Protokoły – skróty:

- SRTP – Secure Real Time Protocol (w VoIP używany)
- NTP – Network Time Protocol
- S/MIME – Secure/Multi Purpose Mail Extension
- POPv3 & IMAPv4
- HTTPS
- IPSEC – Internet Protocol Security
- FTP – File Transfer Protocol
- FTPs – File Transfer Protocol Secure
- SFTP – SSH File Transfer Prtocol
- LDAP
- SNMP – Simple Network Management Protocol
- SMTP

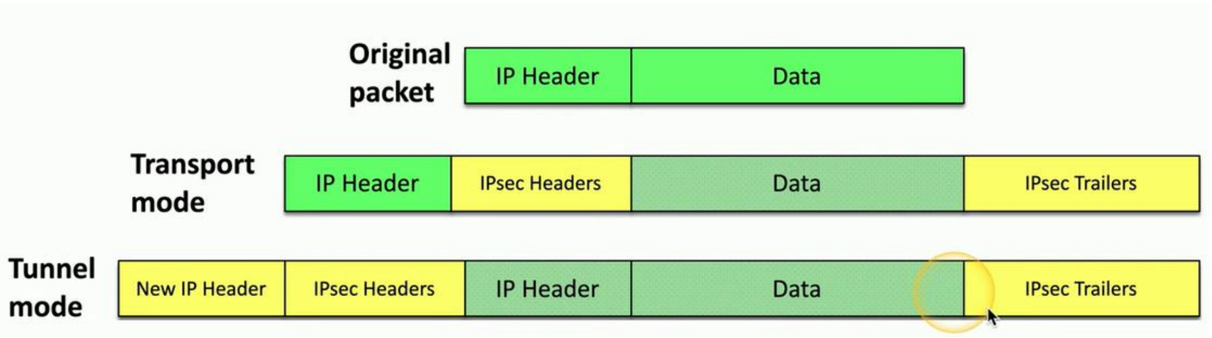
Protokół	Port	Bezpieczny odpowiednik	Port	Zabezpieczenia/komentarz	Layer
SRTP		Protokół jest bezpieczny		- encryption - signing	
NTP	123	NTPsec			
S/MIME		Protokół jest bezpieczny		- encryption - signing	
POP v3	110	STARTTLS extension	995		
IMAP v4	143	STARTTLS extension	993		
SMTP	25	SMTPS - deprecated TLS-based method for securing SMTP SMTP1 I 2 - cleartext			
HTTPS	443	Protokół jest bezpieczny			
IPSEC		Protokół jest bezpieczny		-confidentiality, integrity, anti-replay - authentication & encryption	3
FTP	21	FTPs	989, 990		
		SFTP	22		
LDAP	389	LDAPs	636	X.500 directory	
DNS	53	DNSSEC		- signed DNS records - no encryption	
SNMPv3	161	Protokół jest bezpieczny		v.1 I v.2 nie są bezpieczne i nie mają szyfrowania v.3: - encryption, authentication, and hashing (integrity)	

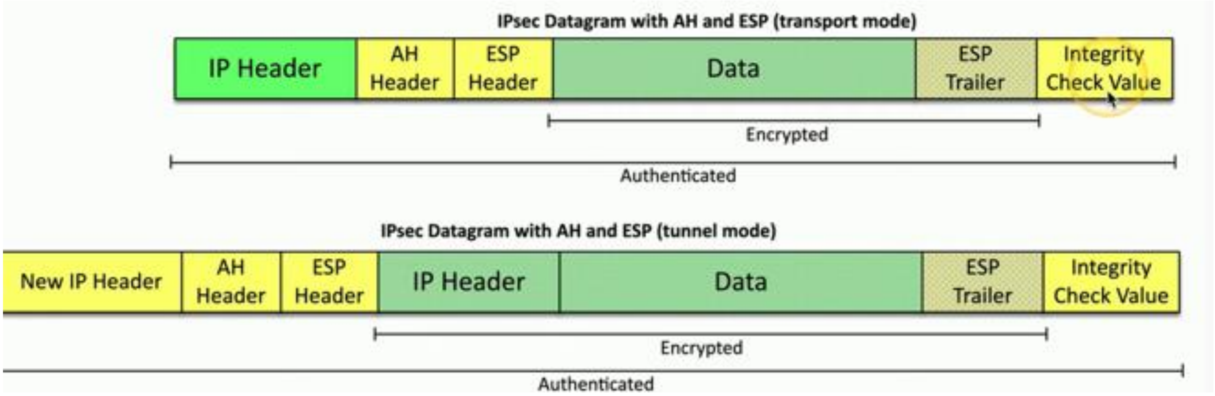
DHCP		Nie jest bezpieczny, konieczny DHCP snooping			
Telnet	23	SSH	22		
RDP	3389				
kerberos	88				
L2TP	1701				
TFTP	69				
radius	1812				

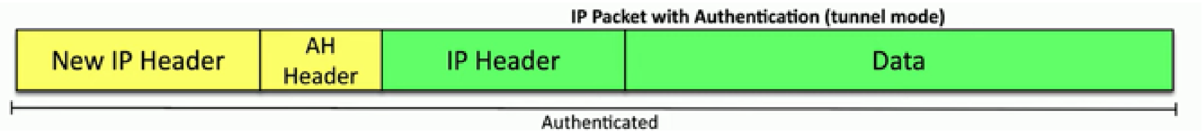
Protokół	Co robi
MIME	Multipurpose Internet Mail Extensions (MIME) specification extends the email message format beyond simple text, enabling the transfer of graphics, audio, and video files over the Internet mail system
RTP	real-time delivery of audio and video over an IP network
POP3 (110 & 995)	Protocol for retrieving emails from a server, POP3 downloads an email from the server then deletes it. POP3 doesn't allow to organize emails in the mail server mailbox
IMAP4 (143 & 993)	Protocol for retrieving emails from a server, IMAP stores the email on the server and syncs it across several devices to access over multiple channels. IMAP allows to organize emails in the mail server mailbox
SMTP (port 25)	Transmitting emails

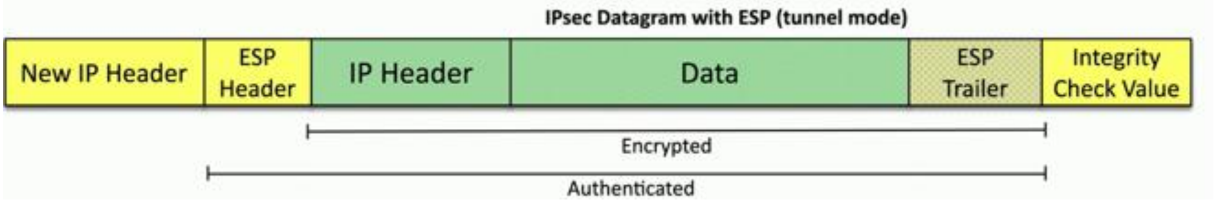
IPSEC budowa:

- Zasadniczo są AH (Authentication Header) i ESP (Encapsulation Security Payload)
- AH = integrity (hash), prevents replay attack (sequential numbers), authentication (guarantee data origin)
- ESP = encryption, authentication
- Jest kilka trybów (modes):
    - Transport mode
    - Tunnel mode









Pojęcia:

- DHCP snooping – kontrola ruchu sieciowego DHCP, tak aby pochodził z zaufanych źródeł, ang.: distribution is only allowed from trusted interfaces, DHCP servers must be authorized
- UEFI - Unified Extensible Firmware Interface, it is a firmware interface designed as a replacement for BIOS. UEFI offers a variety of improvements over BIOS, including Graphical User Interface (GUI), mouse support, or secure boot functionality designed to prevent the loading of malware and unauthorized operating systems during the computer startup process.
- Measured Boot - refers to a security mechanism first introduced by Microsoft in Windows 8. Measured Boot checks system startup components and stores the resulting boot configuration log in the Trusted Platform Module (TPM). The log is then sent for remote attestation to a trusted server on the network to verify the integrity of the Windows startup process. Measured Boot allows for neutralization of hard-to-detect malware and rootkits which are run before the OS.

- SED – Self Encrypting Drive, no operating system, hardware encryption
- FDE – Full Disk Encryption
- TPM – Trusted Platform Module
- HSM – Hardware Security Module
- WPA – WiFi Protected Access
- SAE – Simultaneous Authentication of Equals
- EAP – Extensible Authentication Protocol
- EAPOL – Extensible Authentication Access Protocol over LAN (802.1x)
- COPE – Corporate Owned Personally Enabled
- BYOD – Bring Your Own Device
- CYOD – Choose Your Own Device
- MAM – Mobile Application Management
- MCM – Mobile Content Management
- UEM – Unified Endpoint Management, combines features of MDM, EMM, MAM
- OTA – updates Over The Air
- OTG – USB On The Go
- RCS – Rich Communication Services - is a communication protocol between mobile telephone carriers and between phone and carrier, aiming at replacing SMS messages with a text-message system that is richer, provides phonebook polling, and can transmit in-call multimedia
- KBA = Knowledge Based Authentication (static, dynamic)
- IdP – Identity Provider
- SED – Self Encrypting Drive (no operating system, hardware encryption)
- FDE – Full Disk Encryption (BitLocker, VileVault)
- Carrier unlocking – uwolnienie telefonu od dostawcy usług
- VMI – Virtual Mobile Infrastructure
- IAM – Identity Access Management
- AZ – Availability Zone
- Root CA -> Intermediary CA / Subordinate CA-> Issuing CA / Leaf CA
- Impossible travel / risky login – using AI/ML to determine if authentication try was risky
- PSK – Pre Shared Key

Boot security:

- Chain of trust to następujące po sobie fazy: secure boot, trusted boot, measured boot
- Starts at TPM / HSM
- UEFI BIOS Secure Boot
- Secure boot verifies the bootloader – checks the bootloader's digital signature, if it's signed with a trusted certificate
- Trusted boot: bootloader verifies digital signature of OS kernel
    - The kernel verifies all of the startup components: boot drivers, startup files
    - Just before loading the drivers ELAM (Early Launch Anti Malware) starts checking every driver if it is trusted
- Measured boot
    - Remote attestation – verification report, encrypted and signed with TPM

Narzędzia monitoring I Bezpieczeństwa:

- DLP
- EDR – Endpoint Detection & Response (nie tylko bazuje na sygnaturach, ale może też na zachowaniu)
- NGFW – Next Generation Firewall, inne nazwy: OSI App Layer Gateway, Deep Packet Inspection, Stateful Multilayer Inspection
- HIDS / HIPS
- IDS / IPS
- Host-based firewall – najczęściej program (software), bazujący na IP, protokole, porcie
- SOAR – pobiera dane z różnych narzędzi, w tym z EDR, SIEMa, może robić tickety, alerty
- CASB – Cloud Access Security Broker
- UTM – Unified Threat Management (inna nazwa: Web Security Gateway), łączy ze sobą wiele funkcjonalności, między innymi: URL filter, SPAM filter, IPS, IDS, router, switch, VPN endpoint, malware inspection
- WAF – Web Application Firewall
- Next-Gen SWG – Security Web Gateway – examine API calls, JSON strings, combines features of multiple tools: CASB, DLP

Load balancing / Networking:

- Active-active
- Active-passive – część serwerów wyłączona
- Round-robin – pokolei wybierane serwery, to samo obciążenie każdego
- East-west traffic – within data centers
- Dynamic round-robin – load to server with minimum use
- Affinity – user stuck to the same server
- Always-on VPN
- L2TP – Layer 2 Tunneling Protocol, commonly implemented with IPSec
- PPTP – Point to Point Tunneling Protocol
- NAC - Network Access Control
- dissolvable agent
- agentless
- Out-of-band management - refers to a network device management technique that enables device access through a dedicated communication channel separate from the network where a given device operates
- Extranet – similar design to DMZ, dedicated for vendors, supplyers
- Intranet – only available internally, internal or VPN access only
- VPN concentrator – encrypts and decrypts data
- HTML5 VPN
- Full tunnel – cały czas przez VPN concentrator
- Split tunel – jak chcemy dostać się do strony spoza organizacji to nie musimy iść przez VPN concentrator
- Site-to-site VPN – VPN concentrator po obu stronach
- STP – Spanning Tree Protocol
- BPDU – Bridge Protocol Data Unit:
    - Workstation don't send BPDU, if BPDU frame is seen on a PortFast interface, shut down the interface, it is mechanism to prevent loops
- Stateless firewall:

  - Musi mieć ruch w obie strony zdefiniowany osobno
- Statefull firewall:
  - ACL and session table
- Tap – capture network, physical device

Figure 1 Network tap

- Mirror – capture network, software build-in to switch (SPAN – Switched Port Analyzer)
- Out-of-band connection – separate management interface in network applicance (out-of-band NIC)
- ACL – Access Control List – list of rules for firewall
- Posture assessment – before connecting device to the network, check antivirus, disc encryption etc
- Captive portal – authentication page to connect to the network
- Heatmap – wireless signal strength
- Site survey – chodzenie po budynku I szukanie access pointów
- 2.5 GHZ:
  - Tylko 14 channel
  - Żeby nie było overlappingu to musi być różnica 5 minimum: 1,6,11
- Dissolvable agents – no installation required, runs during posturę assesment and terminates then, user downloads the agent, agent is run once and disappear
- Agentless NAC – integrated with AD, check during login / logoff
- Reverse proxy – loadbalancer is reverse proxy, ukrywa tożsamość serwera
- Transparent proxy – niewidoczne dla użytkownika
- Forward proxy – user -> internet
- Passive monitoring – no way to block in real time, IPS not inline
- Inline monitoring – better (in-band)
- Out-of-band response – after the fact, IPS sends TCP RST frames
- Point-to-point – between buildings
- Ad hoc mode - A wireless ad hoc network (WANET) is a type of local area network (LAN) that is built spontaneously to enable two or more wireless devices to be connected to each other without requiring typical network infrastructure equipment, such as a wireless router or access point
- Tethering/hotspot - You can use your phone's mobile data to connect another phone, tablet, or computer to the internet. Sharing a connection this way is called tethering or using a

hotspot. Some phones can share Wi-Fi connection by tethering. Most Android phones can share mobile data by Wi-Fi, Bluetooth, or USB

- Multiple fat (thic) access points needs to be managed individually
- Multiple thin access points can be managed centrally

Authentication:

- 802.1x
  - Port-based network access control
  - Central authentication
  - Used with RADIUS/ LDAP / TACACS+
  - EAPOL - Extensible Authentication Access Protocol over LAN (802.1x)
- 802.11x
- 802.11ac
- Supplicant – urządzenie, które chce uzyskać dostęp, klient
- Authenticator – urządzenie, które będzie umożliwiało dostęp do sieci
- Authentication Server – validates the client credentials
- EAP - Extensible Authentication Protocol - authentication framework frequently used in wireless networks and point-to-point connections. EAP provides an authentication framework, not a specific authentication mechanism. There are many authentication mechanisms (referred to as EAP methods) that can be used with EAP. Wireless networks take advantage of several EAP methods, including PEAP, EAP-FAST, EAP-TLS, and EAP-TTLS.
- EAP-FAST
  - EAP Flexible Authentication via Secure Tunneling
  - AS and supplicant share a protected access credential (**PAC**) (shared secret)
  - AS and supplicant mutually authenticate and negotiate **TLS tunnel**
  - User authentication occurs over the TLS tunnel
  - Need RADIUS
- PEAP
  - Protected EAP
  - Created by CISCO, Microsoft, RSA Security
  - AS uses **digital certificate** instead of PAC, client doesn't need certificate
  - Also establish **TLS tunnel**
  - User authenticate via MSCHAPv2
  - User can also authenticate with GTC (Generic Token Card)
- LEAP
  - Lightweight EAP
  - Clear text transmission
  - deprecated
- EAP-TLS
  - Highest level of security of: PEAP, EAP-FAST, EAP-TLS, EAP-TTLS (czemu: nie masz sekretu współdzielonego jak w FAST, masz certyfikaty po obu stronach, a nie tylko po jednej jak w PEAP i EAP TTLS)
  - relies on **client-side and server-side certificates** for mutual authentication
  - Also establish **TLS tunnel**
  - PKI needed
  - Not all devices can support the use of digital certificates – tu mogą być czasem problemy

- EAP-TTLS
    - EAP Tunneled TLS
    - **Digital certificate on AS only**
    - Also establish **TLS tunnel**
    - Gives possibility to use any authentication method inside the TLS tunnel: other EAPs, MSCHAPv2, anything else
- WEP
    - has been deprecated in favor of newer standards due to known vulnerabilities resulting from implementation flaws
    - RC4 Stream encryption scheme in use
    - deprecated and should not be used due to their known vulnerabilities
- WPA
    - TKIP encryption scheme in use
- WPA2
    - AES-CCMP (Counter/CBC-Mac Protocol) encryption scheme in use
    - 4-way handshake (sprawdzić)
    - Fully implemented 802.11i standard
- WPA3
    - highest level of protection of: WEP, WPA, WPA2, WPA3
    - AES-CCMP, AES-GCMP (Galouis/Counter Mode Protocol) encryption scheme in use
    - No more handshaking
    - Mutual authentication
    - Perfect Forward Secrecy added (SAE), also known as Dragonfly Key Exchange
    - Not vulnerable to KRACK attack like WPA2 due to the SAE
- WPA3-SAE
    - the best solution for securing a small network that lacks an authentication server
    - SAE used as an client authentication method in WPA3 Personal mode
    - WPA3-PSK
- WPA2-Enterprise
    - Requires RADIUS authentication server
- WPA2-PSK
    - PSK used as an client authentication method in WPA2 Personal mode
- WPA3-Enterprise
    - Requires RADIUS authentication server
    - WPA3-802.1x
- WPS
    - Wi-Fi Protected Setup, called WiFi Simple Config
    - Allows easy setup of mobile device: PIN, NFC, push button on access point
    - simplifies configuration of new wireless networks by allowing non-technical users to easily configure network security settings and add new devices to an existing network
    - deprecated and should not be used due to their known vulnerabilities
    - WPS attack: 8 digit PIN, 7 digit and checksum, first half – 4 digits, second half – 3 digits
- CHAP - Challenge Handshake Authentication Protocol
    - remote access authentication protocol that **periodically re-authenticates client** at random intervals to prevent session hijacking.

  - 3-way handshake – **encrypted challenge sent over the network**
  - Clients respond with hash calculated from challenge and password
- MS-CHAP
  - Microsoft's implementation of CHAP
  - Used commonly on Microsoft's PPTP (Point-To-Point Tunneling Protocol)
  - Not secure – uses DES
- PAP
  - Password Authentication Protocol
  - obsolete authentication protocol that sends passwords in cleartext
- RADIUS
  - Primarily used for network access
  - Combines authentication and authorization
  - Encrypts only the password in the access-request packet
- Shibboleth
  - Based on SAML
  - Control attributes sending to app
- SAML
  - Federation
  - Security Assertion Markup Language
  - Authentication and authorization
  - Not originally designed for mobile apps
- oAuth
  - Federation
  - open standard for Authorization
  - no Authentication
  - created by Twitter, Google
- OpenID
  - Federation
  - Protocol for Authentication
  - Cooperating sites are called Relying Parties (RP)
- TACACS
  - Terminal Access Controller Access-Control System
  - Alternative to RADIUS
- TACACS+
  - Encrypts the entire payload of the access-request packet
  - Primarily used for device administration
  - Separates authentication and authorization
  - The latest and most common version
  - Probably cisco device
  - TCP 49 port
  - No backward compatible
- XTACACS
  - Extended TACACS
  - Additional support for accounting and auditing
  - Developed by CISCO
- Smart card – contains a chip, typically combined with MFA

Network access control models:

- DAC – Discretionary Access Control
    - access control model based on user identity. In DAC, every object has an owner who at his/her own discretion determines what kind of permissions other users can have to that object
    - in most operating systems
- ABAC – Attribute Based Access Control
    - access control model defines access control rules with the use of statements that closely resemble natural language
    - combine multiple parameters: resource, IP address, time of day, desired action
- MAC – Mandatory Access Control
    - Users are not allowed to change access policies at their own discretion
    - Labels and clearance levels can only be **applied** and changed **by an administrator**
    - Every resource has a sensitivity label matching a **clearance level** assigned to a user
    - the strictest set of access rules
    - the most secure
    - every object gets a **label**: confidential, secret, top secret
- RBAC – Rule/**Role Based Acces Control**
    - **Group-based** access control in MS Windows environments (**Role based**)
    - An access control model in which access to resources is granted or denied depending on the contents of Access Control List (**ACL**) entries (**Rule based**) ACL = Rule based
    - Implemented in network devices such as firewalls to control inbound and outbound traffic based on filtering rules (Rule based)
- Conditional access – ten ma dostęp, ten nie ma, ten ma MFA, ten tylko musi się zalogować
- PAM – Privileged Access Management
- F**ACL**:
    - rule-based access control mechanism associated with files and/or directories
    -

Ten hack z 7 cyframi, co miało być 8 to jest: WPS hack

Jailbreaking = iOS

Rooting = Android

Certyfikaty - pojęcia:

- RA – Registration Authority
    - Accepting requests for digital certificates
    - Authenticating the entity making the request
    - Issuing digital certificates
    - Responsible for revocation
- PKI - hierarchical system for the creation, management, storage, distribution, and revocation of digital certificates
- CA - trusted third party that issues digital certificates used for creating digital signatures and public-private key pairs
- IKE?
- OCSP – Online Certificate Status Protocol
    - allow to check whether a digital certificate has been revoked
    - the fastest way for checking the validity of a digital certificate
    - communication via HTTP

- Stapling:
    - allows for checking digital certificate revocation status without contacting Certificate Authority (CA)
    - append staple in the initial TLS handshake
- Pinning:
    - deprecated security mechanism designed to defend HTTPS websites against impersonation attacks performed with the use of fraudulent digital certificates
- EV – Extended Validation:
    - Extended Validation (EV) certificates provide the highest level of trust and protection
    - Green in the browser
- Certificate chaining
    - process of verifying authenticity of a newly received digital certificate. Such process involves checking all the certificates in the chain of certificates from a trusted root CA, through any intermediate CAs, down to the certificate issued to the end user. A new certificate can only be trusted if each certificate in that certificate's chain is properly issued and valid
- root cert – na CA
- SAN – Subject Alternative Name:
    - Allow cert to support many domains
- CRL – Certificate Revocation List
- Pinning:
    - Pinning is the process of associating a host with their expected X509 certificate or public key. Once a certificate or public key is known or seen for a host, the certificate or public key is associated or 'pinned' to the host
    - To samo ale dla aplikacji
- Web of Trust – no CA
- Key escrow – private keys in 3rd party
-

Formaty certów:

- DER
    - Encoded in binary format
    - Generally used for Java servers
    - .der and .cer file extensions
- PEM:
    - Encoded in text (ASCII Base64) format
    - Generally used for Apache servers or similar configurations
    - pem, .crt, .cer and .key file extensions
- PFX & P12:
    - Encoded in binary format
    - Generally used for Microsoft windows servers
    - .pfx and .p12 file extensions
    - Store many X.509 certificates in a single .p12 .pfx file
    - Requiring password to open
    - Można to skonwertować do PEM za pomocą OpenSSLa
- P7B:
    - Encoded in text (ASCII Base64) format

    - Generally used for Microsoft windows and Java Tomcat servers
    - .p7b file extension
- CER:
    - Can be encoded as binary DER format or the ASCII PEM format
    - Usually contains a public key, private keys would be transferred in the .pfx file format
    - Common format for Windows certificates

Inne skróty, pojęcia:

- SASL – Simple Auth and Security Layer:
    - Framework to communicate securely
- Sposoby wykrywania anomalii I zagrożeń:
    - heuristic (dużo czegoś) – wykorzystanie AI
    - signature – elementy w kodzie binarnym
    - anomaly-based – network utilization, file transfers
    - behavior-based – find SQLI
    -
- UAC – Windows User Account Control
- IPv6 = multicast nie broadcast
- FIM – File Integrity Monitoring
- SFC – System File Checker, Windows
- Tripwire – file integrity monitoring on Linux
- MIC – Message Integrity Check
- PAN – Personal Area Network
- TRNG – True Random generator
- IMA – Integrity Measurement Architecture – open source alternative that creates measured runtime environment, creates a list of components that need to load, anchors that list to TPM
- Stress testing- placing load on the system to see where the performance and usability breakpoints exists
- WAP – Wireless Access Protocol
- OID – Object Identifiers
    - Incorporated into PKI and used to assign one or more certificate policies to a given CA
    - AD Cert Services
    - Enable organization PKI to work with another's organization PKI
- ABAC:
    - PEP – Policy Enforcement Point
    - PDP – Policy Decision Point
    - PIP – Policy Information Point
- Opal – specification for SEDs
- WiFi analyzer - diagnostic tool that can be used for measuring wireless signal strength
- Bluetooth - popular, 2.4 GHz short-range wireless technology used for connecting various personal devices in a WPAN
- IR- short distance, line-of-sight technology used for example in home remote controls

- Storage segmentation - A mobile security solution that enables separate controls over the user and enterprise data
- Containerization - In the context of MDM, the isolation of corporate applications and data from other parts of the mobile device is referred to as