	lentity & Access Management	CISSP Cheat Sheet Series comparitech						
Three-factor Authentication (3FA)			T	erminology		Ac	ccess Control	Requirements
Knowledge factor Something that is known by the user			<u> </u>	to allow information flow between objects. es taken to restrict or allow access to syste		Triad: C onf	identiality - Integrity shee	- A vailability (See Domain 1 cheat
Ownership factor Something that is known by the user Ownership factor Something that the user possesses, like a key or a token.		Subject An	entity which i	requires access to an object or objects.			Identity Ma	,
Characteristic A user characteristic, such as biometrics; fingerprints, face factor scan, signature.		Object Entity which consists information.			IAA	AA – I dentif		on - A uthorization - A ccountability. verification of user identity and add an
	-	Centralized		f Access & Control nponent can control access. Highly restricte	Ide	entification	identifier to sy	_
	-Type/category 1 - something you know cation, Secret questions such as mother's maiden name,	administration Decentralized		control done centrally. ntrolled by information owners, Can be less			• User verifica	use user ID or username.
	te food, date of birth, key combination / PIN.	administration Hybrid	consistent.	of centralized and decentralized.		thenticatior uthorization	• Commonly u	used passwords ources for user access
	Terminology and concepts	Access star		allow-by-default or deny-by-defau	Δς.	countability		onsible for the controls, uses logs.
Salted hash	Random data added to a password before hashing and storing in a database on a server. Used instead of	Single		ated ID management				System for Applications in
Saited Hash	plaintext storage that can be verified without revealing password.	Sign-On	authenticatio				a Multi-vendor ogy only authenticate	s initial segment without
ComplEg.	Alphanumeric, more than 10 characters. Includes a	(SSO)	• Cons – Risk access of a k	k of all systems comprised by unauthorized key or keys.	authen	itication and	d other one defines th	rate tickets are in use one for e access privileges for user. Both
password	combination of upper and lower case letters, numbers and symbols.		Authorization			etric and as	ymmetric encryptions Exchange authentic	s are used. cation and authorization information
One-time password (OTP)	Dynamically generated to be used for one session or transaction.	Access control policies: Level of access and controls granted for a user.				AML - AP/XML)	Components: Prince	omains and systems. cipal User • Identity provider • Service
Static password	Password does not change. To be avoided.	Separation of duties		lifferent users different levels of access to acy and security.	,		provider. • Use in directory fe	deration SSO.
Cognitive password	Something used to identify a person, i.e. pets name, favorite color, mother's maiden name etc, place of birth			perform specific functions is granted to two	r		Authorizatio	n Concepts
Cognitive password	etc.	Dual Controls	more users.		Secu dom		et of resources having	the same security policies.
Password Hacking	Unauthorized access of a password file	Split Knowledge		ser can have full information to perform a ta	Iden		ganization having a cothin the federation.	ommon set of policies and standards
Brute force attack	Multiple attempts using all possible password or pin combinations to guess the password.	Principle of Least Privilege	User is give task.	n minimum access level needed to perform			Federatio	n Models
Dictionary attack	Type of brute force attack that uses all the words from	Need-to-Know	Minimum kı	nowledge level to perform a task.		ertification	Every organization i	is certified and trusted by the other not the standards defined internally by
	the dictionary. Gain access by impersonating a user by establishing	No Access		assigned any access for any object.		lodel	said organizations.	Standards defined internally by
Social engineering attack	legitimate user credentials through social manipulation of trusted parties or authorities.	Directory Service	Centrally ma	anaged database for user objects managem	Third	usted d-Party / je Model	Every organization a party.	adheres to the standards set by a third
Rainbow Tables	Precomputed table for reversing cryptographic hash			er model authentication protocol. c Key Cryptography	IDaaS ((Identity as ervice)	Identity and access party organization.	management is provided by a third
	functions and cracking passwords.	Kerberos	Key Distrib	oution Center (KDC) ality and integrity and authentication,		(Single	Access managemen	nt for multiple similar, yet independant
	-Type/category 2 - Something you have			key cryptography	sig	gn-on)	system access.	used for the cloud and SaaS based
•	Create password at regular time intervals. Generate a password based on the challenge-response	Realm	Authenticat cryptograph	ion administrative domain. Uses symmetric ny	ley	d Identity ectory		gement (Office 365) by provider (Microsoft Active directory)
Asynchronous token	technique.	KDC (Key		ets to client for server authentication	Fadanat	ronization ted Identity	On-premises identit	y provider for managing login request.
Memory card	A swipe card containing user information.	Distribution Center)	· AS (Auther	eret keys of all clients and servers in the net ntication Server)	ork	icu identity	(MS AD)	
Smart Cards or Integrated Circuit	A card or dongle that includes a chip and memory, like bank cards or credit cards.		`	et Granting Server) username/password in client PC/Device.			Access Con By default access to	o an object is denied unless explicitly
Card (ICC) Contact Cards	Swiped against a hardware device.			em encrypts credentials using AES to subm		icit Deny	granted.	ed subjects, objects, and access
Contactless Cards	· · ·	The Kerberos		h input credentials against database. e a symmetric key and time-stamped TGT to	М	latrix	controls / privileges	
or Proximity Cards	Simply need to be within proximity to the reader device.	logon process	•	client and the Kerberos server. GT are encrypted using client password has	Capabi	lity Tables		jects whereas capability lists focus on
Hybrid Cards	Allows a card to be used in both contact and contactless systems.		 Client insta using a has 	alls the TGT and decrypts the symmetric key h.		nissions	Access granted for	an object. erform an action on an object.
USB drive	Bespoke USB with access credentials	Authorization Methods				ights vileges		nts and permissions.
Static password Simplest type of security token where the password is token stored within the token.		Discretionary Access Control (DAC) • Mandatory Access Control (MAC) •				A	Access Contro	ol Categories
Challenge/respons	A challenge has to be met by the correct user response.	Role-based Acces	•	e-BAC) • Rule-based Access Control (Rule-Bacter) Uses access control lists (ACLs -	C). Cate	egory	Scope / Purpose	Example Two keys or key and
e token		(DAC) Access-control lists).		Compa			, ,	
Characteristic –Type/category 3 – Something you do / are Biometric technology allows the user to be authenticated based on				,		ensative R	Risk mitigation action.	
Riometric technolog		Mandatory Acce		Subject authorize according to security lal Used by owners to grant or deny access to	els. Corre		Risk mitigation action. Reduce attack impact.	combination to open a safety locker.
physiological behav	gy allows the user to be authenticated based on vior or characteristics.	Mandatory Acce (MAC)		Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects.	els. Corre	ective R	-	combination to open a safety locker. Having fire extinguishers, having offsite data backups.
physiological behav	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints.			Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or	els. Corre	ective Rective D	Reduce attack impact. Detect an attack before	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS).
physiological behave Physiological i.e. I Behavioral i.e. Voi	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. ce pattern Physiological Characteristics	(MAC)	RBAC)	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects required.	corres Determine	ective Rective Dherrent D	Reduce attack impact. Detect an attack before nappens.	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences
physiological behave Physiological i.e. I Behavioral i.e. Voi	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger.	Role-BAC (F	RBAC)	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system.	Determine Determine Direct	ective Rective Dherrent Dective a	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices was norganization.	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences
physiological behave Physiological i.e. I Behavioral i.e. Voi	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. ce pattern Physiological Characteristics	Role-BAC (F Rule-BA Hybrid RE	RBAC) C BAC	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what	Determined Prevented	ective Rective Dective	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices we	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords.
physiological behave Physiological i.e. I Behavioral i.e. Voi	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. Iris pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout	Role-BAC (F Rule-BA Hybrid RE Lattice based	RBAC) C BAC / Label	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label.	Determined Prevented	ective Rective Dherrent Dective a antative Sovery a	Reduce attack impact. Detect an attack before appens. Discourages an attack before and document acceptable practices was organization. Stop an attack. Recovery of a system an attack.	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc.
physiological behave Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. Iris, retina, and fingerprints. Iris, retina, and fingerprints. Iri	Role-BAC (F Rule-BA Hybrid RE	RBAC) C BAC / Label ry access /	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control leverage access to grant or denied to subjects.	Determine Determine Prevented Reco	ective Rective Dherrent Dective a antative Sovery Rective A	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment
physiological behave Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. Iris pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce	RBAC) C BAC / Label ry access / ess control	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central	Determine Determine Prevented Reco	ective Rective Dherrent Dective a antative Sovery Rective Rective Dective Dect	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability asting • Physical Testing	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc.
physiological behave Physiological i.e. In Behavioral i.e. Void Fingerprint Hand Geometry Hand Topography Palm or Hand Scan	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce	RBAC) C BAC / Label ry access / ess control	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. n Methods / Concepts et actions which can be performed with give	Prevented Reco	ective Rective Dherrent Dective a antative Sovery Rective Rective Dective Dect	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and attack.	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment ng • System and Network Testing and Threat Modeling bability of the attack to the application
physiological behave Physiological i.e. In Behavioral i.e. Void Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan	gy allows the user to be authenticated based on vior or characteristics. Iris, retina, and fingerprints. Scans the thumb or edge of the finger. Iris, retina, and fingerprints. Scans the thumb or edge of the finger. Iris, retina, and fingerprints. Scans the thumb or edge of the finger. Iris, retina, and fingerprints. Scans the thumb or edge of the finger. Iris, retina, and fingerprints. Fize pattern Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce	RBAC) C BAC / Label ry access / ess control Orization ace Restrict privilegent Restrict	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts of access to data depends on the content of the	Prever	ective Rective Descrive Description Descripti	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and the property of the prope	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment ng • System and Network Testing and Threat Modeling bability of the attack to the application ems n about the system
physiological behave Physiological i.e. In Physiological i.e. Vois Behavioral i.e. Vois Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict privilegent Restrict object. Grantin	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. The Methods / Concepts access to data depends on the content of the gusers access after a specific condition. Engusers access after a specific condition.	Prever Simular	ective Rective Dective a antative Sovery Rective a antative Personnel Text Person	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system attack. Vulnerability Desting • Physical Testing at to determine the prospect of t	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment ng • System and Network Testing and Threat Modeling bability of the attack to the application ems n about the system n about attack against the system vistem vulnerabilities
physiological behave Physiological i.e. In Physiological i.e. Void Behavioral i.e. Void Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende	RBAC) C BAC / Label ry access / ess control Orizatio ace Restrict privilegent Object. ent Grantin after si Contex	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of angusers access after a specific condition. Expecific date/time. At-dependent control	Prever Simular St	ective Rective Descrive and antative Sersonnel Telegraph Rective an attack	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of the prospect	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. Disaster recovery plans, data backups etc. Assessment Ing • System and Network Testing and Threat Modeling bability of the attack to the application ems In about attack against the system yetem vulnerabilities gainst the system attempting to gain
physiological behave. Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende	RBAC) CBAC July access / ess control Corization Access Restrict Acces	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of the gusers access after a specific condition. Expecific date/time. Act-dependent control sets are given access to object only to perform they need to have.	Prever Simular St	ective Rective Descrive and antative Sersonnel Telegraph Rective an attack	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of the prospect	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment ng • System and Network Testing and Threat Modeling bability of the attack to the application ems n about the system n about attack against the system vetem vulnerabilities gainst the system attempting to gain come of the penetration test
physiological behave. Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut	RBAC) C BAC / Label ry access / ess control Orizatio ace Restrict privileg ent Object. Grantin after si Contex Subject what the contex No m ies Tasks	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts access to data depends on the content of the gusers access after a specific condition. Expecific date/time. In determined the second of the content of the gusers access after a specific condition. Expecific date/time. In determined the second of the content of the gusers access after a specific condition. Expecific date/time. In determined the second of the content of the gusers access after a specific condition. Expecific date/time.	Prever Simular St	ective Rective Description of Test	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices was organization. Stop an attack. Recovery of a system attack. Vulnerability Desting Physical Testing attack. Vulnerability Desting Testing attack. Lenetration Testing attack to determine the prospect of the prospect	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assessment ng • System and Network Testing and Threat Modeling bability of the attack to the application ems n about the system n about attack against the system vetem vulnerabilities gainst the system attempting to gain come of the penetration test
physiological behave. Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege	RBAC) C BAC / Label y access / ess control Orizatio Restrict privileg Restrict object. Grantin after s Contex Subject what th No m ies ies Auditin	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control leviusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of angusers access after a specific condition. Expecific date/time. In determined to the performed by two or more people ges and Reporting • Vulnerability Assessment and Reporting • Vulnerability Assessment access access and Reporting • Vulnerability Assessment access and Reporting • Vulnerability Assessment access to object only to perform the process access acce	Prevented Simularian St	ective Rective Description Des	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system attack. Vulnerability Desting • Physical Testing at to determine the prospect of t	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESMENT Ing • System and Network Testing and Threat Modeling bability of the attack to the application ems In about the system In about attack against the system In stem vulnerabilities Igainst the system attempting to gain come of the penetration test Test Types about possible attack but very limited know about incoming attack except for
physiological behave. Physiological i.e. I.e. Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Retina Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern /	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit	RBAC) CC BAC / Label ry access / ess control Orizatio Restrict privilege Restrict object. Grantin after s Contex Subject what th No m ies ies Tasks ity Auditin Penetr Users a	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of the content	Prever Simular Simular Double	ective Rective Description of the content of the co	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of the prospec	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling Shability of the attack to the application ems In about the system In about attack against the system In about attack against the system In about attack against the system In about the system attempting to gain In accome of the penetration test Test Types Babout possible attack but very limited I know about incoming attack except for e organization who do not exchange
physiological behave. Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit	RBAC) C BAC / Label y access / ess control Orizatio ace Restrict privileger Restrict object. Granting after service what the Normalies acces acces and the Normalies acces a	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of the gusers access after a specific condition. Expecific date/time. Interest are given access to object only to perform they need to have. Interest are given access to object only to perform they need to have. Interest access to detail the performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. In to be monitored for reporting: Network Every medical control of the people of the peop	Prever Simular Doubly To Target	ective Rective Description of the control of the co	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of the prospect	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESMENT Ing · System and Network Testing and Threat Modeling Abability of the attack to the application ems In about attack against the system In about possible attack but very limited In about possible attack including In about possible of the attack, including
physiological behave. Physiological i.e. In the sense of	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict object. Granting after si Contex Subject what th No m ies ies Auditin Penetr Users a perforr Events Applica	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of the gusers access after a specific condition. Expecific date/time. Interest are given access to object only to perform they need to have. Interest are given access to object only to perform they need to have. Interest and the performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med.	Prevented Simulation St. Blind Double To Targe	ective Rective Descrive Description Des	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of the prospect	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences vithin Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESMENT Ing · System and Network Testing and Threat Modeling Abability of the attack to the application ems In about attack against the system In about possible attack but very limited In about possible attack including In about possible of the attack, including
physiological behave. Physiological i.e. I.e. Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern / Print Biometric Considerations Enrollment Time	gy allows the user to be authenticated based on zior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil	RBAC) C BAC / Label ry access / ess control Orizatio Restrict privileg Restrict object. Grantin after si Contex Subject what th No m ies ies Tasks ity Auditin Penetr Users a perform Events Applica Keystro	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requested access an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control level using a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It access to data depends on the content of the grant access after a specific condition. Expecific date/time. In gusers access after a specific condition. Expecific date/time. In gusers access to object only to perform they need to have. In the process of the performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Eventation Events • System Events • User Events	Prevented Records Simulation St. Blind Double To Target Zero-Kn	ective Rective Description of the control of the co	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices was organization. Stop an attack. Recovery of a system attack. Vulnerability Desting Physical Testing at to determine the prosystem of the prosy	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESMENT Ing • System and Network Testing and Threat Modeling Ibability of the attack to the application ems In about attack against the system In about possible attack but very limited Instruction of the penetration test Test Types Instruction about possible attack but very limited Instruction of the eorganization who do not exchange Instruction of the attack, including Instrategies Instruction of the target Instruction of the attack, including Instrategies Instruction of the target Instruction of the attack, including
physiological behave. Physiological i.e. In the sense of	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil	RBAC) C BAC / Label ry access / ess control Orizatio ace Restrict privileg Restrict object. Grantin after si Contex Subject what th No m ies Tasks ies Auditin Penetr Users a perform Events Applica Keystro Acces	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts access to data depends on the content of the desired process of the content of the desired process. In access to data depends on the content of the desired process after a specific condition. Expecific date/time. In determined the desired process to object only to perform they need to have. In the dependent control the same given access to object only to perform they need to have. In the dependent of the desired process are given access to object only to perform they need to have. In the dependent of the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the dependent control and the desired process are given access to object only to perform they need to have. In the definition of the desired process are given access to object only to perform the desired process are given access to object only to perform the desired process are given access to object only to perform the desired process are given access to object only to pe	Prevented Blind Double To Target Knowless	ective Rective Description of the control of the co	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of system. In Record information. Collect information. Collect information. Discover known sy. Penetration Organization knows an access. Document the outon penetration. Organization doesn't very few people in the information. Organization has price key details Penetration Test team doesn't known and the information. Test team doesn't known and the information. Test team doesn't known and the information and the information. Test team doesn't known and the information and	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assesment Ing · System and Network Testing and Threat Modeling Inabout the system In about attack against the system vulnerabilities Ingainst the system attempting to gain about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Instrategies In
physiological behave. Physiological i.e. In the sense of	gy allows the user to be authenticated based on vitor or characteristics. It is, retina, and fingerprints. It is, retina, and finger length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil Auditing and Repo	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict object. Access Auditing Penetric object. It also access / estrict object. Access Auditing Penetric object. Access Access Auditing Penetric object. Access Access Auditing Penetric object.	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It actions which can be performed with give ges. It actions access after a specific condition. Expecific date/time. It dependent control Its are given access to object only to perform they need to have. In ore or no less! Split to be performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Everation Events • System Events • User Events • oke Activity SCONTROL Types Example	Prevented Blind Blind Blind To Target Knowle Full Know	ective Rective Descrive Description	Reduce attack impact. Detect an attack before appens. Discourages an attack Define and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of system. In Record information. Collect information. Collect information. Discover known sy. Penetration Organization knows an access. Document the outon penetration. Organization doesn't very few people in the information. Organization has price key details Penetration Test team doesn't known and the information. Test team doesn't known and the information. Test team doesn't known and the information and the information. Test team doesn't known and the information and	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assesment Ing · System and Network Testing and Threat Modeling Inabout the system In about attack against the system vulnerabilities Ing gainst the system attempting to gain Income of the penetration test Test Types Inabout possible attack but very limited Indicate the system of the attack including Income of the penetration test Test Types Inabout possible attack but very limited Income of the penetration test Test Types Inabout possible attack but very limited Income of the penetration test Test Types Inabout possible attack but very limited Income of the penetration about the target or knowledge of the attack, including In Strategies In Incomplete the system of the target of the system of t
physiological behave. Physiological i.e. I.e. Physiological i.e. Voide Behavioral i.e. Voide Behavioral i.e. Voide Pattern / Print Biometric Considerations Enrollment Time Feature Extraction Accuracy Throughput Rate	gy allows the user to be authenticated based on vitor or characteristics. It is, retina, and fingerprints. It is, retina, and finger length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness. The rate which the system can scan and analyze.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil Auditing and Repo	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict object. Access Auditing Penetric object. It also access / estrict object. Access Auditing Penetric object. Access Access Auditing Penetric object. Access Access Auditing Penetric object.	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts Set actions which can be performed with give ges. Set access to data depends on the content of the grant access to data depends on the content of the grant access to object only to perform they need to have. Set are given access to object only to perform they need to have. Sore or no less! Split to be performed by two or more people and Reporting • Vulnerability Assessment attion Testing • Threat Modeling are responsible for what actions they have med. So to be monitored for reporting: Network Everation Events • System Events • User Events • Oke Activity So Control Types Bation of Concepts Data classification, data labeling, security awarence training.	Prevented Blind Blind Blind To Target Knowle Full Know	ective Rective Descrive Description	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability esting Physical Testing enetration Testing at to determine the prosystem. Record information. Collect information. Collect information. Discover known sy. A. Perform attacks ag access. Document the outon Penetration. Organization knows a knowledge. Organization doesn't very few people in the information. Organization has prickly details Penetration Test team doesn't known and the doesn't knowledge. The testing team known and the control organization's network A.K.A. black the testing team known and the control organization's network and the testing team known and the te	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling shability of the attack to the application ems In about the system In about attack against the system In stem vulnerabilities In gainst the system attempting to gain come of the penetration test Test Types about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies In ow any information about the target box testing. In ows public knowledge about the rik. In ows all available information regarding twork.
physiological behave. Physiological i.e. In the sense of	gy allows the user to be authenticated based on vitor or characteristics. It is, retina, and fingerprints. It is, retina, and finger length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil Auditing and Repo	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict object. Restrict object. Granting after since object. Subject what the Normalies Tasks in the Normalies Auditing Penetral Events Application (Keystro) ACCES Scope Administration of the Normalies of th	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects red access an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control lev using a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It actess to data depends on the content of the gusers access after a specific condition. Expecific date/time. It dependent control Its are given access to object only to perform they need to have. In the performed by two or more people and and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Eve ation Events • System Events • User Events • oke Activity Example Data classification, data labeling, security awarend training. Firewalls, IDS's/ IPS's, encryption, biometrics, si	Prevented Blind Blind Blind Toronto St. St. Zero-Kn Toronto St. Zero-Kn Toronto St. Target Zero-Kn Toronto St.	ective Rective Descrive Description	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices was norganization. Stop an attack. Recovery of a system an attack. Vulnerability Desting • Physical Testing and to determine the prospect of system. In Record information. Collect information. Collect information. Discover known synce access. Document the outer penetration was access. Document the outer penetration. Organization knows and access. Document the outer penetration. Organization has price key details Penetration Test team doesn't known and the organization's network A.K.A. black. The testing team known and the organization's network asswords. Passwords	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling shability of the attack to the application ems In about the system In about attack against the system In stem vulnerabilities In gainst the system attempting to gain come of the penetration test Test Types about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies In ow any information about the target box testing. In ows public knowledge about the rik. In ows all available information regarding twork.
physiological behave. Physiological i.e. I.e. Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern / Print Biometric Considerations Enrollment Time Feature Extraction Accuracy Throughput Rate False Rejection Rate (FRR) False Acceptance	gy allows the user to be authenticated based on vitor or characteristics. ris, retina, and fingerprints. cee pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness. The rate which the system can scan and analyze. The percentage of valid users that will be falsely rejected. Type 1 error. The percentage invalid users that will be falsely accepted.	Role-BAC (F Rule-BAC (F Rule-B	RBAC) CC BAC / Label ry access / ess control Orization ace Restrict object. Restrict object. Granting Auditing Penetry Users a perform Events Applicated Keystro ACCES Scope Administratorganizati personal. Restrict acces and access and acces an	Subject authorize according to security lal Used by owners to grant or deny access to other users. ACL defines the level of acces granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control leviusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It access to data depends on the content of access to date depends on the content of the ges. It access to date depends on the content of the grant access after a specific condition. Expecific date/time. It dependent control Its are given access to object only to perform they need to have. In or on less! Split to be performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Eve ation Events • System Events • User Events • oke Activity Scontrol Types Types Tirewalls, IDS's/ IPS's, encryption, biometrics, sicards, and passwords. Berimeter security Perimeter security Perimeter security Perimeter security	els. Corre Deter Direct Prever Reco Simulation St Blinct Doubl To Targe Zero-Kn To Roule Full Knowle F	ective Rective Descrive Description Des	Reduce attack impact. Detect an attack before appens. Discourages an attack before appens. Discourages an attack befine and document acceptable practices wan organization. Stop an attack. Recovery of a system an attack. Vulnerability besting Physical Testing and to determine the prospect of the prosp	combination to open a safety locker. Having fire extinguishers, having offsite data backups. e CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. Assesment Ing • System and Network Testing and Threat Modeling Inabout the system In about attack against the system system vulnerabilities Ingainst the system attempting to gain come of the penetration test Test Types about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies In St
physiological behave Physiological i.e. I Physiological i.e. I Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Facial Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern / Print Biometric Considerations Enrollment Time Feature Extraction Accuracy Throughput Rate False Rejection Rate (FRR)	gy allows the user to be authenticated based on vitor or characteristics. ris, retina, and fingerprints. cee pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness. The rate which the system can scan and analyze. The percentage of valid users that will be falsely rejected. Type 1 error.	Role-BAC (F Rule-BA Hybrid RE Lattice based Non-discretionar Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil Auditing and Report Type Administrative Controls Logical /	RBAC) CC BAC / Label ry access / ess control Orization ace Restrict object. Restrict object. Granting Auditing Penetry Users a perform Events Applicated Keystro ACCES Scope Administratorganizati personal. Restrict acces and access and acces an	Subject authorize according to security lat Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control leviusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It access to data depends on the content of access to date depends on the content of access after a specific condition. Expecific date/time. It dependent control Its are given access to object only to performely need to have. In or on less! Split to be performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Eve ation Events • System Events • User Events • oke Activity SCONTROL Types The Younge of the Control Types The	els. Corre Deter Direct Prever Recco Simulation St Blind Doubl To Targe Knowle Full Knowle Full Knowle Full Knowle Full Knowle Co	ective Rective Rective Determination Approximation Approxi	Reduce attack impact. Detect an attack before appens. Discourages an attack befine and document acceptable practices wan organization. Stop an attack. Recovery of a system at attack. Vulnerability esting • Physical Testing at to determine the prosystem. In Record information. Collect information. Collect information. Discover known sy. A. Perform attacks ag access Document the outon penetration. Organization knows a knowledge. Organization doesn't very few people in the information. Organization has price key details Penetration Test team doesn't known and the organization's new organization's	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). I. User identification and authentication, fences Within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. I. Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling I. Spatial the system and about the system valuerabilities gainst the system attempting to gain about attack against the system verse vulnerabilities gainst the system attempting to gain about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies I. Strategies
physiological behave Physiological i.e. Iele Behavioral i.e. Voi Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Retina Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern / Print Biometric Considerations Enrollment Time Feature Extraction Accuracy Throughput Rate False Rejection Rate (FRR) False Acceptance Rate (FAR)	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. ce pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness. The rate which the system can scan and analyze. The percentage of valid users that will be falsely rejected. Type 1 error. The point at which FRR equals FAR. This is expressed as a percentage - lower CER is better.	Role-BAC (F Rule-BAC (F Rule-B	RBAC) CC BAC / Label ry access / ess control Orizatio ace Restrict object. Restrict object. Granting after since Context Subject what the Normalies Tasks ites Ity Auditing Penetral Lysers aperform Events Applicating Events Applications Events Events Applicat	Subject authorize according to security lat Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requacess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control leviusing a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It access to data depends on the content of access to date depends on the content of access after a specific condition. Expecific date/time. It dependent control Its are given access to object only to performely need to have. In or on less! Split to be performed by two or more people and Reporting • Vulnerability Assessment ation Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Eve ation Events • System Events • User Events • oke Activity SCONTROL Types The Younge of the Control Types The	els. Corre Deter Direct Prever Reco Simulation St Blinc Doubl To Targe Zero-Kn To Pa Knowle Full Knowl	ective Rective Rective Description of the certification of the certifica	Reduce attack impact. Detect an attack before appens. Discourages an attack before appens. Discourages an attack befine and document acceptable practices was norganization. Stop an attack. Recovery of a system as an attack. Vulnerability besting Physical Testing as to determine the prosystem. I. Record information. Collect information. Discover known sy. A. Perform attacks as access. Document the outon penetration. Organization doesn't very few people in the information. Organization has prick key details Penetration Test team doesn't known as knowledge. Penetration	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling Subability of the attack to the application ems In about attack against the system In about possible attack but very limited Come of the penetration test Test Types about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies In owa any information about the target box testing. In ows public knowledge about the rk. In ows all available information regarding twork. In owa and incoming attack except for exception and lowercase letters. Combination of two unmatching dictionary words. Requires that a long phrase be used. Passwords that are valid for a single session login.
physiological behave Physiological i.e. Iele Behavioral i.e. Voi Behavioral i.e. Voi Fingerprint Hand Geometry Hand Topography Palm or Hand Scan Retina Scan Retina Scan Retina blood vessel scan Vascular Scans Voice print Signature Dynamics Keystroke Dynamics Voice Pattern / Print Biometric Considerations Enrollment Time Feature Extraction Accuracy Throughput Rate False Rejection Rate (FRR) False Acceptance Rate (FAR) Crossover Error	gy allows the user to be authenticated based on vior or characteristics. ris, retina, and fingerprints. cee pattern Physiological Characteristics Scans the thumb or edge of the finger. Size, shape, bone length, finger length, or other layout attributes of a user's hand are taken. Hand peaks and valleys pattern. Fingerprint and geometry combination of palm. Facial features such as bone, eye length, nose, chin shape etc. Retina blood vessel scan. Scans the colored part of the eye around the pupil. Scans the pattern of the veins in the users hand or face. Verify speech sound patterns. Scanning Behaviors Pen pressure and acceleration is measured. Scan the typing pattern. Measures the sound pattern of a user read particular word. Does not change throughout human life and unique. High accuracy rate. Sample processing for use by the biometric system. The process of obtaining the information from a collected sample. Scan the most important elements for correctness. The rate which the system can scan and analyze. The percentage of valid users that will be falsely rejected. Type 1 error. The point at which FRR equals FAR. This is expressed as	Role-BAC (F Rule-BAC Hybrid RE Lattice based Non-discretional Mandatory-Acce Auth Constrained Interf Applications Content-Depende Work Hours Least Privilege Separation of Dut and Responsibilit User Accountabil Auditing and Report Type Administrative Controls Logical / Technical Controls Physical Controls Procedical Regular user accountabile	RBAC) CC BAC / Label y access / ess control Orization ace Restrict object. Ent Granting after since Context Subject what the Norm ies ies Tasks ies Auditing Penetral Applications Acces A	Subject authorize according to security lat Used by owners to grant or deny access to other users. ACL defines the level of access granted or denied to subjects. Task-based access controls - subjects requaccess an object based on its role or assigned tasks. Uses a set of rules or filters to define what can or cannot be done on a system. Limited RBAC Objects are classified based on control levising a label. Based on policies defined by a central authority. Role based or task based. In Methods / Concepts It actions which can be performed with give ges. It actions which can be performed with give ges. It actions which can be performed with give ges. It actions which can be performed by the content of guine saccess to object only to perform help need to have. In the performed by two or more people grand Reporting • Vulnerability Assessment attorn Testing • Threat Modeling are responsible for what actions they have med. It to be monitored for reporting: Network Everation Events • System Events • User Events • oke Activity SCONTROL Types Tirewalls, IDS's/ IPS's, encryption, biometrics, sincards, and passwords. Perimeter security, biometrics and cabling.	els. Corre Deter Direct Prever Reco Simulation St Blinc Doubl To Targe Zero-Kn To Pa Knowle Full Knowl	ective Rective Rective Descrive and antative Sovery Rective and antative Sovery Rective an attack depends on the control of th	Reduce attack impact. Detect an attack before appens. Discourages an attack before appens. Discourages an attack befine and document acceptable practices was organization. Detected a system as a system as a system and attack. Vulnerability besting Physical Testine enetration Testing as to determine the prospect of t	combination to open a safety locker. Having fire extinguishers, having offsite data backups. CCTV, intrusion detection systems (IDS). er. User identification and authentication, fences within Acceptable Use Policy (AUP) Locks, biometric systems, encryption, IPS, passwords. after Disaster recovery plans, data backups etc. ASSESSMENT Ing • System and Network Testing and Threat Modeling Inabout the system In about attack against the system stem vulnerabilities gainst the system attempting to gain come of the penetration test Test Types about possible attack but very limited know about incoming attack except for e organization who do not exchange or knowledge of the attack, including Strategies low any information about the target box testing. Dows public knowledge about the rk. Single word usually a mixture of upper and lowercase letters. Combination of two unmatching dictionary words. Requires that a long phrase be used. Passwords that are valid for a single