconsistencies or errors. Periodically, account management staff should review and update lists of users and authorizations and validate these with the business for appropriateness. Review should occur automatically when employees transfer departments or locations or are assigned new or different duties.

3

Monitoring is system administrators should log both successful and failed attempts to log on to the system. Logging of the use of systems resources (files, programs, printers, and so on) should be enabled based on risk assessment of the value of those resources. These logs should be reviewed—for example, as part of SOC (Security Operations Center) operations.

4

Revocation account management staff and system administrators should promptly revoke privileges when they are no longer needed, especially for users who have been fired.

6.3 Privileged Access Management (PAM) Tools

PAM enable an organization to regulate who can get privileged access to their critical systems.

01

Provide transparency to the user.
Where possible, the PAM tool will take the authentication process out of the user's hands. The user will interact with the PAM tool, which will, in turn, authenticate them to the service and log the authentication attempt.

02

Policy enforcement point
Privileged Access Management tools also allow organizations to set strict rules on access and password policies. The PAM tool enforces password policies and limits privileged access. For example, it can only connect from this device to the management interfaces of other systems within your network.

03

Generate strong shared secrets
Choosing a strong password is complex. A PAM tool will take this responsibility on itself and generate long, random strings as the password for each privileged account.

04

Securely store credentials
As strong credentials are often tricky to remember, and organizations usually need many of them, the PAM tool will act as a password vault and securely store all credentials.

05

Rotate credentials
Even the best passwords are capable of being found. This means frequently changing a credential for a privileged account is essential. The PAM tool will handle this automatically and change credentials after a set period without user intervention.

06

Monitor and log privileged access
The PAM tool will log any access to privileged accounts for security management to review unusual or unauthorized access.

07

Generate reports
Legislation often requires frequent auditing of all access to privileged accounts. PAM tools will generate audit reports automatically to make the process easier for the organization.

Some examples of popular Privileged Access Management (PAM) tools that are frequently used by organizations:

- **CyberArk**
- **HashiCorp Vault**
- **Entra ID (Formerly known as Azure Active Directory)**

6.4 Active Directory

- **Active Directory (AD)** is Microsoft's directory and identity management service for Windows domain networks. It is used by a variety of Microsoft solutions like Exchange Server and SharePoint Server, as well as third-party applications and services.
- AD is essential for organizing and managing users, their attributes, group membership, computer accounts, network resources, and so on.
- It equips teams with centralized authentication and authorization services.
- AD is designed to check if someone has the proper credentials (authentication) and determines what files or applications they can access based on their role or group membership (authorization).
- In simple terms, AD offers critical features and components like group policy management, domain services, and Lightweight Directory Access Protocol (LDAP) support.
- Domain services provide a hierarchical organizational structure that helps manage interactions between users and devices in distributed networks.
- LDAP, or Lightweight Directory Access Protocol (LDAP), is a protocol that helps users find data about organizations, persons, and more.
- AD enables teams to effectively manage users, computers, additional devices, and other resources from one central location.
- Active Directory stores information as "objects," which are any resources within the network, such as computers, user accounts, contacts, groups, organizational units, and shared folders.
- Objects are categorized by name and attributes. The information is kept in a structured data store optimized to enhance query performance and scalability.

6.5 3-Tiered Privileged Access Management

Users are often logged on as local administrators on their devices. Suppose one of those devices in your network gets infected with malware. In that case, the attacker will usually use that device to harvest the credentials of any user who has previously logged onto that device to move to other devices inside the network.
This is what's called lateral movement.

So, how can you prevent lateral movement?

- First, you should not allow your users to log in with administrative privileges.

- Keep all privileged groups in your Active Directory empty as much as possible.

- Restrict the use of privileged AD accounts.

- Structure your Active Directory so that it uses a tiered administrative model.

The **tiered administration model** separates the administration of end-user workstations and domain controllers. The tiered model is composed of three levels and only includes admin accounts:

- Tier 0 has direct control of enterprise identities in the environment. This tier includes accounts, groups, and other assets used to manage the domain controllers, AD forest, domains, and all its assets.
- Tier 1 can control the enterprise servers and applications. This includes server operating systems, cloud services, and enterprise applications. The administrators have control of a large number of assets.
- Tier 2 controls the user workstations and devices. The administrators in this tier are often part of the helpdesk or other support group.

7. Storing Passwords

Typically, you want to store a password in a unique and irreversible format, which is referred to as password hashing.

Hashing is a one-way transformation of a password (different from encryption, which is two- way) that turns it into a unique string called a password hash. One-way means it's practically impossible to turn that string into the original readable password.
Thanks to current technology, we can calculate multiple hashes in a couple of minutes. This is typically how a user is authenticated without knowing the clear text password. Based on the users' input, the hash is calculated from the clear text password and compared with the hash stored on the system.

7.1 Key Derivation Functions (KDF)

- The first characteristic of a KDF is that it is based on an irreversible hash function. A hash function takes an arbitrary amount of data as its input and uses it to calculate a fixed-length output value called a digest.
- The fascination of hashing the password is that after hashing, the value is entirely unrecognizable, and the original input value cannot be retrieved.
- Another property of essential derivation functions is that they are capable of input transformation, which can be used to obtain keys of a specifically required format. This allows us to create longer, more difficult brute-force keys from potentially weak, shorter passwords. We call this technique **key stretching**.
- To further strengthen the algorithm, we want to ensure that no two stored values are the same, even if users have chosen the same password. This is where a **salt value** comes into the picture. The salt value is a randomly generated string of characters added to each password before hashing it and stored next to the hashed value. Even more secure is a **pepper**, which is, in essence, a salt that is kept secret and stored in a secure location.
- Last, to discourage attempts at password cracking, a KDF implements a so-called difficulty factor. This value makes it intentionally more difficult to calculate the resulting hash to slow down any brute-force guessing attacks.

What Determines the Strength of a Password Hash?

1 Quality of Key Derivation Function

Fundamental principles for a qualitative algorithm are the level of confusion and diffusion. **Confusion** means that the algorithm renders an output very different from the input, and **diffusion** implies generating widely different outputs for closely matching inputs. Many algorithms are believed to be reasonably secure until proven otherwise. Using an algorithm that has been available for a long time and is well-tested is recommended. Good choices are PBKDF2, SHA256, SHA512 bcrypt, scrypt, and Argon2.

2 Password & Derived Key Length

A larger hashing key means that there are more possible keys to uniquely identify the input of the hash function and, therefore, a smaller chance of collisions. Although this is considered the most crucial feature of hashes concerning data integrity, the limited length of passwords employed by users makes key length only a minor contributor when considering the strength of password hashes. Related to password hashes, the key length of a hash could be viewed as a real issue if it cannot uniquely identify all possible passwords within the minimum password length and complexity requirements determined in the company's password policy.

3 Character Set Support

The strength of a chosen password depends heavily on the length of the selected password and the character set used when choosing the password. A seven-character password of a maximum of 26 characters results in 8 billion possible passwords (which is generally easy to brute force within hours). When a 52-character set can be used, brute force will take 128 times longer.

4 Difficulty Factor

Because hashes cannot be reversed, an attacker must hash possible passwords and compare these hashes with the obtained password hash of an existing user to determine the credentials that can be used to log in. The number of password tries per second an attacker can launch against a hash depends on the number of CPU cycles the hashing function uses to compute the hash of a password. The more tries per second, the sooner all possible combinations can be tested.

MD5

MD5 (Message Digest) is a cryptographic hash algorithm that produces a hash value in hexadecimal format. This algorithm has serious weaknesses as it is known to have hash collisions. A collision happens when two unique plaintext hash to the same hash value.

LM

Lan Manager hash was introduced by Microsoft in 1980 and has multiple weaknesses. The LM Hash is typically stored in the SAM/NTDS database system. Two severe weaknesses are a maximum password length of 14 characters and passwords being converted to uppercase.

SHA

SHA stands for Secure Hash Algorithm. SHA is a family of cryptographic functions. There are several iterations: SHA, SHA1, SHA2 and SHA3. Passwords saved in online databases are typically stored as a SHA hash.

NTLM

NT LAN Manager is the Microsoft authentication protocol created to be LM's successor. This protocol uses the MD4 hash to create the hash-based on a series of mathematical calculations, and MD4 is known to be stronger than DES.

7.2 Password Dumps

To crack passwords, an adversary must first get a list of password hashes. This list is often acquired by searching the internet (or buying) password dumps. Password dumps happen after an online service gets breached and user data is stolen. Afterward, the hacker can sell the information online or even give it away for free.

REAL CASE

In January 2019, a large number of credentials were leaked on the MEGA file-sharing website. Approximately 770 million account details were discovered in the dump, which seemed to have been gathered from various data breaches in the past. The initial investigation of the breach was carried out by Troy Hunt, the founder of 'haveibeenpwned.com,' and it was added to the website's account database. Following its discovery, the breach was named "Collection #1," and it is considered the largest known dump of user credentials to date. Users who are concerned and wish to check if their credentials have been involved in any publicly known password dumps can visit the HaveIBeenPwned website and enter their email address to verify if it has been part of any known breaches. If necessary, they can then proceed to change their password(s). [8]

[8] https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/

7.3 Password Cracking

Computers use one-way hashing algorithms to encrypt passwords for storage. A one-way hash is mathematically easy to compute in one direction (for encryption) but impossible to calculate the other way, even for computers. This is important because someone who recovers a password file can't use the hashed values to reverse the one-way encryption function and recover the original passwords. But **how does the computer use the encrypted information to authenticate users?**

The technique is simple. Even though hashing functions can't be reversed, they can consistently produce the same output, given the same input. Thus, the computer stores only the hashed passwords (rather than the original passwords) on a disk. When a user attempts to authenticate to either the machine itself or the network, the computer applies the hash algorithm to the user's password for authentication. If the hash of the user-supplied password matches the hash stored on disk, the password is correct, and the user is authenticated.

Password cracking is guessing or determining plaintext passwords, given only hashed passwords. The process does not break the encryption; it mimics the actions that would take place if a user tried passwords until guessing the right one. Each guess is hashed and compared to the stored value. When a match is found, the user is authenticated. The cracking operation is usually performed offline against a recovered password file.

The general method for cracking is the following:

1. **Obtain a list of hashed passwords, using password hashing tools (Mimikatz, Hashcat...) or other dumps.**
2. **Determine the hash function used.**
3. **Create a list of possible passwords.**
4. **Hash each password in the list.**
5. **Determine whether there is a match with the collected hashes.**

8. Specialized Attacks

There are four general methods for cracking passwords:

Dictionary Attack

The fastest method for cracking passwords is a **dictionary attack**, testing all the words in a dictionary or word file against the password hashes. Many websites have downloadable dictionaries you can use. These attacks are quite effective because people tend to choose dictionary words for passwords.

Brute Force Attack

The most potent cracking method is the **brute force** method. It will always recover the password no matter how complex it is -it's just a matter of time. Very complex passwords containing characters not directly available on the keyboard might take too long that trying to crack them is not feasible on a single machine using today's hardware.

Hybrid Attack

The **hybrid attack** builds on the dictionary method by adding numerals and symbols to dictionary words. Many users choose passwords such as he11o!! (in which ones replace the cells) to satisfy policies and filters. These passwords are just dictionary words slightly modified with additional numerals and symbols. The hybrid attack rapidly generates these passwords and computes their hashes. As a result, this type of password is still easily crackable, even though it will pass through many password filters and policies.

Pre-Computation Attack

By **pre-computing** hashes of potential passwords and storing the results in a database or table, CPU time can be invested when processing power is available. When the actual cracking needs to be done, matching hashes with passwords is only a matter of searching through the pre-computed tables, which requires more memory but takes only a fraction of the time needed to brute force a hash. The files containing the pre-computed password hash values are called "**rainbow tables**.".

8.1 Passwords Cracking Tools

Some tools frequently used for password cracking are:

Hashcat

A tool that takes advantage of the potential hardware acceleration provided by parallelizing the workload over multiple cores.

Mimikatz

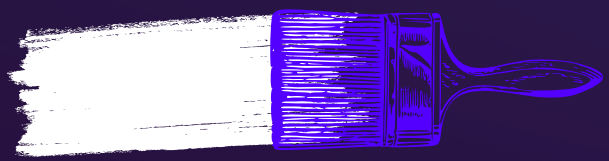
Post-exploitation tool for extracting passwords, PINs, hashes, and Kerberos from Windows system memory. It can exploit vulnerabilities and use various credential-gathering techniques.

Hashcat has support for a variety of operation modes, such as:

Dictionary Attack a.k.a. List attack	Go through a given list of words from a text file and try each as a password candidate.
Combinator Attack	The combinator attack builds on the dictionary attack by concatenating two strings from the provided wordlist to each other.
Brute-force Attack & Mask Attack	The brute-force attack tries each possible combination from a given keyspace.
Hybrid Attack	A hybrid attack is a variant of the combinator attack. It will combine the entries from the wordlist on one side and add the result of a mask attack on the other side.

Some main features modules of Mimikatz are:

Sekurlsa	This module extracts credentials from the memory of the lsass (Local Security Authority Subsystem Service).
Kerberos	They are long-duration (sometimes non-expiring) authentication tickets for administrator users.
Lsadump	Dump system data from the Windows Local Security Authority (LSA) with the sam command.



SPEEDING UP THE CRACKING PROCESS

Modern password-cracking tools automatically detect hardware in the system that can accelerate the cracking process. Because calculating the hashes can be split up over large amounts of processing units, hardware like **Graphics Processing Units** (GPUs) can be effectively used to gain a significant speed improvement.

Additionally, the new guidelines discourage so-called "security questions" for password resets or SMS for two-factor authentication tokens, as **SIM-swapping attacks** are becoming more prevalent in some countries.

Rainbow crack and the **rainbow tables** implement a faster cryptanalytic time-memory trade-off developed by Philippe Oechslin.

Research on pre-computing password hashes was not entirely new. In 1980, Martin Hellman described a cryptanalytic time-memory trade-off that reduces the cryptanalysis time by using recalculated data stored in memory. Philippe managed to reduce the number of necessary calculations further.

Reducing the required CPU cycles makes this method even more suitable for cracking password hashes.

Pre-computation attacks can be fought by preventing hashes from being exact representations of passwords.

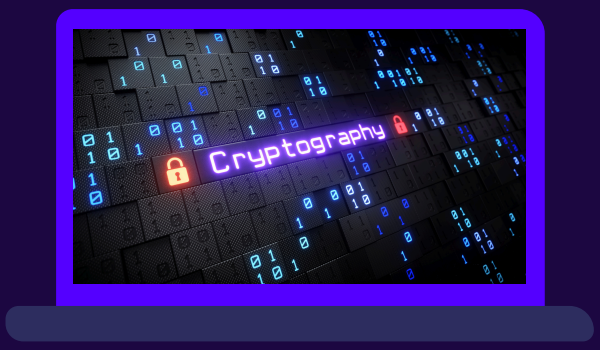
Pre-computation is only successful if you are sure that the hashes in the pre-computed tables will match the hashes of passwords discovered during future audits. If two people have the same password, they will have the same hash, and a pre-computation attack will work.

The way to defeat this is to assign to each account a random value, known as a **salt**. Since each account has a unique salt, if you combine the salt with the password and run it through a hash, even if two people have the same password, they will have different hashes because they have different salts.

A **pepper** is very similar to a salt, but as opposed to a salt, it is kept secret.

9. Cryptography

The science of hidden writing helps us communicate without revealing the meaning of information to adversaries.



Cryptography is often referred to as a science concerned with how to hide the 'meaning' of a communication.

Cryptanalysis is often seen as the science that studies the methods used by cryptographic systems to try and defeat them (in other words, looking for cryptographic weakness).

Cryptography is vitally essential to information security. One of the main goals of cryptography is to protect information from unauthorized disclosure. The idea is that communicating over any medium has the inherent risk that an unauthorized third party could be listening, and we want to minimize or eliminate that risk.

A **cryptosystem** collects all possible inputs and outputs, including the algorithm and keys.

Cryptographic keys are simply values used to initialize a particular algorithm. The critical aspect of keys regarding cryptosystems is that only the key, not the algorithm, needs to be protected. This means that algorithms might be widely distributed and their internal workings publicly documented. Only the key must be protected from thievery by communicating entities.

There are three general types of cryptosystems: **Secret key or symmetric, public key or asymmetric, and hash (hashing).** Each is used because it provides a different function from the other cryptosystems. The number of keys employed usually distinguishes these schemes.

Symmetric key cryptography	Asymmetric key cryptography	Hashing
It uses a single key for encryption and decryption; this key is the shared secret between the sender and receiver.	Asymmetric encryption algorithms use a pair of Asymmetric encryption algorithms use a pair of huge, mathematically related keys. In this two-key system, one of the keys is used to encrypt data, and the other is used for decryption. This depends on the existence of so-called trapdoor functions that are easy to calculate, whereas the inverse function is complex .	Hashing algorithms do not use a key. Hash values are fixed in length and computed in a way that renders it impossible for the original message or its size to be recovered. The fixed-length output is often called the key length of a hash function. The primary application of hash functions in cryptography is message integrity.

9.1 Public Key Infrastructure

Public Key Infrastructure (PKI)
It is a system of functionality for creating, maintaining, and revoking certificates. Certificates are data structures that can bind a public key to the entity to which it belongs.

- **Certificate registration**
- **Certificate creation**
- **Certificate distribution**
- **Certificate revocation**
- **Certificate expiration**

9.2 Certificates

Certificates are the digital equivalent of physical, real-world identification documents (such as driver's licenses and passports).

When someone provides a physical identification document, we tend to trust it because we believe in the authority that issued it. Government-issued identity documents rely on this trust. If we trust the issuing authority's verification process, we can validate someone's identity by simply comparing the document to the presenter. Digital certificates operate on a similar level of trust for digital identities.

Physical identity documents often have physical markings or other unique characteristics (such as holograms) to help us visually identify whether the document is legitimate (not counterfeit). It turns out that certificates also have specific characteristics to help us digitally identify if they are legitimate.

The most specific characteristic comes in the form of a **digital signature**. That's correct—digital signatures again for the win. We need to verify a certificate's legitimacy, especially when considering that the public key is intrinsic to so many of the cryptographic functions we wish to achieve. Suppose an adversary could fool us into believing that a given certificate (and its public key) is for someone that it is not. In that case, the entire security of a cryptographic system might be defeated.

9.3 Secure Web Traffic: HTTPS (SSL/TLS)

Cryptographic protocols can provide security and data integrity over TCP/IP networks. Two such protocols, SSL and TLS, encrypt the segments of network connections at the Transport Layer.

SSL was most commonly employed on the web with the Hypertext Transfer Protocol (HTTP) for E-commerce transactions, although SSL was not limited to HTTP or financial transactions. SSL uses cryptography to provide message privacy, message integrity, and client and server authentication.

It was designed to operate on TCP port 443. SSL is mentioned for historical significance. SSL should not be used due to the many security issues that have been discovered.

TLS, while having a name different from SSL, is designed with the same capabilities in mind that were provided through SSL.

TLS is the long-term replacement protocol for SSL. While the goals of TLS are the same as SSL, TLS does take on additional considerations regarding how secure sessions are formed to provide extra security beyond simply ensuring data is protected in transit.

Confidentiality with symmetric encryption

Integrity via hashing

Session key establishment

Authentication