Glossary of Terms

yubico

This document supplies a list of commonly used terms for internal YubiKey users.

Access management
The processes associated with a user's login across a realm of applications or information repositories. IAM services authorize user access to protected resources, but delegate the authorization decisions to the applications' owners.

Active Directory Federation Services (ADFS)
A federated authentication system for Microsoft-centric networks that use Microsoft Active Directory as their directory services system. ADFS aims to provide seamless authentication and single sign-on functionality across a very large organization, while supporting autonomy for each organizational group to manage their own access control needs.

Application owner
The users responsible for deciding the business needs of applications with respect to IAM. They work with the IAM program team on how best to integrate their applications with IAM services, as well as directing the configuration of their applications.

Authentication
Commonly called "logging in", it's the process of validating that people or entities are who they say they are.

Authentication Factors
This refers to three mutually reinforcing categories of authentication schemes:
1. Something you are (e.g. your retina, thumbprint, voice characteristics)
2. Something you have (e.g. a specific device, a fob, a YubiKey)
3. Something you know (e.g. a password, a secret code)

Authenticator
An authenticator is used to confirm the identity of a user and can be something you know, something you have, or something you are. In the case of digital authentication, a person authenticates to a computer system or application by demonstrating that he or she has possession and control of an authenticator.

Authenticator App
An authenticator app adds a layer of security for online accounts by generating 2-step verification codes on a mobile or desktop device.

Authorization

The process of determining if a user has the right to access a service or perform an action.

Biometrics

Biometrics are physical or behavioral human characteristics that can be used to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns, voice or typing cadence.

Built-in Authenticator

A built-in authenticator (also referred to as a platform authenticator) is built into a particular client device platform, that is, it is implemented on device. An example would be biometrics capabilities that now ship with modern devices.

Brute Force Attack

In cryptography, a brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found.

Bring Your Own Device (BYOD)

A policy permitting employees to carry personal devices into their work environment for business use.

Certificate Authority (CA)

An entity that issues digital certificates as part of a Public Key Infrastructure (PKI). Certificates issued by CAs verify the identity of the "issued-to" object to third-parties. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) rely on CA certificate verification when establishing secure communications.

Credential Stuffing

Credential stuffing is a type of cyberattack where stolen account credentials typically consisting of lists of usernames and/or email addresses and the corresponding passwords are used to gain unauthorized access to user accounts through large-scale automated login requests directed against a web application.

CTAP

Developed by the FIDO Alliance, the Client to Authenticator Protocol enables communication between an external authenticator (i.e. mobile phones, connected devices) and another client (e.g. browser) or platform (re: operating system).

Data Breach

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Approximately 81% of data breaches are caused by stolen credentials such as passwords.

External Authenticator

An external authenticator (also known as a roaming authenticator) is a cross-platform authenticator that is portable. An example would be a hardware security key.

Federated Identity

In a federated identity system, multiple software systems can share identity data from a larger centralized system. For example, an application for consumers may allow its users to log in using a Google or Facebook account.
An enterprise network may use a federated system so that branch offices can manage their own identity system, while connecting systems from each branch through a system at head office. This would allow employees traveling to a different branch office to use the computer systems, but different access policies would likely still apply.

FedRAMP

The FedRAMP Program Management Office (PMO) mission is to promote the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment.

FIDO Alliance

The FIDO Alliance is an open industry association launched in February 2013 whose mission is to develop and promote authentication standards that help reduce the world's over-reliance on passwords. Yubico has pioneered the development of authentication standards that the FIDO Alliance has adopted.

FIDO CTAP 1

The Client to Authenticator Protocol (CTAP) enables an external and portable authenticator (such as a hardware security key) to interoperate with a client platform (such as a computer). The CTAP specification refers to two protocol versions, the CTAP1/U2F protocol and the CTAP2 protocol.

FIDO CTAP 2

An authenticator that implements CTAP2 is called a FIDO2 authenticator (also called a WebAuthn authenticator). If that authenticator implements CTAP1/U2F as well, it is backward compatible with U2F. A YubiKey 5 Series security key can support both CTAP 1 and CTAP 2 which means it can support both U2F and FIDO2 and deliver strong single factor (passwordless), strong two-factor and strong multi-factor authentication.

FIDO Universal 2nd Factor (U2F)

U2F was developed by Yubico and Google, and contributed to the FIDO Alliance after it was successfully deployed for Google employees. The protocol is designed to act as a second factor to strengthen existing username/password-based login flows. It's built on Yubico's invention of a scalable public-key model in which a new key pair is generated for each service and an

unlimited number of services can be supported, all while maintaining full separation between them to preserve privacy.

FIDO2

FIDO2 is the passwordless evolution of FIDO U2F. The overall objective for FIDO2 is to provide an extended set of functionality to cover additional use-cases, with the main driver being passwordless login flows. The U2F model is still the basis for FIDO2 and compatibility for existing U2F deployments is provided in the FIDO2 specs.

FIPS 140-2

The Federal Information Processing Standard Publication 140-2, is a U.S. government computer security standard used to approve cryptographic modules. It is published by the U.S. National Institute of Standards and Technologies (NIST) and is a security standard recognized by the U.S. and Canadian governments, as well as the European Union. It is often a specification that a security solution needs to meet for some of the more security-conscious organizations globally.

Hardware Authenticator or Token

A Hardware Authenticator is a physical object that verifies the user's identity as they log into a system. The user needs to prove that they are in physical possession of the authenticator by plugging the device into the workstation, or mobile phone using a USB or NFC communication method.

HSM

An HSM is a hardware security module that delivers enhanced protection for cryptographic keys, securing modern infrastructures. It can securely generate, store and manage digital keys.

IAM

Identity management, also known as identity and access management, is a framework of policies and technologies for ensuring that the proper people in an enterprise have the appropriate access to the right technology resources, based on their roles and privileges in the organization.

IDP

An identity provider (abbreviated IdP or IDP) is a system entity that creates, maintains, and manages identity information for principals, such as individuals, computers or services, while providing authentication services to relying applications within a federation or distributed network.

Man-in-the-Middle (MiTM) Attacks

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

Multi-Factor Authentication (MFA)

A combination of at least two of the three authentication factor categories. MFA is a more general form of two-factor authentication. It often refers to a system that combines two or more authentication requirements in different circumstances. MFA significantly increases system security, especially in the case of credential compromise, because each additional authentication factor requires additional effort to compromise.
For instance, phishing for passwords has a relatively high success rate and can be done at scale remotely, but stealing the corresponding physical token from a user's keychain would be quite difficult.

OATH - TOTP (Time)

OATH is an organization that specifies two open authentication standards: TOTP and HOTP. To authenticate using TOTP, the user enters a 6-8 digit code that changes every 30 seconds. The code is generated using HMAC(sharedSecret, timestamp), where the timestamp changes every 30 seconds. The shared secret is often provisioned as a QR-code or preprogrammed into a hardware security key.

OATH - HOTP (Event)

HOTP works just like TOTP, except that an authentication counter is used instead of a timestamp. The advantage of this is that HOTP devices require no clock. However, HOTP is susceptible to losing counter sync. That is, if the user generates an OTP without authenticating with it, the device counter will no longer match the server counter. This can be mitigated on the server by testing several subsequent counter values. This can not happen with Yubico OTP since its counter is encrypted (as opposed to hashed).

One-Time Password (OTP)

A one-time passcode or password (OTP) is a code that is valid for only one login session or transaction. An OTP is typically sent via SMS to a mobile phone, and they are frequently used as part of two-factor authentication (2FA). The NIST organization has recently deprecated SMS as a weak form of 2FA and encourages other approaches for strong 2FA.

Passwordless

Passwordless refers to passwordless authentication or login which represents a massive shift in how billions of users, both business and consumer, will securely log in to their critical resources and systems. The user can simply authenticate using a passwordless device, such as a FIDO2-based hardware security key to verify their credential with the application or system.

Phishing

Phishing is the art of tricking people into revealing personal information. Usernames, passwords, and credit card numbers are often targeted for phishing attacks, with the intent of taking over user accounts. 59% of phishing attacks are financially motivated.

PIV
A Personal Identity Verification (PIV) credential is a US Federal governmentwide credential used to access Federally controlled facilities and information systems at the appropriate security level.

Platform
A computing platform or digital platform is the environment in which a piece of software is executed. It may be the hardware or the operating system (OS), even a web browser and associated application programming interfaces, or other underlying software, as long as the program code is executed with it.

Platform Authenticator
A platform authenticator is built into a particular client device platform, that is, it is implemented on device. An example would be biometrics capabilities that now ship with modern devices.

Public Key Cryptography
Public key encryption, or public key cryptography, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. A hardware security key offers the strongest protection for private keys as it is stored in the secure element and cannot be exfiltrated, or gained via a remote attack.

Root of Trust
A root of trust is an external hardware authenticator that can be used with any computer or mobile device to identify that the person accessing an account is the rightful owner.

Roaming Authenticator
A roaming authenticator is a cross-platform authenticator that is portable. An example would be a hardware security key.

Security Key
A security key is a single purpose hardware device for authentication which is controlled by an end user. The security key enables FIDO authentication across platforms, browsers and applications.

Secure Static Password
A static password requires no back-end server integration, and works with most legacy username/password solutions. Using the YubiKey Personalization tool a YubiKey can store a user-provided password on the hardware device that never changes. Please note that a static password does not provide the same high level of security as one-time passwords.

Smart Card

A smart card is a physical card that has an embedded integrated chip that acts as a security token. Smart cards are typically the same size as a driver's license or credit card and can be made out of metal or plastic. Hardware security keys can also act as a smart card with simplified deployment.

Service provider (SP)

A system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use.

Software Authenticator or Token

A software-based authenticator may be implemented on a general-purpose electronic device such as a laptop, a tablet computer, or a smartphone. For example, a software-based authenticator can be implemented as an authenticator app on a mobile device.

Strong Two Factor Authentication (2FA)

Two-factor authentication (also known as 2FA or two-step verification) is a method to confirm a user's claimed online identity by using a combination of two different types of factors. Factors used for 2FA include something that you know (e.g. password or PIN), or something that you have (e.g. a security key or phone) or something that you are (e.g. facial recognition).

Strong Multi-factor Authentication (MFA)

Multi-factor authentication (MFA) can greatly enhance security while delivering a positive user experience. MFA is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence, or factors, to an authentication mechanism. Hardware security keys offer strong MFA because the credential secrets are stored securely on the hardware key and cannot be exfiltrated. Other forms of MFA, while offering stronger security than a password, cannot offer the same level of iron-clad protection as a security key.

WebAuthn

WebAuthn is a new W3C global standard for secure authentication on the Web supported by all leading browsers and platforms. WebAuthn makes it easy to offer users a choice of authenticators to protect their accounts, including external/portable authenticators such as hardware security keys, and built-in platform authenticators, such as biometric sensors

YubiKey

The industry's #1 security key, enabling strong two-factor, multi-factor and passwordless authentication.

YubiOTP

Yubico OTP is a simple yet strong authentication mechanism that is supported by the YubiKey 5 Series and YubiKey FIPS Series out-of-the-box. Yubico OTP can be used as the second factor in a 2-factor authentication scheme or on its own providing strong single factor authentication.

Zero Trust

Zero Trust is a security framework developed by Forrester Research in 2009 that throws away the idea that we should have a trusted internal network vs an untrusted external network. Rather we should consider all network traffic untrusted.

This research has evolved to discuss an Zero Trust Extended Ecosystem that includes the need to secure the workforce through strong identity and access management, along with multi-factor authentication. Forrester has coined the term “next-generation access” to describe this critical component.

EXTRA STUFF:

Okta:

Access Management – The process of configuring the level of access for each user and group within a software system. Through this process, system administrators grant access to authorized users and restrict access to unauthorized users. This may be done hierarchically through the use of user groups. Access management requires periodic auditing and maintenance to keep up with evolving business needs and employee roles.

Further Resources: An Overview of Identity and Access Management (IAM)

IAM (Identity and Access Management): A guide to keeping the identity of your business in check

---

Active Directory Federation Services (ADFS) – A federated authentication system for Microsoft-centric networks that use Microsoft Active Directory as their directory services system. ADFS aims to provide seamless authentication and single sign-on functionality across a very large organization, while supporting autonomy for each organizational group to manage their own access control needs.

Further Resources: Microsoft Active Directory and Active Directory Federation Services

Single Sign-On: The Difference Between ADFS vs. LDAP

Authentication – The process of determining that the party with which you are communicating is indeed who they claim to be. In other words, the process of determining a user's identity.

Further Resources: Authentication: Achieve scale and security with innovative authentication solutions for your team

Security Starts with Authentication

The Okta Authentication Guide

Authentication Factors – This refers to three mutually reinforcing categories of authentication schemes:

1. Something you are (e.g. your retina, thumbprint, voice characteristics)

2. Something you have (e.g. a specific device, a fob)

3. Something you know (e.g. a password, a secret code)

Authorization – The process of determining whether a given identity is allowed to access a given resource or function.

Further Resources: What is an Authorization Server?

Brute Force – A method of attack whereby an attacker systematically attempts all possible combinations of inputs, usually by automating the process with a script.

Cloud Identity Management – A service such as Okta that is hosted in the cloud, offering identity, authentication, and authorization functions for other cloud-hosted software services. A cloud identity management system is an alternative to traditional directory service systems, which typically manage identity for on-premises monolithic enterprise applications. These often leave cloud services with siloed identity services that must be managed individually, thus complicating lifecycle management.

Data Breach – Refers to an incident whereby data is accessed by an unauthorized individual or software system.

Further Resources: Smart Authentication Can Stop Data Breaches

Stop Data Breaches with Smarter Authentication

CIO eGuide: Preventing Data Breaches

Data Breach Prevention – Includes technology, people, and process considerations — all of which work together to protect an organization. From a technology perspective, this includes well-maintained user authentication and authorization configuration, systems that scan and block network activity in real time based on content filtering policies, or "circuit breakers" that detect potential exfiltration based on an abnormally high outbound data rate.

Further Resources: Smart Authentication Can Stop Data Breaches

Stop Data Breaches with Smarter Authentication

CIO eGuide: Preventing Data Breaches

Deprovisioning – The process of removing access for a particular user from software systems. For example, when an employee leaves the organization, their user profile must be deprovisioned.

Deprovisioning is generally more complicated than simply deleting the account, because it's often desirable to retain and accurately attribute the user's previous contributions, so the account must remain in some type of disabled state.

Employee Identity Management – The process of cataloguing employees in a software system. Employee identity management often includes representing the organizational structure of functional groups.

Employee identity management requires ongoing maintenance, such as when employees are hired or leave the organization. It also often includes an authentication scheme, such as having the employee set their account password.

Federated Identity – In a federated identity system, multiple software systems can share identity data from a larger centralized system. For example, an application for consumers may allow its users to log in using a Google or Facebook account.

An enterprise network may use a federated system so that branch offices can manage their own identity system, while connecting systems from each branch through a system at head office. This would allow employees traveling to a different branch office to use the computer systems, but different access policies would likely still apply.

Identity as a Service (IDaaS) – This is a variant on the concept of Software as a Service (SaaS), indicating that identity management can be outsourced and purchased as a cloud-based service instead of either purchasing the software and operating it in-house or building the functionality from scratch in-house.

Further Resources: What is IDaaS? Understanding Identity as a Service and Its Applications

Modernizing the IT Infrastructure in Government with IDaaS

Identity and Access Management (IAM) – The process of codifying not only users and groups in a software system, but also what resources they are each able to access and what functions they are each able to perform. IAM addresses authentication, authorization, and access control.

Further Resources: An Overview of Identity and Access Management (IAM)

IAM (Identity and Access Management): A guide to keeping the identity of your business in check

Identity and Access Management Strategy

Identity Management – The process of codifying users and groups, as well as the metadata related to each of these entities, such as contact details, location, photo, etc. Includes mechanisms for authentication of these entities.

Lifecycle Management – This term recognizes that many entities represented in a software system will be at a certain stage in a lifecycle, and their access needs to be managed accordingly. For instance, an employee may start off as a "candidate," then become a "full employee" with one or more positions over their tenure, and ultimately cease to be an employee and be deprovisioned entirely.

Lifecycle management can also apply to other things. For instance, devices may be purchased, provisioned for a particular user, reprovisioned for a different user, and ultimately deprovisioned and sold or discarded.

Multi-Factor Authentication (MFA) – A combination of at least two of the three authentication factor categories. MFA is a more general form of two-factor authentication. It often refers to a system that combines two or more authentication requirements in different circumstances. MFA significantly increases system security, especially in the case of credential compromise, because each additional authentication factor requires additional effort to compromise.

For instance, phishing for passwords has a relatively high success rate and can be done at scale remotely, but stealing the corresponding physical token from a user's keychain would be quite difficult.

Password Spray – A type of brute force password attack whereby a single common password (e.g.: password1) is tried in combination with many usernames, rather than the other way around. Many systems can detect a brute force attack against a single user and will lock the account after a number of failed attempts. By executing a brute force attack along a different axis, the attacker often goes unnoticed.

Further Resources: Best Practices: Password Management for the App Explosion

Moving Beyond User Name & Password

Passwordless Authentication – Describes a range of approaches to authenticate users by means other than a password. This could be one of the two other authentication factor categories (something you are, or something you have) or it may refer to a process by which an email or text containing a secret single-use code authenticates you with no other password required.

Some applications offers this option for users, who can request a single-use code or link by email that authenticates them to access the application.

Further Resources: Customer Story: Passwordless Auth for TAL Customers

---

Phishing – A type of socially engineered attack whereby a user is presented with a seemingly plausible and often mundane request, and is tricked into divulging their authentication credentials to a facade.

One common phishing attempt is an email that appears to be from the user's IT department, claiming their account requires verification, with a link directing them to a lookalike website. When they log in to the fake website, their credentials are sent to the attacker, which the attacker can then use to impersonate the user on the real site.

Provisioning – The process of establishing an identity and associated access configuration in a software system. An example is when a new user signs up for a service, or a new employee begins at an organization. Provisioning requires establishing a method for subsequent authentication (e.g. receiving user login credentials, choosing a password, etc.).

Further Resources: Provisioning and Deprovisioning

Okta Incident Response Guide

Public-Key Cryptography – An application of asymmetric cryptography, where one key is private and the other is public. Asymmetric cryptography means a message encrypted with one key can only be decrypted by the other. The public one is widely distributed, so that anyone wishing to send the owner of the private key a message can do so knowing that only the intended recipient will be able to decrypt it.

Security Assertion Markup Language (SAML) – This is a standardized protocol used to integrate authentication and authorization functions between multiple systems. It is most

often used to gain single sign-on functionality between multiple applications from different vendors.

SAML implementations act as an "identity provider," which handle authentication and authorization on behalf of one or more applications.

Single Sign-On (SSO) – SSO enables a user to authenticate to multiple software systems with a single authentication session. A common business application of this is an employee enters their credentials once into a company SSO product and gains access to all their business apps without logging into each app separately. This is particularly helpful if the software systems are within the same organization and managed by the same authority.

From the end user perspective, SSO removes the fatigue of logging in to multiple systems or remembering multiple account passwords.

Okta SSO also includes additional features such as self service password resets, AD and LDAP integration, customizable end user experience, and a central access policy engine.

From the IT perspective, this enables faster, more secure deployment of business apps, while reducing help desk calls from tasks such as password resets.

Time-Based One-Time Password (TOTP) – An algorithmically-generated code that is deterministic based on the current date and time and a secret "seed" value. The server knows the seed, and can easily verify that a given code is valid for the current time period. TOTP can significantly increase security because even if a code is intercepted, it is worthless after the time window has passed (usually less than a minute). This makes the logistics of an attack much more difficult.

TOTP can be implemented on a simple and inexpensive hardware device or on a smartphone. The seed is installed and is made difficult or impossible to recover or duplicate.

Token Authentication – A method of authenticating to an application using a signed cookie containing session state information. A more traditional authentication method is usually used to initially establish user identity, and then a token is generated for re-authentication when the user returns.

Two-Factor Authentication (2FA) – The combination of two out of the three authentication factor categories. Two-factor authentication is a subset of multi-factor

authentication, and significantly increases security, because each authentication factor requires a different style of attack to compromise.

Universal Authentication Frameworks (UAF) – UAF is an open standard developed by the FIDO Alliance with the goal of enabling a secure passwordless experience for primary authentication, as opposed to a second factor as described in U2F. Under the spec, the user presents a local biometric or PIN and is authenticated into the service. This protocol is not yet embedded in the major browsers, which has limited its adoption.

Universal 2nd Factor (U2F) – U2F is an open standard, whereby a hardware token device can attest the holder's identity through a challenge and response protocol. The token device is connected via USB or NFC (near-field communication).

It is the standard maintained by the FIDO Alliance and is supported by Chrome, Firefox, and Opera.

WebAuthn – An evolution of the FIDO U2F and UAF protocols. WebAuthn continues in the FIDO tradition of allowing for using credentials for step up authentication. However, it's biggest innovation is in enabling users to authenticate to services without necessarily needing the user to identify themselves first (through the use of a username and password combination).

Further Resources: WebAuthn: A Developer's Guide to What's on the Horizon

Zero Trust – Zero Trust is a security framework developed by Forrester Research in 2009 that throws away the idea that we should have a trusted internal network vs an untrusted external network. Rather we should consider all network traffic untrusted.

This research has evolved to discuss an Zero Trust Extended Ecosystem that includes the need to secure the workforce through strong identity and access management, along with multi-factor authentication. Forrester has coined the term "next-generation access" to describe this critical component.

****

https://iam.harvard.edu/glossary

Access management *The processes associated with a user's login across a realm of applications or information repositories. IAM services authorize user access to protected resources, but delegate the authorization decisions to the applications' owners.*
Application owner *The users responsible for deciding the business needs of applications with respect to IAM. They work with the IAM program team on how best to integrate their applications with IAM services, as well as directing the configuration of their applications.*

Authentication *Commonly called "logging in", it's the process of validating that people or entities are who they say they are.*

Authorization *The process of determining if a user has the right to access a service or perform an action.*

Central Authentication Service (CAS) *A "single sign-on" protocol for the web, as well as an authentication engine implementation. CAS uses a simple but robust authentication protocol that is widely deployed in higher education.*

Credential *An item — such as login name/password — used by a person or entity to prove him/her/itself to a system.*

Directory service *The software system that stores, organizes, and provides access to information in a directory for entities such as people, groups, devices, resources, etc.*

Federation *Also known as federated identity management, this is a technical implementation that enables identity information to be developed and shared among several entities and across trust domains.*

Identity and access governance *Identity and access governance tools establish a lifecycle process that allows business owners of identities to have comprehensive governance of identities and access requests. It allows organizations to identify access risks and make sure access meets organization policies.*

HarvardKey *HarvardKey is a new, unified login credential for users across the Harvard Community, supported by the service that authenticates users of online applications created by or affiliated with Harvard. Authenticating with HarvardKey verifies users' identities in order to allow them to access applications; to do this, the user provides a unique login name (in the form of an email address) and confirms that identity by submitting the correct password. Two-step verification (see below) is available with HarvardKey for an extra level of security assurance.*

Identity management *The processes and solutions that provide for the creation and management of user information.*

Identity provider (IdP) *A system that validates the identity of a user in a federated system. The service provider (or SP; see below) uses the IdP to get the identity of the current user.*

Identity stores *User information stored across a variety of technologies, including databases, LDAP, Active Directory, etc.*

InCommon *Operated by the Internet2 consortium of U.S. higher education and research institutions and their partners, InCommon is home to an identity management federation and a related assurance program, and offers certificate and two-step verification services. Harvard acts as a Bronze-certified identity provider (IdP) within the InCommon federation, and a variety of Harvard units are also InCommon service providers (SPs) under Harvard's membership.*

People administrator *A person who assigns roles, group memberships, and/or other attributes to a user.*

SailPoint IdentityIQ (IIQ) *Harvard's provisioning and identity management toolset.*

Security Assertion Markup Language (SAML) *Originally developed by the OASIS Security Services Technical Committee, SAML is an XML-based framework for communicating user authentication and attribute information. Harvard's authentication system supports version 2.0 of the SAML protocol.*

Service provider (SP) *A system that provides a generic service to the user in a federated system. To users, a service provider is the same thing as the application they are trying to use.*

Sponsored affiliation *A user who does not have a long-term affiliation with the University, but requires access to Harvard resources. As the name implies, sponsored affiliation must be sponsored by a staff or faculty member with the appropriate authorization.*

Two-step verification *Sometimes called "multifactor authentication", two-step verification strengthens the security of a user's login by combining something the user knows (login name and password) with something the user has (in may cases, a text-message login code sent to their phone, or a smartphone push notification). HarvardKey users can set up optional two-step verification using their cell phone, mobile device, or even landline phone.*

User *A term used to generalize and reference multiple user types, such as Harvard users (i.e. staff, students, or faculty), sponsored affiliates, and Harvard application users.*

User provisioning *A set of technologies that create, modify, and de-activate user accounts and their profiles across IT infrastructure and business applications.*

Duo:

Breach

An incident that exposes data to an unauthorized party. Two-factor authentication helps prevent breaches by providing a secure second layer of defense, protecting the various types of accounts a user logs into, and offering authentication through a second device

---

Bring Your Own Device (BYOD)

A policy permitting employees to carry personal devices into their work environment for business use.

Learn more about "Bring Your Own Device (BYOD)"

Certificate Authority (CA)

An entity that issues digital certificates as part of a Public Key Infrastructure (PKI). Certificates issued by CAs verify the identity of the "issued-to" object to third-parties. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) rely on CA certificate verification when establishing secure communications.

Denial of Service (DoS)

An attack against a computer, network, or website in which bandwidth is flooded or resources are overloaded to the point that it is rendered unavailable to users. Can also be carried out by malicious code that simply shuts down resources.

Learn more about "Denial of Service (DoS)"

Domain Hijacking / Spoofing

Manipulating a domain name in order to associate a legitimate, trusted URL with a malicious, imposter website, to phish and perpetrate other online scams. This is

achieved by blocking access to the domain's DNS server and replacing it with their own, but could be prevented by implementing multi-factor authentication.

Encryption

A security measure that uses an algorithm to convert plaintext to a format that is readable only to authorized users with a key to decipher it.

Learn more about "Encryption"

Endpoint

Any device that connects to a network and runs network-based applications, e.g., laptops, desktop computers, servers, and mobile devices.

Federal Information Processing Standard (FIPS)

U.S. government security standards for document processing, encryption algorithms, and other technology practices used by government agencies and adjacent contractors and vendors, issued and recognized by the National Institute of Standards and Technology (NIST).

Firewall

A hardware- or software-based gateway that limits and protects the traffic coming into and out of a network. All data that enters or leaves a network must pass through a firewall, which analyzes the information and based on its security policy either grants or denies access.

IDaaS

An authentication infrastructure that lives in the cloud.

Information Security

The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction, in order to provide

confidentiality, integrity, and availability — having control of your information and trusting that those you've provided it to can keep it safe.

Key

A series of letters, numbers, or symbols used to encode or decode encrypted data.

Learn more about "Key"

Least Privilege

Share

-
-
-
-
-

A policy of granting users or applications only the permissions necessary to perform their official duties. Limiting their amount of access decreases the chances of unauthorized activity and security breaches.

Man-in-the-Middle (MiTM)

Share

-
-
-
-
-

An attack in which a hacker intercepts the communication between two sources, like a client and a server, and impersonates both parties to gain access to sensitive

information. For example, a malicious router in a public location offering free wi-fi, or a fake website masquerading as legitimate in order to capture a user's login credentials.

Learn more about "Man-in-the-Middle (MiTM)"

Managed Service Provider

Share

-
-
-
-
-

An internet service provider that offers network security tools, like virus blocking, spam filtering, intrusion detection, firewalls, and VPN management, saving organizations money by outsourcing these functions.

Mobile Device Management (MDM)

Share

-
-
-
-
-

The process of optimizing the function and security of mobile devices within an organization while protecting the organization's network. One of the best known methods is BYOD, in which users provide a personal mobile device for business purposes.

Patch

Share

-
-
-
-
-

An update to an operating system, application, or other software, released by the manufacturer to repair an identified bug or vulnerability.

Learn more about "Patch"

Payment Card Industry Data Security Standard (PCI DSS)

Share

-
-
-
-
-

*Policies and procedures for organizations that process, transmit, or store payment cardholder data that e****Phishing***

Share

-
-
-
-

-

An attempt to deceive users and illegally acquire sensitive information by contacting them under the guise of a trusted source. Phishing typically employs emails or instant messages that appear to be legitimate, combined with imposter websites, to make bogus requests for personal details such as names, passwords, Social Security numbers, or financial credentials.

nsure it is protected and secured.

Point of Sale (POS)
Share

-
-
-
-
-

The time when a retail transaction is completed. Because various retail situations call for customized software for devices like cash registers, scanners, touch screens, and cloud-based solutions, POS is a large target for breaches and malware. With two-factor authentication, POS vendors and other retail companies can add a second layer of security to their logins to keep unauthorized remote users out of their systems.

Learn more about "Point of Sale (POS)"

Privacy
Share

-
-

-
-
-

The ability to understand and control how others use your information, and the assurance that the confidentiality of and access to your information is protected.

Learn more about "Privacy"

Public Key Infrastructure (PKI)

Share

-
-
-
-
-

A set of services that uses a public and private cryptographic key pair to allow users on an unsecured network to securely exchange data. Typically, this is composed of a certificate authority, which verifies users' identities; a registration authority, approved by the certificate authority to issue certificates for specific uses; a certificate database, which stores requests and issues and revokes certificates; and a certificate store, which houses issued certificates and private keys.

Single Sign-On (SSO)

Share

-
-
-
-
-

An authentication process that allows a user to enter one username and password to access multiple applications, eliminating re-authentication and reducing helpdesk requests to improve productivity, as well as minimizing phishing and improving compliance. Credentials are stored on a dedicated server that authenticates the user for all of the applications where they have been granted access, eliminating additional prompts between applications during the same session.

Social Engineering

Share

-
-
-
-
-

Taking advantage of people's tendency to trust others, this method of deception uses communication online or by phone to trick users into disclosing personal information such as passwords. Examples include sending an email under the guise of a legitimate institution and asking the user to reply to update or confirm their password, or providing a download to a file that appears to be benign but actually is malicious.

Learn more about "Social Engineering"

Spyware

Share

-
-
-
-

-

A program that installs on a user's computer without their consent, often bundled with a legitimate application, that gathers personal data and relays that information to a third party. Some spyware monitors web browsing activity, while others record keystrokes to steal sensitive information.

Threat Agent
Share

-
-
-
-
-

An individual or group that acts, or has the power to, exploit a vulnerability or conduct other damaging activities.

Learn more about "Threat Agent"

Threat Assessment
Share

-
-
-
-
-

The process of identifying or evaluating the types of vulnerabilities that an organization could be exposed to.

Learn more about "Threat Assessment"

Token

Share

-
-
-
-
-

A physical tool or device that a user carries to authenticate their identity and authorize access to a network. Tokens are often in the form of a smart card, or embedded in an everyday object like a keyring.

Learn more about "Token"

Trojan Horse

Share

-
-
-
-
-

A program that appears legitimate, but also contains malicious functions which when installed can access personal information, delete files, or possibly allow attackers to gain control of a computer remotely.

Learn more about "Trojan Horse"

Trusted Access

Share

-
-
-
-
-

Verifying the authenticity of users and security of their devices before they connect to applications.

Learn more about "Trusted Access"

Two-Factor Authentication (2FA)

Share

-
-
-
-
-

An additional way to verify a user's identity before granting login access. When logging in, two-factor authentication requires the user to prove their identity in two different ways, for example: Something you know (like a username and password) Something you have (like a smartphone with an authentication app installed) Something you are (like your fingerprint or retina scan) There are many different methods of authentication, including via push notifications, SMS passcodes, phone calls, tokens and more.