**900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7**

**LEARNER GUIDE**

**MODULE THREE (3)**

|  |  |
| --- | --- |
| **Module #** | 900103-000-00-KM-03 |
| **NQF Level** | 4 |
| **Notional hours** | 70 |
| **Credit(s)** | 7 |
| **Occupational Code** | 900103-000-00-00 |
| **SAQA QUAL ID** | SP - 220330 |
| **Qualification Title** | Cybersecurity Defender |

|  |  |
| --- | --- |
| **Name** |  |
| **Contact Address** |  |
| **Telephone (H)** |  |
| **Telephone (W)** |  |
| **Facsimile** |  |
| **Cellular** |  |
| **E-mail** |  |

**Note to the learner**

This Learner Guide provides a comprehensive overview of the module. It is designed to improve the skills and knowledge of learners, and thus enabling them to effectively and efficiently complete specific tasks.

**Purpose of the Module**

The main focus of the learning in this knowledge module is to build an understanding of the cybersecurity measures and checks to be implemented to defend a company against malicious attacks and breaches of information

The learning will enable learners to demonstrate an understanding of:

* KM-03-KT01 : End-user access point security 10%
* KM-03-KT02 : Types of cybersecurity software/tools 20%
* KM-03-KT03 : Encryption 15%
* KM-03-KT04 : Personal security 20%
* KM-03-KT05 : Mobile Security 20%
* KM-03-KT06 : Password protection 15%

**Entry Requirements**

NQF 3 (Gr 11) with Computer Literacy, English and Math Lit

**Provider Accreditation Requirements for the Knowledge Module**

*Physical Requirements:*

* The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the application modules
* QCTO/ MICT SETA requirements

*Human Resource Requirements:*

* Lecturer/learner ratio of 1:20 (Maximum)
* Qualification of lecturer (SME):

NQF 5 qualified in industry recognised qualifications with 1 years’ experience in the IT industry

Cybersecurity vendor certification

* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* Legal (product) licences to use the software for learning and training
* OHS compliance certificate
* Ethical clearance (where necessary)

AM

*Physical Requirements:*

* Valid licenses software and application, including OS.
* Internet connection and hardware availability.
* Examples and information specified in the scope statement and all the case studies, scenarios and access to hardware and software implied in the scope statements of the modules.
* Remote learners: Provider must provide business IT simulation system (e.g. invoice processing).

*Human Resource Requirements:*

* Qualification of lecturer (SME):  
  o NQF 5 industry recognised qualification with 1 year relevant experience
* Assessors and moderators: accredited by the MICT SETA

*Legal Requirements:*

* + Legal (product) licences to use the software for learning and training
  + OHS compliance certificate
  + Ethical clearance (where necessary)

**Venue, Date and Time:**

Consult your facilitator should there be any changes to the venue, date and/or time.

Refer to your timetable.

**Assessments**

**Associated Assessment Criteria (AACs)**

* Basic governance principles and concepts related to cybersecurity are understood.
* Basic concepts and principles of cybersecurity are understood.
* Basic concepts and principles of cyber threats and attacks are understood.
* Basic concepts and principles of cyber defence are understood.
* Ethical considerations in ethical hacking and penetration testing are understood.
* Procedures to respond to cybersecurity incidents are understood.

**Associated Assessment Criteria (AACs)**

* User and host identities are verified.
* Mechanisms are put in place to prevent system intrusions.
* Automated tools are used to guard against intrusions.
* Network confidentiality is ensured.
* The security posture is evaluated to detect vulnerabilities and to enhance resilience.

**Associated Assessment Criteria (AACs)**

* Threats to the cybersecurity of the company are detected.
* Adversary techniques, tactics and practices (TTPs) are emulated
* using an emulation platform.
* Network traffic is monitored and analysed using a suitable platform.
* Incidents are identified, responded to and reported.

**Associated Assessment Criteria (AACs)**

* Foot-printing tools are used against a target and intelligence is gathered.
* Vulnerabilities are identified using penetration testing tools.
* Servers and devices are attacked to build better defences.
* Clients are manipulated to uncover internal threats.
* Targets are exploited to increase cybersecurity.

Antivirus and intruder detection systems (IDS) are tested

# PURPOSE OF THE QUALIFICATION

Cybersecurity Defenders are responsible for proactively protecting organisations’ systems from attacks, they are the first line of defence against cyberattacks, the first responders to cybersecurity breaches and are responsible for the hardening of the information systems of organisations ensuring compliance with legislation

# QUALIFICATION RULES

This Skills Programme consist of two components namely Knowledge/Theory component and Application component. The following are compulsory modules in each of the two components:

**Knowledge/Theory Component:**

The following Modules are compulsory:

* 900103-000-00-KM-01, Cyber Defence Introduction, NQF Level 4, Credits 7
* 900103-000-00-KM-02, Cyber Threats and Attacks, NQF Level 4, Credits 7
* 900103-000-00-KM-03, Cybersecurity, NQF Level 4, Credits 7
* 900103-000-00-KM-04, Responding to Cybersecurity Incidents, NQF Level 4, Credits 5

Total number of credits for Knowledge Component: 26

**Application Component:**

* 900103-000-00-PM-01, Protect against cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-02, Detect cybersecurity threats, intrusions and attacks, NQF Level 4, Credits 11
* 900103-000-00-PM-03, Conduct Penetration Testing Techniques to Determine Security, NQF Level 4, Credits 12

Total number of credits for Application Component: 34

# EXIT LEVEL OUTCOMES

**Exit Level Outcomes (ELO) 1**

Demonstrate knowledge and understanding of cybersecurity, cyber

threats and attacks and cyber defence

**Exit Level Outcomes (ELO) 2**

Protect against cybersecurity intrusions and attacks

**Exit Level Outcomes (ELO) 3**

Detect cybersecurity threats and attacks

**Exit Level Outcomes (ELO) 4**

Use different penetration testing tools to identify vulnerabilities in the security posture of an organisation

# KM-03-KT01: End-user access point security 10%

**Topic elements to be covered include:**

* KT0101 Organisation network infrastructure basics and weaknesses
* KT0102 The web and common attacks
* KT0103 Using an operating system
* KT0104 Script a set of ??
* KT0105 Scripting and automation

**KT0101 Organisation network infrastructure basics and weaknesses**

Organization network infrastructure refers to the underlying framework of hardware, software, and communication protocols that enable the flow of data and information within an organization. It forms the backbone of an organization's IT environment and connects various devices, systems, and users together. Understanding the basics and weaknesses of network infrastructure is crucial for implementing robust cybersecurity measures. Here are some key components and potential weaknesses:

**1. Basics of Network Infrastructure:**

* **Network Devices**: This includes routers, switches, firewalls, and access points that facilitate data transmission and control network traffic.
* **Network Cabling**: The physical medium used to connect network devices and transfer data.
* **Network Protocols**: The set of rules and conventions that govern how data is transmitted and received across the network.
* **Network Segmentation**: Dividing the network into smaller segments to improve security and control traffic flow.
* **Network Topology**: The arrangement of network devices and connections that form the network layout.

**2. Weaknesses in Network Infrastructure:**

* **Vulnerabilities in Network Devices**: Network devices may have known vulnerabilities that could be exploited by attackers. Regular patching and updates are necessary to address these weaknesses.
* **Insufficient Network Segmentation**: Poorly segmented networks can allow attackers to move laterally and gain access to critical systems once they breach a single entry point.
* **Weak Authentication and Access Controls**: Inadequate password policies or weak access controls can allow unauthorized users to gain access to the network.
* **Lack of Encryption**: Unencrypted data transmission makes it easier for attackers to intercept and manipulate sensitive information.
* **Misconfigured Firewalls**: Improper firewall configurations can lead to inadequate protection or accidental exposure of services to the internet.
* **Outdated or Unsupported Software**: Running outdated software increases the risk of exploitation since security patches may not be available.
* **Phishing and Social Engineering**: Human error, such as falling for phishing scams or providing sensitive information, can compromise network security.
* **Denial-of-Service (DoS) Attacks**: An attacker may attempt to overwhelm network resources, causing service disruptions.
* **Weak Physical Security**: Physical access to network infrastructure by unauthorized individuals can lead to various security breaches.

**3. Mitigating Weaknesses:**

* **Regular Patch Management**: Keep all network devices, firmware, and software up to date with the latest security patches and updates.
* **Network Segmentation**: Divide the network into separate segments and limit access based on the principle of least privilege.
* **Strong Authentication**: Implement multi-factor authentication (MFA) for sensitive systems and accounts.
* **Firewall Configuration**: Configure firewalls to allow only necessary traffic and block unauthorized access.
* **Encryption**: Use encryption for data transmission, especially for sensitive information.
* **Security Awareness Training**: Educate employees about cybersecurity best practices, including how to identify and report phishing attempts.
* **Physical Security**: Restrict physical access to network infrastructure and critical assets.

A comprehensive cybersecurity strategy should address the weaknesses in an organization's network infrastructure. Regular risk assessments, vulnerability scanning, and penetration testing can help identify and remediate potential weaknesses before they are exploited by attackers. Additionally, staying informed about the latest security threats and industry best practices is essential for maintaining a secure network infrastructure.

**KT0102 The web and common attacks**

The web has become an integral part of modern life, but its popularity also makes it a prime target for various cyber attacks. Here are some common attacks that target the web:

**1. Cross-Site Scripting (XSS):**

* **Description**: XSS is a vulnerability that allows attackers to inject malicious scripts into web pages viewed by other users. These scripts execute in the victim's browser, enabling the attacker to steal sensitive information, hijack sessions, or deliver malware.
* **Impact**: XSS can lead to the theft of user credentials, financial data, or personal information. It can also compromise the integrity of web pages, leading to defacement or unauthorized content modifications.

**2. SQL Injection (SQLi):**

* **Description**: SQLi is a type of attack where attackers manipulate a web application's input fields to execute malicious SQL commands against the underlying database. This can lead to unauthorized access, data exfiltration, or data manipulation.
* **Impact**: Successful SQL injection attacks can compromise the confidentiality, integrity, and availability of the database, potentially exposing sensitive data or rendering the application unusable.

**3. Cross-Site Request Forgery (CSRF):**

* **Description**: CSRF involves tricking a user's web browser into making unauthorized requests to a website on which the user is authenticated. The attacker exploits the user's trust in the website to perform actions on their behalf.
* **Impact**: CSRF attacks can lead to unauthorized transactions, account manipulation, or data modification on the victim's behalf.

**4. Distributed Denial of Service (DDoS):**

* **Description**: DDoS attacks flood a web server or network with an overwhelming amount of traffic, rendering it inaccessible to legitimate users.
* **Impact**: DDoS attacks disrupt web services, causing downtime and loss of revenue. They can also serve as a distraction from other attacks or malicious activities.

**5. Phishing:**

* **Description**: Phishing involves using deceptive emails or websites to trick users into revealing sensitive information, such as login credentials or financial details.
* **Impact**: Successful phishing attacks can lead to identity theft, financial loss, or unauthorized access to online accounts.

**6. Man-in-the-Middle (MitM) Attacks:**

* **Description**: In a MitM attack, an attacker intercepts and possibly alters communication between two parties without their knowledge. This can be done by eavesdropping on data transmissions or by impersonating one of the parties involved.
* **Impact**: MitM attacks can lead to the theft of sensitive information, such as login credentials or financial data, and compromise the privacy and security of web communications.

**7. Drive-by Downloads:**

* **Description**: Drive-by downloads occur when users visit compromised or malicious websites, and malware is automatically downloaded and executed on their devices without their knowledge or consent.
* **Impact**: Drive-by downloads can infect users' devices with malware, such as ransomware, viruses, or spyware, leading to data loss, financial theft, or system compromise.

Web developers and administrators must take measures to secure their web applications and websites against these common attacks. This includes implementing secure coding practices, input validation, proper authentication and authorization mechanisms, regular security testing, and staying informed about emerging threats and vulnerabilities. Additionally, users should practice safe web browsing habits, be cautious of suspicious links and emails, and keep their software and browsers up to date to minimize the risk of falling victim to web-based attacks.

**KT0103 Using an operating system**

Using an operating system (OS) is a fundamental aspect of interacting with a computer or computing device. The OS is responsible for managing various hardware and software components, providing a user-friendly interface, and enabling users to run applications and perform tasks efficiently. Here's a general overview of using an operating system:

**1. Booting the System:** To start using an operating system, you first need to power on the computer or device. During the boot process, the OS is loaded into the computer's memory, initializing all the necessary components for it to function correctly.

**2. User Login:** If the OS requires user authentication, you will be prompted to log in with your username and password. Some devices may use other authentication methods, such as biometric (fingerprint, facial recognition) or PIN.

**3. Desktop Environment:** After successful login, you will be presented with the desktop environment, which serves as the user interface of the operating system. The desktop typically consists of icons, a taskbar or dock, and a start menu or application launcher.

**4. File Management:** The OS provides a file management system that allows you to create, access, organize, and manage files and folders on your computer. You can create new documents, save files, move, copy, and delete them as needed.

**5. Running Applications:** Using the OS, you can launch and run various applications to perform tasks, such as web browsing, word processing, email, media playback, and more. Applications may come pre-installed with the OS or can be installed separately.

**6. Multitasking:** Modern operating systems support multitasking, which means you can run multiple applications simultaneously. You can switch between applications using shortcuts, the taskbar, or the application switcher.

**7. System Settings and Configuration:** The OS provides a settings or control panel where you can customize various aspects of your computer, such as display settings, network settings, sound preferences, security options, and more.

**8. Updates and Maintenance:** To keep the OS and applications secure and up to date, you should regularly check for updates and install them when available. This helps patch security vulnerabilities and improves system performance.

**9. Shutting Down or Restarting:** When you are done using the computer, you can shut down or restart the system through the OS interface. This ensures a proper and controlled shutdown, saving your work and closing applications safely.

**10. Troubleshooting and Support:** In case of issues or problems, the OS may provide built-in troubleshooting tools or offer access to online support resources to help you resolve the problem.

Remember that the exact steps and procedures may vary depending on the specific operating system you are using. The most commonly used operating systems for personal computers are Microsoft Windows, macOS (for Apple devices), and various Linux distributions. Mobile devices also use operating systems such as Android (by Google) and iOS (by Apple). Each OS has its unique features and interface, but the core principles of using an OS are generally similar.

**KT0104 Script a set of ??**

Python offers a built-in data structure called a "set" that is an unordered collection of unique elements. Here's a simple Python script to create a set of random numbers:

pythonCopy code

import random def generate\_random\_set(num\_elements, min\_value, max\_value): """ Generate a set of random numbers. Parameters: num\_elements (int): Number of elements to generate in the set. min\_value (int): Minimum value of the random numbers. max\_value (int): Maximum value of the random numbers. Returns: set: A set of random numbers. """ random\_set = set() while len(random\_set) < num\_elements: random\_set.add(random.randint(min\_value, max\_value)) return random\_set if \_\_name\_\_ == "\_\_main\_\_": num\_elements = 5 min\_value = 1 max\_value = 20 random\_set = generate\_random\_set(num\_elements, min\_value, max\_value) print("Random Set:", random\_set)

In this script, the function **generate\_random\_set** takes three parameters: **num\_elements**, **min\_value**, and **max\_value**. It generates a set with **num\_elements** random integers within the range from **min\_value** to **max\_value**, inclusive.

When you run the script, it will generate a random set of 5 integers between 1 and 20 and print the set to the console. The output will vary each time you run the script due to the random nature of the numbers generated.

**KT0105 Scripting and automation**

Scripting and automation are powerful tools in the field of computer programming and IT. They involve writing code or scripts to automate repetitive tasks, simplify complex processes, and improve efficiency. Here's an overview of scripting and automation:

**Scripting:**

* Scripting refers to writing code in a scripting language to perform specific tasks or operations. Scripting languages are usually interpreted, which means the code is executed directly without the need for compilation. Popular scripting languages include Python, JavaScript, Ruby, Bash, PowerShell, and more.

**Advantages of Scripting:**

* **Automation**: Scripts can automate repetitive tasks, saving time and effort for users.
* **Simplicity**: Scripting languages often have concise and easy-to-understand syntax, making it quicker to develop solutions.
* **Rapid Prototyping**: Scripts allow for rapid prototyping and testing of ideas before creating more complex applications.
* **Integration**: Scripts can integrate different systems and technologies to work together seamlessly.

**Automation:**

* Automation is the process of using scripts or software tools to perform tasks with minimal human intervention. It aims to reduce manual effort, eliminate human errors, and streamline workflows.

**Examples of Automation:**

* **File Management**: Automating tasks like file backups, file transfers, and renaming files based on specific criteria.
* **System Maintenance**: Automating software updates, system health checks, and routine maintenance tasks.
* **Data Processing**: Automating data extraction, transformation, and loading (ETL) processes.
* **Testing and Deployment**: Automating software testing, continuous integration, and deployment pipelines.

**Scripting vs. Programming:**

* Scripting and programming are closely related, but there are some distinctions. Scripting is typically used for smaller-scale tasks and automation, while programming often involves larger, more complex applications.

**When to Use Scripting and Automation:**

* Use scripting when you need to perform quick, one-off tasks or automate simple processes.
* Use automation for repetitive tasks, large-scale processes, and when you want to reduce manual intervention.

**Common Automation Tools:**

* There are various automation tools available, such as Ansible, Chef, Puppet, Jenkins, and AutoHotkey, that can be used for specific tasks and environments.

**Considerations for Automation:**

* While automation can improve efficiency, it's essential to consider security and potential risks associated with automated processes.
* Regularly review and update automation scripts to ensure they align with changing requirements and environments.

Overall, scripting and automation play a crucial role in modern IT operations, enabling users to optimize workflows, increase productivity, and focus on more strategic tasks. By using scripts and automation tools effectively, organizations can achieve greater efficiency and reliability in their processes.

***Internal Assessment Criteria and Weight***

* IAC0101 End-user access point security is understood.
* IAC0102 Pro-security (access-point, end-points, distribution points) is described.

***(Weight 10%)***

# KM-03-KT02 : Types of cybersecurity software/tools 20%

**Topic elements to be covered include:**

* KT0201 Open source availability
* KT0202 Web security monitoring tools
* KT0203 Encryption Tools
* KT0204 Web vulnerability scanning tools (scanning and evaluation of websites and environment)
* KT0205 Network defence wireless tools
* KT0206 Packet sniffers (evaluating what passes across the connection)
* KT0207 Antivirus software
* KT0208 Firewalls
* KT0209 PKI services (Public Key Infrastructure)
* KT0210 Managed detection services
* KT0211 Ethical hacking and penetration testing (confirm that security measures are fit for purpose)

**KT0201 Open source availability**

Open source availability refers to software that is released with a license that grants users the freedom to view, modify, and distribute the source code openly. In other words, the source code is accessible and can be freely used, studied, modified, and shared by anyone. Open source software is typically developed collaboratively by a community of developers who contribute their expertise to improve and expand the software.

The key characteristics of open source software include:

1. **Access to Source Code**: Open source software provides access to the original source code, allowing users to examine how the software works, make changes, and contribute improvements.
2. **Distribution and Modification**: Users have the freedom to redistribute the software, including modified versions, without any restrictions. This fosters collaboration and community-driven development.
3. **Transparency and Security**: The availability of source code enables transparency, allowing users to verify the software's security and privacy features.
4. **No Vendor Lock-in**: Open source software prevents vendor lock-in because users can access and modify the source code independently of any specific vendor.
5. **Community Collaboration**: Open source projects often have a community of developers who collaborate, review code, and contribute to the software's evolution.

Examples of well-known open source software include:

* **Operating Systems**: Linux (various distributions like Ubuntu, Fedora, and Debian), FreeBSD.
* **Web Browsers**: Mozilla Firefox, Chromium (the open-source base for Google Chrome).
* **Office Suites**: LibreOffice, Apache OpenOffice.
* **Web Servers**: Apache HTTP Server, Nginx.
* **Programming Languages**: Python, Ruby, PHP, Java (OpenJDK).
* **Database Management Systems**: MySQL, PostgreSQL, MongoDB.

Open source software is widely used across various industries and sectors, from web development and data analysis to scientific research and government applications. It offers flexibility, cost-effectiveness, and a strong community-driven development model that encourages innovation and collaboration.

As an important note, while open source software is freely available, it's essential to review the specific license terms of each project to understand its permissions, obligations, and any potential restrictions. Some popular open source licenses include the GNU General Public License (GPL), MIT License, Apache License, and the Mozilla Public License (MPL), among others. Each license has its own terms regarding how the software can be used, modified, and redistributed.

**KT0202 Web security monitoring tools**

Web security monitoring tools are essential for detecting, analyzing, and mitigating potential threats and vulnerabilities in web applications and websites. These tools help organizations proactively safeguard their web assets from various cyber attacks. Here are some popular web security monitoring tools:

**1. Web Application Firewalls (WAF):**

* WAFs protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. They can detect and block malicious requests, such as SQL injection, cross-site scripting (XSS), and other application-layer attacks.

**2. Security Information and Event Management (SIEM) Systems:**

* SIEM systems collect and analyze security event logs from various sources, including web servers and applications. They help identify patterns of malicious activity and provide real-time alerts for potential security incidents.

**3. Web Vulnerability Scanners:**

* Web vulnerability scanners automatically identify security weaknesses in web applications. They simulate attacks to uncover common vulnerabilities like SQL injection, XSS, and insecure configurations.

**4. Web Content Security Policy (CSP) Analyzers:**

* CSP analyzers review and validate the content security policy implemented on a website. CSP helps prevent the execution of malicious scripts and unauthorized content by defining a policy for acceptable sources of content.

**5. Malware Scanners:**

* Malware scanners detect and remove malicious files, code injections, and other malware present on web servers. They ensure the integrity and security of web application files.

**6. Web Traffic Analyzers:**

* Web traffic analyzers monitor incoming and outgoing traffic to identify unusual patterns, potential threats, and security incidents. They help in detecting distributed denial-of-service (DDoS) attacks and unauthorized access attempts.

**7. Network Intrusion Detection/Prevention Systems (NIDS/NIPS):**

* NIDS and NIPS monitor network traffic for signs of suspicious activity or known attack patterns. They can detect and block malicious traffic before it reaches the web server.

**8. Log Analysis Tools:**

* Log analysis tools help review and analyze web server logs and application logs for signs of unauthorized access, error messages, or security events.

**9. Web Application Performance Monitoring:**

* While not directly security-focused, performance monitoring tools help identify anomalies that may indicate a security incident or the presence of malicious activities.

**10. Website Defacement Monitoring:**

* Website defacement monitoring tools track changes to a website's appearance or content, helping to detect unauthorized modifications or cyber attacks.

It's important to note that no single tool can provide complete web security coverage. A comprehensive web security strategy combines multiple tools and practices, including secure coding practices, regular vulnerability assessments, penetration testing, and employee training. Additionally, staying informed about the latest security threats and best practices is vital to maintaining robust web security.

**KT0203 Encryption Tools**

Encryption tools are software applications or libraries designed to secure sensitive data by converting it into unreadable ciphertext using encryption algorithms. These tools play a crucial role in protecting data privacy, ensuring confidentiality, and safeguarding information from unauthorized access or interception. Here are some popular encryption tools used for various purposes:

**1. GPG (GNU Privacy Guard) / PGP (Pretty Good Privacy):**

* GPG and PGP are widely used encryption tools that provide email and file encryption. They use public-key cryptography to secure communications and data.

**2. OpenSSL:**

* OpenSSL is an open-source library that provides SSL/TLS encryption for secure communications over networks like the internet. It is commonly used to secure web servers and other network services.

**3. VeraCrypt:**

* VeraCrypt is an open-source disk encryption tool that allows users to create encrypted virtual disks or containers. It supports various encryption algorithms and can encrypt entire partitions or external storage devices.

**4. BitLocker:**

* BitLocker is a disk encryption feature included in some versions of Microsoft Windows. It encrypts the entire hard drive to protect data on the operating system level.

**5. FileVault:**

* FileVault is a disk encryption tool built into macOS. It encrypts the entire startup disk on Mac computers, providing data protection at rest.

**6. AES Crypt:**

* AES Crypt is a simple file encryption tool that uses the Advanced Encryption Standard (AES) algorithm. It is available for various platforms and is easy to use for encrypting individual files.

**7. AxCrypt:**

* AxCrypt is a user-friendly file encryption tool for Windows, macOS, and mobile platforms. It integrates with the file explorer, making it easy to encrypt and decrypt files.

**8. Symantec Endpoint Encryption:**

* Symantec Endpoint Encryption is an enterprise-level encryption solution that offers full-disk encryption, file/folder encryption, and removable media encryption.

**9. Boxcryptor:**

* Boxcryptor is a cloud-based encryption tool that encrypts files stored in cloud storage services like Google Drive, Dropbox, and OneDrive.

**10. Signal Protocol:**

* Signal Protocol is an open-source encryption protocol used in the Signal messaging app, WhatsApp, and other secure communication platforms. It provides end-to-end encryption for messages and calls.

When selecting an encryption tool, consider factors like the encryption algorithms used, ease of use, compatibility with your operating system or platform, and whether it meets your specific security requirements. Remember that proper key management and strong passwords or passphrases are essential to ensuring the security of encrypted data.

**KT0204 Web vulnerability scanning tools (scanning and evaluation of websites and environment)**

Web vulnerability scanning tools are software applications designed to automatically identify and evaluate potential security vulnerabilities in web applications and websites. These tools help organizations proactively assess their web environment's security posture, identify weaknesses, and prioritize remediation efforts. Here are some popular web vulnerability scanning tools:

**1. OWASP ZAP (Zed Attack Proxy):**

* OWASP ZAP is a widely used open-source web application security scanner. It provides automated scanning, active and passive vulnerability detection, and support for various security testing methodologies.

**2. Acunetix:**

* Acunetix is a powerful web vulnerability scanner that performs comprehensive security assessments, including automated scanning, crawling, and reporting. It supports various technologies and can identify a wide range of vulnerabilities.

**3. Burp Suite:**

* Burp Suite is a popular web vulnerability scanner and penetration testing tool. It offers both free and paid versions and includes features like active scanning, passive scanning, and manual vulnerability testing.

**4. Nessus:**

* Nessus is a versatile vulnerability scanner that can assess web applications along with network infrastructure. It provides vulnerability detection, configuration assessment, and compliance checking.

**5. Nikto:**

* Nikto is an open-source web server scanner that focuses on identifying known vulnerabilities and misconfigurations. It is designed to quickly scan multiple web servers for potential issues.

**6. OpenVAS (Open Vulnerability Assessment System):**

* OpenVAS is an open-source vulnerability scanner that offers a web-based interface for managing and running security scans. It includes a comprehensive database of known vulnerabilities.

**7. Nmap (Network Mapper):**

* Nmap is primarily known as a network scanner, but it can also detect open web ports and identify web server and application vulnerabilities.

**8. Qualys Web Application Scanning (WAS):**

* Qualys WAS is a cloud-based web application scanner that provides automated scanning and vulnerability assessment for web applications.

**9. AppSpider:**

* AppSpider is a dynamic application security testing (DAST) tool that assesses web applications for security vulnerabilities. It includes features like automated scanning, custom vulnerability checks, and reporting.

**10. Netsparker:**

* Netsparker is a web application security scanner that offers a comprehensive vulnerability scanning solution. It includes a variety of scanning techniques to identify potential threats.

Web vulnerability scanning tools are essential for maintaining the security of web applications and websites. However, it's crucial to remember that no scanning tool can replace a thorough security assessment performed by cybersecurity professionals. Regular security assessments, penetration testing, and continuous monitoring are key components of a comprehensive web security strategy.

**KT0205 Network defence wireless tools**

Wireless networks present unique security challenges due to their broadcast nature and potential for unauthorized access. Network defense wireless tools help organizations protect their wireless environments, monitor for suspicious activities, and ensure the security of wireless communications. Here are some common network defense wireless tools:

**1. Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS):**

* WIDS/WIPS tools monitor wireless networks for unauthorized access, rogue access points, and suspicious activities. WIDS identifies potential security threats, while WIPS can take automated actions to block or mitigate detected threats.

**2. Wi-Fi Scanners:**

* Wi-Fi scanners help network administrators discover and identify nearby Wi-Fi networks, detect rogue access points, and identify potential signal interference issues.

**3. Wireless Packet Analyzers:**

* Wireless packet analyzers capture and analyze network traffic in wireless networks. They can identify security vulnerabilities, monitor for suspicious packets, and perform in-depth analysis of wireless communications.

**4. Wireshark:**

* Wireshark is a popular open-source packet analyzer that can be used to capture and analyze wireless network traffic. It supports various wireless protocols and can help detect security issues.

**5. Aircrack-ng:**

* Aircrack-ng is a suite of tools for auditing wireless networks' security. It includes tools for capturing packets, analyzing captured data, and performing wireless network attacks, primarily for educational and security testing purposes.

**6. Kismet:**

* Kismet is an open-source wireless network detection and intrusion detection system. It passively collects wireless packets to identify nearby Wi-Fi networks and detect unauthorized devices.

**7. NetStumbler (Windows) / InSSIDer (Windows, macOS):**

* NetStumbler and InSSIDer are wireless network discovery tools that help identify nearby Wi-Fi networks and their signal strengths. They can also detect rogue access points.

**8. WiFi Pineapple:**

* The WiFi Pineapple is a hardware device used for wireless security testing and auditing. It can simulate rogue access points and conduct wireless attacks.

**9. Wifiphisher:**

* Wifiphisher is a rogue access point framework designed to perform phishing attacks on Wi-Fi clients, leading them to disclose sensitive information.

**10. Hostapd:**

* Hostapd is a user-space daemon for access point and authentication servers. It can be used for setting up a secure and controlled Wi-Fi access point.

It's important to note that while these tools can be valuable for network defense and security testing, using them ethically and responsibly is essential. Unauthorized use of these tools can be illegal and may result in severe consequences. Always ensure you have proper authorization to test and assess the security of wireless networks, and use these tools in compliance with the law and ethical guidelines.

**KT0206 Packet sniffers (evaluating what passes across the connection)**

Packet sniffers, also known as network analyzers or packet analyzers, are tools used to capture and analyze network traffic as it passes across a network connection. These tools are essential for network administrators, security professionals, and researchers to troubleshoot network issues, monitor network performance, and identify security threats. Here's how packet sniffers work and their typical uses:

**How Packet Sniffers Work:**

1. **Packet Capture**: Packet sniffers capture data packets from the network interface of a computer or network device. They can operate in promiscuous mode, allowing them to capture all network traffic, including packets not addressed to the specific device.
2. **Packet Analysis**: The captured packets are then analyzed to extract information such as source and destination IP addresses, port numbers, protocols used, payload data, and any potential anomalies or security issues.
3. **Packet Filtering**: Packet sniffers often include filtering capabilities to focus on specific types of packets or traffic, making it easier to target the information of interest.

**Typical Uses of Packet Sniffers:**

1. **Network Troubleshooting**: Packet sniffers help identify and diagnose network issues, such as packet loss, high latency, or misconfigurations.
2. **Network Performance Monitoring**: Administrators can use packet sniffers to monitor network performance and identify bandwidth bottlenecks or resource-intensive applications.
3. **Security Analysis**: Packet sniffers are valuable tools for security professionals to monitor and detect suspicious or malicious network activities, including potential intrusion attempts or malware communications.
4. **Protocol Analysis**: Researchers and developers use packet sniffers to analyze and debug network protocols, ensuring proper communication and adherence to standards.
5. **Traffic Analysis and Profiling**: Packet sniffers can be used to understand the typical traffic patterns and behaviors on a network, aiding in network optimization and capacity planning.
6. **Intrusion Detection**: Sniffers can be integrated into intrusion detection systems (IDS) to monitor network traffic for signs of malicious activities or known attack patterns.

It's important to note that packet sniffing can raise privacy and security concerns, as it can capture sensitive information, such as passwords or private data transmitted over unencrypted connections. Therefore, the use of packet sniffers should be carried out responsibly and in compliance with applicable laws and regulations. In secure environments, encryption and other security measures should be used to protect sensitive data from interception and unauthorized access. Additionally, only authorized personnel should use packet sniffers for legitimate purposes, such as network administration and security monitoring.

**KT0207 Antivirus software**

Antivirus software, also known as anti-malware software, is a type of cybersecurity tool designed to detect, prevent, and remove malicious software (malware) from computer systems and networks. It plays a critical role in protecting devices from various types of threats, including viruses, worms, Trojans, ransomware, spyware, and other forms of malware. Here's how antivirus software works and its key features:

**How Antivirus Software Works:**

1. **Signature-based Detection:** Antivirus software uses a signature-based approach to detect known malware. It maintains a database of known malware signatures, and when a file or program is scanned, the antivirus compares its signature to the ones in the database. If a match is found, the antivirus flags the file as malicious.
2. **Heuristic Analysis:** Antivirus software employs heuristic analysis to detect new or previously unseen malware. It looks for behavioral patterns and characteristics common to malware and flags suspicious files or activities.
3. **Behavioral Analysis:** Some advanced antivirus solutions use behavioral analysis to identify malware based on its behavior. If a file exhibits suspicious or malicious behavior, even if it does not match any known signatures, the antivirus may take action.
4. **Real-time Scanning:** Antivirus software can provide real-time scanning, where it actively monitors files and programs as they are accessed or executed. This helps prevent malware from infecting the system in real-time.
5. **On-demand Scanning:** Users can manually initiate on-demand scans to check specific files, folders, or the entire system for malware.
6. **Automatic Updates:** Antivirus software regularly updates its signature database and program components to stay up-to-date with the latest threats.
7. **Quarantine and Remediation:** When malware is detected, the antivirus software may quarantine the infected files, isolating them from the rest of the system. Users can then decide whether to remove or remediate the threats.

**Key Features of Antivirus Software:**

1. **Malware Detection and Removal:** Antivirus software's primary function is to detect and remove malware from infected systems.
2. **Real-time Protection:** Antivirus software offers real-time protection to prevent malware from executing or infecting the system.
3. **Scanning Options:** Antivirus software provides various scanning options, including quick scans, full system scans, and custom scans.
4. **Scheduled Scans:** Users can schedule automatic scans at specific intervals to ensure regular system checks.
5. **Firewall Integration:** Some antivirus products include a firewall to monitor and control network traffic for additional security.
6. **Browser Protection:** Antivirus software may include browser extensions or tools to block malicious websites and prevent phishing attempts.
7. **Email Protection:** Some antivirus solutions offer email scanning to detect and block malicious email attachments.

It's important to keep antivirus software up to date to ensure it can detect the latest threats effectively. Additionally, users should practice safe browsing habits, exercise caution when downloading files or clicking on links, and keep all software and operating systems patched to further enhance cybersecurity.

**KT0208 Firewalls**

Firewalls are essential network security devices or software applications that act as a barrier between a trusted internal network and untrusted external networks, such as the internet. They monitor and control incoming and outgoing network traffic based on predefined security rules, helping to prevent unauthorized access, data breaches, and malicious activities. Firewalls play a crucial role in protecting networks and devices from various cyber threats. Here's how firewalls work and their key features:

**How Firewalls Work:**

1. **Packet Filtering:** Firewalls inspect data packets as they pass through the network. They analyze packet headers, such as source and destination IP addresses, port numbers, and protocol types, to determine whether to allow or block the packets based on predefined rules.
2. **Stateful Inspection:** Stateful firewalls keep track of the state of network connections. They allow inbound traffic that corresponds to an established outbound connection and block other unsolicited traffic.
3. **Proxying:** Some firewalls act as intermediaries between the internal network and external networks. They receive requests from internal users and forward them on their behalf, helping to hide internal network details.
4. **Application Layer Filtering:** Advanced firewalls can inspect data at the application layer (Layer 7 of the OSI model), enabling granular control over specific applications and protocols.
5. **Logging and Monitoring:** Firewalls log information about network traffic and events, allowing administrators to review and analyze network activity for potential security incidents.

**Types of Firewalls:**

1. **Network Firewalls:** These are hardware or software firewalls that protect entire networks or network segments. They are often placed between an organization's internal network and the internet.
2. **Host-based Firewalls:** These firewalls are installed on individual devices, such as computers and servers, and protect the specific device from unauthorized network traffic.
3. **Next-Generation Firewalls (NGFW):** NGFWs combine traditional firewall capabilities with advanced features, such as intrusion prevention, deep packet inspection, application awareness, and identity-based access control.
4. **Proxy Firewalls:** Proxy firewalls act as intermediaries between internal and external networks, handling requests and responses on behalf of internal users.

**Key Features of Firewalls:**

1. **Access Control:** Firewalls use access control rules to allow or block network traffic based on specified criteria.
2. **Network Address Translation (NAT):** Firewalls can perform NAT, allowing internal devices to share a single public IP address for internet access.
3. **Virtual Private Network (VPN) Support:** Some firewalls provide VPN functionality to secure remote access to the internal network.
4. **Intrusion Prevention System (IPS):** Advanced firewalls may include IPS capabilities to detect and prevent network-based attacks.
5. **Content Filtering:** Some firewalls offer content filtering to block access to specific websites or content categories.
6. **Logging and Reporting:** Firewalls log events and provide reports to help administrators monitor network activity and identify security incidents.

Firewalls are a fundamental component of network security and serve as the first line of defense against cyber threats. They help organizations enforce security policies, protect sensitive data, and ensure a secure and reliable network environment.

**KT0209 PKI services (Public Key Infrastructure)**

Public Key Infrastructure (PKI) services are a set of technologies, policies, and procedures that enable the secure management and distribution of digital certificates and cryptographic keys. PKI is used to establish trust in electronic communications and transactions, ensuring the confidentiality, integrity, and authenticity of sensitive information exchanged over networks. PKI services are a fundamental component of modern cybersecurity and play a crucial role in various applications, including secure communication, digital signatures, encryption, and authentication.

Key components and services in a PKI include:

**1. Certificate Authority (CA):**

* The Certificate Authority is a trusted entity responsible for issuing digital certificates to individuals, organizations, or devices. These certificates contain the public key and other identifying information of the certificate holder.

**2. Digital Certificates:**

* Digital certificates are electronic documents issued by the Certificate Authority that bind the public key to the identity of the certificate holder. They also contain information about the certificate's validity period and the CA's digital signature.

**3. Public and Private Key Pair:**

* PKI uses asymmetric encryption, where each entity has a unique pair of keys: a public key and a private key. The public key is included in the digital certificate and can be freely shared, while the private key must be kept secure and only known to the certificate holder.

**4. Certificate Revocation:**

* In case a certificate holder's private key is compromised or the certificate's validity is no longer trustworthy, the CA can revoke the certificate. Certificate revocation ensures that compromised or expired certificates cannot be used for fraudulent activities.

**5. Certificate Validation and Trust Chains:**

* Before trusting a digital certificate, applications and users need to validate the certificate's authenticity. This involves verifying the certificate's digital signature and checking whether the certificate is issued by a trusted CA.

**6. Registration Authorities (RAs):**

* RAs assist CAs in verifying the identity of individuals or organizations applying for digital certificates. They help maintain the accuracy and trustworthiness of the PKI.

**7. Certificate Repository:**

* The Certificate Repository stores and publishes digital certificates for users and systems to access and verify.

**8. Key Management:**

* PKI services include key management to handle the generation, distribution, storage, and revocation of cryptographic keys.

**9. Time Stamping:**

* PKI may also provide time-stamping services, where digital signatures are timestamped to establish the signing time and prevent repudiation.

PKI services are widely used in securing various aspects of modern technology, such as secure web browsing (HTTPS), email encryption and signing (S/MIME), secure authentication (SSL/TLS), digital signatures, and more. They provide a robust framework for establishing trust and ensuring security in digital communications and transactions.

**KT0210 Managed detection services**

Managed Detection and Response (MDR) services are cybersecurity offerings provided by specialized service providers to help organizations proactively detect and respond to cyber threats and security incidents. MDR services combine advanced threat detection technologies, experienced security analysts, and 24/7 monitoring to provide comprehensive and continuous threat detection and incident response capabilities.

Key features and components of Managed Detection and Response services include:

**1. Threat Detection Technologies:**

* MDR providers deploy advanced security tools and technologies to monitor network traffic, endpoints, and cloud environments. These may include Intrusion Detection Systems (IDS), Endpoint Detection and Response (EDR) tools, Security Information and Event Management (SIEM) systems, and behavioral analytics.

**2. 24/7 Monitoring and Alerting:**

* MDR services offer continuous monitoring of an organization's IT infrastructure. Security analysts are available around the clock to analyze security alerts and respond to potential threats in real-time.

**3. Threat Hunting and Analysis:**

* MDR teams proactively hunt for potential threats and suspicious activities within an organization's environment. They perform in-depth analysis to identify indicators of compromise and emerging threats.

**4. Incident Response and Mitigation:**

* In the event of a security incident, MDR providers assist with incident response and containment. They work closely with the organization's IT team to mitigate the impact of the incident and restore normal operations.

**5. Expert Security Analysts:**

* MDR services are staffed with skilled cybersecurity analysts who possess expertise in threat detection, incident response, and malware analysis. These analysts interpret security alerts, investigate potential threats, and provide actionable recommendations.

**6. Threat Intelligence Integration:**

* MDR services leverage threat intelligence from various sources to stay informed about the latest cyber threats and attack trends. This helps enhance their detection capabilities and proactive threat hunting efforts.

**7. Reporting and Analysis:**

* MDR providers deliver regular reports and insights to their clients, detailing detected threats, security incidents, and overall security posture. These reports help organizations understand their risk exposure and make informed decisions about security improvements.

**8. Incident Coordination and Collaboration:**

* MDR teams collaborate with the organization's internal IT and security teams, providing support during incident investigations and ensuring effective coordination.

Managed Detection and Response services offer an important layer of defense for organizations of all sizes, particularly those lacking in-house cybersecurity expertise or facing resource constraints. By outsourcing threat detection and incident response to MDR experts, organizations can strengthen their security posture, detect and respond to threats more effectively, and focus on their core business operations.

**KT0211 Ethical hacking and penetration testing (confirm that security measures are fit for purpose)**

Ethical hacking and penetration testing are cybersecurity practices aimed at identifying security vulnerabilities in computer systems, networks, and applications. Both practices involve simulating real-world cyber attacks to assess the effectiveness of security measures and ensure that they are "fit for purpose" in protecting against potential threats. Let's understand each concept:

**1. Ethical Hacking:**

* Ethical hacking, also known as penetration testing or white-hat hacking, involves authorized professionals (ethical hackers) attempting to exploit vulnerabilities in a system or network to identify potential weaknesses. Ethical hackers use the same techniques and tools as malicious hackers but do so with the explicit permission and for the purpose of improving security. They perform a controlled and systematic assessment of the target, attempting to gain unauthorized access, extract sensitive data, or execute other attack scenarios.

**2. Penetration Testing:**

* Penetration testing is a subset of ethical hacking and focuses specifically on assessing the security of a target system, network, or application. The objective is to identify and exploit security weaknesses before malicious actors can do so. Penetration testers use various methodologies to assess the target, combining manual techniques and automated tools to simulate real-world attacks. The goal is to provide organizations with a clear understanding of their security posture and recommend necessary improvements.

**Importance and Purpose:** Ethical hacking and penetration testing are essential for several reasons:

1. **Identifying Vulnerabilities:** By simulating real attacks, ethical hackers and penetration testers can identify and document potential vulnerabilities that may be overlooked in routine security assessments.
2. **Evaluating Security Measures:** The process helps organizations assess the effectiveness of their existing security measures and policies. It identifies areas that need improvement to ensure the organization's security posture is adequate.
3. **Risk Management:** The results of ethical hacking and penetration testing help organizations prioritize security investments and allocate resources more effectively to address critical security risks.
4. **Regulatory Compliance:** Many industries and regulatory standards require organizations to conduct regular security assessments, making ethical hacking and penetration testing crucial for compliance.
5. **Preventing Data Breaches:** By identifying and fixing vulnerabilities proactively, organizations can reduce the risk of data breaches and potential financial losses.
6. **Enhancing Incident Response:** Ethical hacking and penetration testing reveal weaknesses in incident response capabilities, helping organizations improve their ability to detect and respond to security incidents effectively.
7. **Building Trust:** Regularly conducting ethical hacking and penetration testing demonstrates an organization's commitment to security and builds trust among stakeholders and customers.

Ethical hacking and penetration testing should be performed by skilled professionals or reputable cybersecurity firms to ensure the assessments are conducted responsibly, safely, and within the bounds of legal and ethical guidelines. The results and recommendations obtained from these assessments enable organizations to strengthen their security measures and better protect against potential cyber threats.

***Internal Assessment Criteria and Weight***

* IAC0201 Various cybersecurity software/tools are described in terms of what they are used for.
* IAC0202 Various cybersecurity software/tools are compared in terms of how effective they are with regard to cyber resilience.

***(Weight 20%)***

# KM-03-KT03 : Encryption 15%

**Topic elements to be covered include:**

* KT0301 Legislative
* KT0302 Symmetric vs asymmetric cryptography
* KT0303 Basic concepts of cryptography
* KT0304 Explain cryptography algorithms and their basic characteristics
* KT0305 Install and configure wireless security settings
* KT0306 Implement public key infrastructure

**KT0301 Legislative**

Encryption legislation refers to laws or regulations enacted by governments or legislative bodies that aim to govern the use of encryption technologies and the exchange of encrypted data within a country or jurisdiction. Encryption is a critical technology used to protect sensitive information, secure communications, and maintain privacy. However, its widespread adoption has also raised concerns among some governments and law enforcement agencies that it can be misused by criminals or terrorists to hide their activities.

There have been debates and discussions around the world about striking the right balance between privacy and security when it comes to encryption. Some governments have proposed or implemented legislation to address their concerns regarding encryption. The key aspects and goals of encryption legislation may include:

**1. Access to Encrypted Data by Law Enforcement:**

* Some governments seek to require technology companies and service providers to provide law enforcement agencies with access to encrypted data under certain circumstances. This is often referred to as "backdoor access" or "lawful access."

**2. Encryption Standards and Regulations:**

* Governments may introduce regulations or set standards for encryption technologies used within their jurisdiction. This can include requirements for the strength of encryption algorithms or key management practices.

**3. Export Controls:**

* Some countries have export controls on encryption products and technologies, limiting their distribution to certain countries or entities to prevent their misuse.

**4. Data Retention Policies:**

* Legislation related to data retention may require service providers to retain encryption keys or decrypted data for a specific period to assist law enforcement investigations.

**5. Decryption Orders and Warrants:**

* Governments may seek legal mechanisms to obtain decryption orders or warrants, compelling individuals or organizations to provide access to encrypted data during investigations.

**6. Collaboration with Tech Companies:**

* Governments may work with technology companies to develop solutions that enable access to encrypted data while preserving user privacy and security.

**Challenges and Concerns:** The debate surrounding encryption legislation raises several challenges and concerns:

1. **Privacy and Civil Liberties:** Encryption legislation that grants backdoor access to law enforcement raises concerns about potential violations of privacy and civil liberties.
2. **Security Risks:** Introducing backdoors or weakening encryption could expose encrypted data to unauthorized access, including cybercriminals and state-sponsored hackers.
3. **Global Implications:** Encryption is a global technology, and laws in one country may have implications beyond its borders, affecting individuals and organizations worldwide.
4. **Impact on Innovation:** Encryption is a fundamental aspect of digital security and innovation. Restricting encryption could stifle technological advancements and hinder secure communications and transactions.
5. **Balance of Interests:** Governments must strike a balance between public safety and national security concerns on one hand and protecting individual privacy and digital rights on the other.

Different countries have taken diverse approaches to encryption legislation based on their legal systems, national security priorities, and public sentiment. The debate continues as policymakers and stakeholders seek to find an appropriate balance between protecting privacy and ensuring public safety in the digital age.

**KT0302 Symmetric vs asymmetric cryptography**

Symmetric and asymmetric cryptography are two fundamental encryption techniques used to secure data and communications in the field of cybersecurity. Each approach has its strengths and weaknesses, and they are often used in combination to achieve different security goals. Let's explore the differences between symmetric and asymmetric cryptography:

**1. Symmetric Cryptography:**

* Symmetric cryptography, also known as secret-key cryptography, uses the same secret key for both encryption and decryption of data. The sender and receiver must both possess and keep the key secret to secure their communications. It is a fast and efficient method, making it suitable for encrypting large volumes of data.

**Key Features:**

* Single Key: The same secret key is used for both encryption and decryption.
* Speed: Symmetric encryption is faster and computationally less intensive than asymmetric encryption.
* Efficiency: It is more efficient for encrypting and decrypting large amounts of data.
* Key Distribution: The challenge is securely distributing the secret key to all parties that need to communicate.

**Use Cases:**

* Secure Data Storage: Symmetric encryption is often used to encrypt data at rest, such as files or databases.
* Secure Communication: Symmetric encryption is suitable for secure communications between parties that have already exchanged the secret key.

**2. Asymmetric Cryptography:**

* Asymmetric cryptography, also known as public-key cryptography, employs a pair of keys: a public key and a private key. The public key is freely distributed, while the private key is kept secret. Data encrypted with the public key can only be decrypted with the corresponding private key and vice versa.

**Key Features:**

* Key Pair: Asymmetric cryptography uses a pair of keys: public key and private key.
* Secure Communication: The public key can be freely shared, enabling secure communication without the need for a pre-shared secret key.
* Digital Signatures: Asymmetric cryptography allows the creation of digital signatures to verify the authenticity of a message or document.
* Key Distribution: The public key can be openly distributed, while the private key must be kept confidential.

**Use Cases:**

* Secure Key Exchange: Asymmetric cryptography is used to securely exchange secret keys for symmetric encryption.
* Digital Signatures: Asymmetric cryptography is used to create and verify digital signatures for message authentication and integrity.
* Secure Communication: Asymmetric encryption allows secure communication without the need for a shared secret key.

**Hybrid Cryptography:**

* In practice, many secure communication systems use a combination of both symmetric and asymmetric cryptography. This approach is called hybrid cryptography. It leverages the speed and efficiency of symmetric encryption for data encryption, while asymmetric encryption is used to securely exchange the symmetric encryption keys.

**Summary:**

* Symmetric cryptography uses a single secret key for encryption and decryption and is fast and efficient but requires secure key distribution.
* Asymmetric cryptography uses a pair of keys for encryption and decryption, allows secure key exchange, and enables digital signatures for authentication.

**KT0303 Basic concepts of cryptography**

Cryptography is the science and practice of securing communication and data by converting plain, readable information (plaintext) into an unintelligible form (ciphertext) using mathematical algorithms and keys. The basic concepts of cryptography revolve around various components, techniques, and goals that ensure data confidentiality, integrity, authentication, and non-repudiation. Here are the fundamental concepts of cryptography:

**1. Encryption and Decryption:**

* Encryption is the process of converting plaintext into ciphertext using a cryptographic algorithm and a secret encryption key. Decryption is the reverse process of converting ciphertext back into plaintext using the same algorithm and a secret decryption key.

**2. Cryptographic Algorithms:**

* Cryptographic algorithms are mathematical procedures used for encryption, decryption, and other cryptographic operations. They can be symmetric (use the same key for encryption and decryption) or asymmetric (use a pair of keys: public key for encryption and private key for decryption).

**3. Symmetric Encryption:**

* Symmetric encryption employs a single secret key for both encryption and decryption. The sender and receiver must share this secret key in a secure manner before communication.

**4. Asymmetric Encryption:**

* Asymmetric encryption uses a pair of keys: a public key for encryption and a private key for decryption. The public key can be freely distributed, while the private key must be kept secret.

**5. Key Management:**

* Key management involves generating, distributing, storing, and protecting cryptographic keys. Secure key management is crucial to maintaining the security of encrypted data.

**6. Key Exchange:**

* Key exchange mechanisms allow parties to securely establish shared secret keys for symmetric encryption over insecure communication channels.

**7. Hash Functions:**

* Hash functions are one-way mathematical functions that convert input data into a fixed-length output called a hash value or digest. They are used for data integrity verification and creating digital signatures.

**8. Digital Signatures:**

* Digital signatures use asymmetric cryptography to verify the authenticity and integrity of digital documents or messages. The signer uses their private key to create the signature, and others can verify it using the signer's public key.

**9. Secure Hash Algorithm (SHA):**

* SHA is a family of cryptographic hash functions commonly used for integrity verification and digital signatures.

**10. Message Authentication Code (MAC):**

* MAC is a short piece of information generated using a secret key to authenticate a message's integrity and authenticity.

**11. Non-Repudiation:**

* Non-repudiation ensures that the sender of a message cannot later deny sending the message, and the receiver cannot deny receiving it. Digital signatures provide non-repudiation.

**12. Cryptanalysis:**

* Cryptanalysis is the study of analyzing and breaking cryptographic algorithms to uncover weaknesses or vulnerabilities.

Cryptography is a critical aspect of modern cybersecurity, and its proper implementation ensures the confidentiality, integrity, and authenticity of sensitive information in various applications, including secure communication, data storage, digital signatures, and more.

**KT0304 Explain cryptography algorithms and their basic characteristics**

Cryptography algorithms are mathematical procedures used in encryption, decryption, and other cryptographic operations to protect data and communication. These algorithms play a crucial role in ensuring data confidentiality, integrity, and authenticity. Cryptographic algorithms can be classified into two main categories: symmetric and asymmetric (also known as public-key) algorithms. Let's explore their basic characteristics:

**1. Symmetric Cryptography Algorithms:**

* In symmetric encryption, the same secret key is used for both encryption and decryption of data. The sender and receiver must share this secret key before communication. Symmetric algorithms are faster and more efficient for encrypting large volumes of data.

**Characteristics:**

* **Single Key:** Symmetric algorithms use a single secret key for both encryption and decryption.
* **Speed:** Symmetric encryption is fast and computationally less intensive, making it suitable for encrypting and decrypting large amounts of data.
* **Efficiency:** Since only one key is used, symmetric algorithms are more efficient for bulk data encryption.
* **Key Management:** Secure key distribution and management are essential since the same key must be shared between the communicating parties.
* **Examples:** Common symmetric encryption algorithms include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Triple DES (3DES).

**2. Asymmetric (Public-Key) Cryptography Algorithms:**

* In asymmetric encryption, a pair of keys is used: a public key for encryption and a private key for decryption. The public key can be freely distributed, while the private key must be kept secret. Asymmetric algorithms provide secure key exchange and digital signature capabilities.

**Characteristics:**

* **Key Pair:** Asymmetric algorithms use a pair of keys: a public key and a private key.
* **Secure Communication:** The public key can be freely shared, enabling secure communication without the need for a pre-shared secret key.
* **Digital Signatures:** Asymmetric cryptography allows the creation and verification of digital signatures, ensuring data integrity and authenticity.
* **Key Distribution:** Since the public key can be openly distributed, there is no need for a secure key exchange mechanism.
* **Examples:** Common asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography).

**3. Hybrid Cryptography:**

* In practice, many secure communication systems use a combination of both symmetric and asymmetric cryptography. This approach is called hybrid cryptography. It leverages the speed and efficiency of symmetric encryption for data encryption, while asymmetric encryption is used to securely exchange the symmetric encryption keys.

**4. Hash Functions:**

* Hash functions are one-way mathematical functions that convert input data into fixed-length output called a hash value or digest. Hash functions are used for data integrity verification, digital signatures, and creating message authentication codes (MAC).

**5. Security and Cryptanalysis:**

* The strength of a cryptographic algorithm lies in its resistance to cryptanalysis, the study of analyzing and breaking cryptographic algorithms. Cryptographers design algorithms to withstand various attack techniques, including brute-force attacks, differential cryptanalysis, and more.

Properly implemented cryptographic algorithms are crucial for ensuring the security of sensitive data and communication in various applications, including secure messaging, digital signatures, secure key exchange, and data storage. As computing power increases, cryptographic algorithms must be periodically reviewed and updated to maintain their effectiveness against evolving threats.

**KT0305 Install and configure wireless security settings**

Always refer to the router's user manual or manufacturer's website for specific instructions.

Here's a general outline to set up wireless security settings:

1. **Access Router Settings:**
   * Connect your computer to the router using an Ethernet cable or via Wi-Fi. Open a web browser and enter the router's IP address (usually something like 192.168.0.1 or 192.168.1.1) in the address bar. You may need to enter the router's admin username and password to access the settings page.
2. **Change Default Login Credentials:**
   * Once logged in, change the default login credentials for the router to prevent unauthorized access. Use a strong and unique password.
3. **Enable Encryption (WPA2/WPA3):**
   * Under the wireless settings section, look for the security options. Choose WPA2 (Wi-Fi Protected Access 2) or WPA3, which are the latest and most secure encryption protocols. Avoid using WEP (Wired Equivalent Privacy) as it is outdated and easily cracked.
4. **Set the Network Name (SSID):**
   * Change the default network name (SSID) to something unique and not easily identifiable with your household. This helps prevent unauthorized users from identifying your network.
5. **Enable Network Encryption:**
   * Enable WPA2/WPA3 encryption and choose a strong passphrase (password) for your Wi-Fi network. Use a mix of uppercase and lowercase letters, numbers, and special characters. Longer passphrases are generally more secure.
6. **Disable WPS (Wi-Fi Protected Setup):**
   * WPS is a feature that allows easy connection of devices to the Wi-Fi network using a PIN. However, it has known vulnerabilities. Disable WPS to enhance security.
7. **Enable MAC Address Filtering (Optional):**
   * If your router supports MAC address filtering, you can enable it to restrict Wi-Fi access to specific devices based on their MAC addresses. However, keep in mind that MAC addresses can be spoofed.
8. **Regularly Update Firmware:**
   * Check for firmware updates for your router regularly and apply them as they often include security patches and improvements.
9. **Keep Router in a Secure Location:**
   * Physically place your router in a secure and central location to minimize signal leakage outside your home or office.

Remember, securing your wireless network is essential to prevent unauthorized access and protect your data and devices. Always follow best practices and use the latest encryption standards to ensure your wireless network is well protected.

**KT0306 Implement public key infrastructure**

Implementing a Public Key Infrastructure (PKI) involves setting up the necessary components and processes to manage digital certificates and cryptographic keys securely. PKI is used to establish trust in electronic communications and transactions by providing authentication, confidentiality, integrity, and non-repudiation. Below are the key steps to implement a PKI:

1. **Planning and Design:**
   * Define the scope and requirements of the PKI. Identify the purpose of the PKI, the types of certificates needed (e.g., SSL/TLS certificates for web servers, digital certificates for email encryption), and the intended user base.
2. **Certificate Authority (CA) Setup:**
   * Choose whether to set up an internal private CA or use a commercial CA. An internal CA gives you more control but requires additional infrastructure and maintenance.
3. **Root CA and Subordinate CA Setup:**
   * Establish a Root CA as the top-level certificate authority and create one or more Subordinate CAs to issue certificates to end entities (users, devices, servers).
4. **Hardware Security Modules (HSMs) (Optional):**
   * Consider using HSMs for secure key storage and cryptographic operations to protect the private keys of the Root CA and Subordinate CAs.
5. **Certificate Policy and Practice Statement (CP/CPS):**
   * Develop CP and CPS documents that outline the rules, processes, and procedures for issuing, managing, and revoking certificates.
6. **Certificate Lifecycle Management:**
   * Establish procedures for certificate enrollment, validation, issuance, renewal, and revocation. Implement mechanisms for certificate revocation lists (CRLs) and online certificate status protocol (OCSP) for certificate validation.
7. **Secure Key Management:**
   * Implement strong key management practices, including key generation, distribution, and archival. Protect private keys from unauthorized access.
8. **End-Entity Certificate Enrollment:**
   * Set up a secure enrollment process for end entities (users, servers) to request and obtain certificates from the CA.
9. **Certificate Repository:**
   * Establish a secure repository to store issued certificates and make them accessible for validation.
10. **Public and Private Key Infrastructure:**

* Use the private key infrastructure for certificate issuance and management. Public keys are widely distributed for validation purposes.

1. **Security Monitoring and Auditing:**

* Implement security monitoring to detect and respond to potential security incidents. Regularly audit the PKI for compliance and effectiveness.

1. **Backup and Disaster Recovery:**

* Establish a backup and disaster recovery plan to ensure continuity of the PKI in case of hardware failures or data loss.

1. **Education and Training:**

* Train administrators, operators, and end-users on PKI usage, best practices, and security guidelines.

PKI implementations require careful planning, proper management, and ongoing maintenance. It's crucial to ensure the security, availability, and reliability of the PKI to maintain trust in digital certificates and cryptographic operations.

***Internal Assessment Criteria and Weight***

* IAC0301 The purpose of encryption is understood.

***(Weight 15%)***

# KM-03-KT04 : Personal security 20%

**Topic elements to be covered include:**

* KT0401 Antivirus and anti-malware software
* KT0402 The correct use of antivirus and anti-malware software and explain SSL
* KT0403 Security certificates
* KT0404 Cookies
* KT0405 VPN (creates a secure tunnel between a user's computer and the Virtual private network server)
* KT0406 Personal information and identity theft
* KT0407 Targeted advertising and ad blocking
* KT0408 Cloud computing

**KT0401 Antivirus and anti-malware software**

Antivirus and anti-malware software are essential tools in the field of cybersecurity used to protect computers and devices from various types of malicious software, commonly known as malware. While the terms "antivirus" and "anti-malware" are often used interchangeably, they have slightly different focuses. Let's understand each of them:

**1. Antivirus Software:**

* Antivirus software is designed primarily to detect, prevent, and remove traditional forms of computer viruses. Computer viruses are malicious programs that infect other files or software and replicate themselves, spreading from one system to another.

**Key Features:**

* **Virus Detection:** Antivirus software scans files and programs on a computer for known virus signatures and behaviors.
* **Real-Time Protection:** Antivirus programs provide real-time protection, monitoring files and incoming data to prevent virus infection.
* **Virus Removal:** When a virus is detected, the antivirus software will attempt to quarantine or remove the infected files.

**Use Cases:**

* Antivirus software is particularly effective against known viruses and can provide proactive protection against known threats.

**2. Anti-Malware Software:**

* Anti-malware software, on the other hand, is a broader term that encompasses a wider range of malicious software beyond viruses. It is designed to detect, prevent, and remove various types of malware, including viruses, worms, Trojans, spyware, adware, ransomware, and more.

**Key Features:**

* **Malware Detection:** Anti-malware software employs various techniques to identify and neutralize different types of malware.
* **Behavioral Analysis:** It uses behavioral analysis to identify suspicious activities and behaviors associated with malware.
* **Real-Time Protection:** Like antivirus software, anti-malware software provides real-time protection to block and prevent malware infections.

**Use Cases:**

* Anti-malware software offers more comprehensive protection against a wider range of threats beyond traditional viruses. It is effective against various forms of malware that may have different propagation and attack mechanisms.

**Hybrid Solutions:**

* Many modern security solutions combine antivirus and anti-malware technologies, offering a comprehensive defense against a broad range of threats. These hybrid solutions may also include other security features like firewall protection, intrusion detection/prevention, and phishing protection.

**Considerations:**

* When choosing security software, consider factors like the software's effectiveness in detecting and removing threats, its impact on system performance, regular updates, and support from the vendor.

**Important Note:**

* Regardless of the type of security software you use, it is essential to keep it up-to-date with the latest virus definitions and security patches to ensure it can effectively protect against new and emerging threats. Additionally, practicing safe browsing habits and being cautious about downloading files or clicking on suspicious links can also help prevent malware infections.

**KT0402 The correct use of antivirus and anti-malware software and explain SSL**

**The Correct Use of Antivirus and Anti-Malware Software:**

To ensure the effective use of antivirus and anti-malware software, follow these best practices:

1. **Choose Reputable Software:** Select well-known and reputable antivirus and anti-malware software from trusted vendors. Look for programs that offer regular updates and support.
2. **Install and Update Regularly:** Install the software on all devices, including computers, smartphones, and tablets. Keep the software up-to-date with the latest virus definitions and security patches to protect against new threats.
3. **Enable Real-Time Protection:** Turn on real-time protection to ensure the software actively monitors for and blocks malware in real-time.
4. **Perform Regular Scans:** Schedule regular full-system scans to detect and remove any malware that might have slipped past real-time protection.
5. **Avoid Duplicate Software:** Do not run multiple antivirus or anti-malware programs simultaneously, as they can interfere with each other and cause performance issues.
6. **Use Additional Security Layers:** Consider using a comprehensive security suite that includes features like firewall protection, intrusion detection/prevention, and phishing protection for added layers of security.
7. **Exercise Caution Online:** Practice safe browsing habits, avoid clicking on suspicious links or downloading files from untrusted sources, and be cautious with email attachments.

**SSL (Secure Sockets Layer):**

SSL, or Secure Sockets Layer, is a cryptographic protocol used to establish secure and encrypted connections between a client (typically a web browser) and a server (a website or online service). SSL is now considered outdated, and its successor is Transport Layer Security (TLS). However, the term "SSL" is still commonly used to refer to the updated versions of the protocol.

**Key Characteristics of SSL/TLS:**

1. **Encryption:** SSL/TLS uses encryption algorithms to protect data transmitted between the client and server, ensuring it remains confidential and cannot be easily intercepted by unauthorized parties.
2. **Authentication:** SSL/TLS provides a mechanism for mutual authentication, allowing the client to verify the server's identity and vice versa. This prevents man-in-the-middle attacks and ensures that users are connecting to legitimate websites.
3. **Data Integrity:** SSL/TLS ensures that the data remains unchanged during transmission. Any tampering or alteration of the data during transit will be detected, and the connection will be terminated.
4. **Certificate-Based Security:** SSL/TLS relies on digital certificates issued by trusted Certificate Authorities (CAs) to verify the authenticity of servers and websites. When a client connects to a server, the server presents its digital certificate, which the client verifies to ensure it is connecting to the correct entity.
5. **HTTPS:** SSL/TLS is primarily used to secure web traffic, and its implementation on web servers is known as HTTPS (HyperText Transfer Protocol Secure). Websites using HTTPS display a padlock icon in the browser's address bar, indicating a secure connection.
6. **TLS Versions:** Over time, different versions of TLS have been developed to address security vulnerabilities and enhance encryption. It's crucial to use the latest TLS version (TLS 1.3 at the time of writing) to ensure the strongest security.

SSL/TLS is an essential technology for securing sensitive information transmitted over the internet, such as passwords, financial data, and personal information. By encrypting data and providing authentication, SSL/TLS helps protect users and maintain the privacy and integrity of online communications.

**KT0403 Security certificates**

Security certificates, also known as digital certificates or SSL/TLS certificates, are a critical component of the Public Key Infrastructure (PKI) used to secure communication over the internet. These certificates are issued by Certificate Authorities (CAs) and play a vital role in establishing trust, ensuring confidentiality, integrity, and authenticity of digital communications. Let's explore the key aspects of security certificates:

**1. Purpose:**

* Security certificates are used to encrypt data, verify the identity of websites, and establish secure connections (HTTPS) between clients (e.g., web browsers) and servers (e.g., websites).

**2. Components:**

* A security certificate typically consists of the following components:
  + **Public Key:** The public key is used for encryption and is included in the certificate.
  + **Private Key:** The private key is kept securely by the server and used for decryption.
  + **Issuer:** The Certificate Authority that issued the certificate.
  + **Subject:** The entity (e.g., website) to which the certificate is issued.
  + **Validity Period:** The time frame during which the certificate is considered valid.
  + **Digital Signature:** The CA's digital signature, which ensures the authenticity of the certificate.

**3. Types of Certificates:**

* There are various types of security certificates based on their intended use:
  + **SSL/TLS Certificates:** Used for securing websites and establishing encrypted connections (HTTPS).
  + **Code Signing Certificates:** Used to sign software and application code to prove authenticity and prevent tampering.
  + **Email Certificates:** Used for digitally signing and encrypting emails.
  + **Client Certificates:** Used for client authentication in various applications.

**4. Certificate Authorities (CAs):**

* Certificate Authorities are trusted entities responsible for issuing and managing security certificates. Web browsers and operating systems come pre-installed with a list of trusted CAs, and certificates issued by these CAs are automatically trusted.

**5. Certificate Chains:**

* Certificate chains are used to establish trust. The client (e.g., web browser) validates a certificate by checking its digital signature, ensuring it was issued by a trusted CA, and verifying the chain of trust from the root CA to the end-entity certificate (website/server).

**6. HTTPS (HTTP Secure):**

* HTTPS is the secure version of the HTTP protocol, used to encrypt data transmission between clients and servers. It relies on security certificates to establish a secure and encrypted connection.

**7. Certificate Revocation:**

* In case a security certificate is compromised or no longer valid, it can be revoked by the CA before its expiration date. Revocation information is published in Certificate Revocation Lists (CRLs) or using the Online Certificate Status Protocol (OCSP).

**8. Renewal and Expiration:**

* Security certificates have a defined validity period, typically ranging from a few months to several years. Certificate owners need to renew their certificates before they expire to maintain secure communications.

Security certificates are vital for securing sensitive information, building trust with users, and preventing man-in-the-middle attacks. They are an integral part of the secure communication infrastructure of the internet and play a significant role in maintaining the confidentiality and integrity of online transactions and communications.

**KT0404 Cookies**

Cookies are small pieces of data stored on a user's device (typically in the web browser) by websites they visit. These files are designed to remember specific information about the user's browsing activity and interactions with the website. Cookies are an essential part of modern web browsing and play various roles, such as personalization, session management, and user tracking. Here's an overview of cookies and how they work:

**1. Purpose of Cookies:**

* Cookies serve multiple purposes, including:
  + **Session Management:** Cookies help maintain user sessions, allowing websites to recognize users as they navigate between pages. This is particularly important for websites that require users to log in.
  + **Personalization:** Cookies can store user preferences and settings, enabling websites to deliver a personalized experience based on past interactions.
  + **Tracking and Analytics:** Cookies allow website owners to collect data on user behavior, track site usage, and analyze traffic patterns. This data is often used to improve website performance and user experience.
  + **Advertising:** Cookies are commonly used for targeted advertising, allowing advertisers to display relevant ads based on a user's browsing history and interests.

**2. Types of Cookies:**

* There are two main types of cookies:
  + **Session Cookies:** These are temporary cookies that are stored in the browser's memory during a user's session. They are deleted once the user closes the browser or navigates away from the website.
  + **Persistent Cookies:** These cookies are stored on the user's device for a specified duration, even after the browser is closed. They remain on the device until their expiration date or until the user manually deletes them.

**3. First-Party and Third-Party Cookies:**

* Cookies can also be categorized as:
  + **First-Party Cookies:** These are set by the website domain the user is visiting and are typically used for session management and personalization.
  + **Third-Party Cookies:** These are set by domains other than the website the user is visiting. Third-party cookies are often used for tracking and advertising purposes by external services and advertisers.

**4. Cookie Security and Privacy:**

* While cookies are generally harmless and serve useful purposes, concerns about privacy and security have led to increased scrutiny. Some users and privacy advocates are concerned about the potential for tracking and profiling users based on their cookie data.
* To address these concerns, web browsers often offer cookie settings that allow users to control and manage cookie behavior. Users can choose to block or delete cookies, manage cookie permissions, or set preferences for accepting cookies.

**5. Cookie Consent and GDPR:**

* The General Data Protection Regulation (GDPR) in the European Union requires websites to obtain explicit user consent before storing certain types of cookies, especially those used for tracking and targeted advertising.

**6. Clearing Cookies:**

* Users can clear cookies from their browsers at any time. Clearing cookies will remove stored information, such as login credentials and preferences, and reset website behavior.

In summary, cookies are a fundamental part of the web ecosystem and play a vital role in providing personalized experiences and session management. However, privacy and security considerations have prompted increased transparency and user control over cookie usage.

**KT0405 VPN (creates a secure tunnel between a user's computer and the Virtual private network server)**

A Virtual Private Network (VPN) is a technology that creates a secure and encrypted tunnel between a user's computer (or device) and a VPN server. This tunnel allows the user to access the internet or other network resources securely and privately. VPNs are commonly used for various purposes, including enhancing online privacy, bypassing geo-restrictions, and ensuring secure remote access to corporate networks. Here's how a VPN works:

**1. Secure Tunnel Creation:**

* When a user connects to a VPN, the VPN client on their device establishes a secure connection with the VPN server. This connection is encrypted, ensuring that data transmitted between the user's device and the VPN server is protected from interception and eavesdropping by unauthorized parties.

**2. Encryption and Data Privacy:**

* VPNs use strong encryption protocols to protect data as it travels through the secure tunnel. This ensures that even if someone intercepts the data, it appears as encrypted gibberish without the decryption keys.

**3. IP Address Masking:**

* When connected to a VPN server, the user's original IP address is replaced with the IP address of the VPN server. This process is called IP address masking or IP address spoofing. As a result, the user's online activities appear to originate from the VPN server's location rather than their actual location, providing a degree of anonymity and privacy.

**4. Bypassing Geo-Restrictions:**

* Since the user's traffic appears to be coming from the VPN server's location, VPNs can be used to bypass geo-restrictions imposed by certain websites or online services. For example, a user in a country with content restrictions can connect to a VPN server in a different country to access content that would otherwise be blocked.

**5. Secure Remote Access:**

* VPNs are commonly used for secure remote access to corporate networks. Employees can connect to the company's VPN server from remote locations, ensuring that their communication with the company's internal resources is encrypted and protected.

**6. Types of VPNs:**

* VPNs can be classified into two main types:
  + **Remote Access VPN:** These are used by individuals to connect to a private network securely from remote locations, such as employees accessing their company's network from home or on the go.
  + **Site-to-Site VPN:** These are used to connect entire networks together securely, allowing different offices or branches of an organization to communicate with each other as if they were on the same local network.

**7. VPN Protocols:**

* VPNs use various protocols to establish and maintain the secure connection, such as OpenVPN, L2TP/IPsec, IKEv2/IPsec, and PPTP. Each protocol has its own strengths and weaknesses in terms of security and speed.

Overall, VPNs are powerful tools for enhancing online security, privacy, and accessibility, making them popular among individuals and businesses alike. However, it's essential to choose a reputable and trustworthy VPN service, as not all VPN providers offer the same level of security and privacy protection.

**KT0406 Personal information and identity theft**

Personal information and identity theft are critical issues in the realm of cybersecurity and online privacy. Identity theft occurs when someone uses another person's personal information without their consent to commit fraud, financial crimes, or other malicious activities. Personal information refers to any data that can identify an individual, either directly or indirectly. Here's a closer look at these concepts:

**1. Personal Information:**

* Personal information includes, but is not limited to:
  + Full name
  + Date of birth
  + Social Security Number (or equivalent national identification number)
  + Address
  + Email address
  + Phone number
  + Financial information (bank account details, credit card numbers)
  + Online account credentials (username and passwords)
  + Medical records
  + Biometric data (fingerprints, facial recognition)

It's essential to protect personal information from falling into the wrong hands, as it can be used for malicious purposes.

**2. Identity Theft:**

* Identity theft occurs when a malicious actor obtains and uses someone's personal information without their knowledge or consent. The thief may use the stolen information to:
  + Open fraudulent credit card accounts
  + Make unauthorized purchases
  + Access the victim's bank accounts
  + Apply for loans or mortgages in the victim's name
  + File false tax returns to claim refunds
  + Commit other types of fraud or criminal activities

Identity theft can have severe financial and emotional consequences for the victim.

**3. Methods of Identity Theft:**

* Identity thieves use various methods to obtain personal information, such as:
  + Phishing: Sending fraudulent emails or messages to trick victims into revealing sensitive information.
  + Social Engineering: Manipulating individuals to divulge personal information or perform actions that compromise their security.
  + Data Breaches: Hackers gain unauthorized access to databases containing personal information.
  + Dumpster Diving: Physically searching through trash to find discarded documents with personal data.
  + Skimming: Placing devices on ATMs or point-of-sale terminals to capture credit card information.
  + Pretexting: Using fabricated scenarios to deceive individuals into disclosing personal information.

**4. Preventing Identity Theft:**

* Protecting personal information and preventing identity theft are essential for safeguarding one's financial and personal well-being. Here are some preventive measures:
  + Use strong and unique passwords for online accounts.
  + Enable two-factor authentication for added security.
  + Be cautious with sharing personal information online or over the phone.
  + Regularly review bank and credit card statements for suspicious activity.
  + Shred documents containing sensitive information before disposal.
  + Keep software and operating systems up-to-date to prevent vulnerabilities.
  + Be vigilant against phishing attempts and suspicious communications.
  + Monitor credit reports regularly for unusual activity.

By being proactive and cautious with personal information, individuals can reduce the risk of falling victim to identity theft and other forms of cybercrime.

**KT0407 Targeted advertising and ad blocking**

**Targeted Advertising:** Targeted advertising, also known as personalized advertising or behavioral advertising, is a form of online advertising that uses data collected from users' online activities to deliver advertisements tailored to their interests and preferences. The goal of targeted advertising is to present users with ads that are more relevant and engaging, increasing the likelihood of user engagement and conversion.

**How Targeted Advertising Works:**

1. **Data Collection:** Various entities, such as websites, advertisers, and ad networks, collect data about users' browsing behavior, search history, location, interests, and demographics using cookies and other tracking technologies.
2. **User Profiling:** The collected data is used to create user profiles, which contain information about users' interests, preferences, and behavior. These profiles are used to categorize users into specific audience segments.
3. **Ad Selection:** Advertisers use the user profiles to select ads that are most likely to resonate with each audience segment. The selected ads are then served to the corresponding users when they visit websites or use online services.
4. **Ad Delivery:** Targeted ads are delivered to users through various digital channels, including websites, social media platforms, mobile apps, and search engines.

**Benefits of Targeted Advertising:**

* Improved Relevance: Users are presented with ads that align with their interests, making them more likely to engage with the ads.
* Higher ROI: Advertisers can target specific audience segments, increasing the efficiency and effectiveness of ad campaigns.
* Enhanced User Experience: Users may find targeted ads less intrusive and more helpful compared to irrelevant or irrelevant ads.

**Ad Blocking:** Ad blocking refers to the use of software or browser extensions to prevent the display of ads on websites and other online platforms. Ad blockers work by blocking or filtering ad content, preventing it from loading and being displayed to the user.

**Reasons for Ad Blocking:**

* Improved Page Loading Speed: Ad-heavy websites can slow down page loading times, and ad blocking can improve the overall browsing experience.
* Privacy Concerns: Ad blockers can help prevent the collection of user data and protect privacy from aggressive tracking.
* Reduction of Intrusive Ads: Some users find certain ads disruptive, distracting, or annoying, and ad blocking helps to minimize such intrusions.
* Data Usage and Bandwidth Conservation: Blocking ads can reduce data usage, which is especially valuable for users on limited data plans or slow internet connections.

**Implications of Ad Blocking:**

* Impact on Publishers: Ad blocking can affect the revenue of website publishers and content creators who rely on ad revenue to support their services.
* Evading Non-Intrusive Ads: Some ad blockers can block non-intrusive and acceptable ads, which can negatively impact the business model of websites that adhere to non-intrusive advertising standards.
* Ethical Considerations: While ad blocking can benefit users, it can also raise ethical questions about content consumption and supporting free content on the internet.

**Conclusion:** Targeted advertising aims to provide relevant and engaging ads to users based on their preferences, while ad blocking offers users the option to control their online experience and protect their privacy. Both targeted advertising and ad blocking continue to be areas of debate in the digital advertising ecosystem, prompting discussions on the balance between user experience, privacy, and the sustainability of online content and services.

**KT0408 Cloud computing**

Cloud computing is a technology paradigm that enables the delivery of on-demand computing resources over the internet. Instead of hosting applications, services, and data on local servers or personal computers, cloud computing allows users to access and use computing resources, such as servers, storage, databases, networking, software, and other services, through the internet from cloud service providers. These resources are typically provided and managed by third-party vendors, offering a scalable and flexible solution for businesses and individuals. The key characteristics of cloud computing are:

**1. On-Demand Self-Service:** Users can provision and manage computing resources, such as server instances or storage, without requiring human intervention from the service provider.

**2. Broad Network Access:** Cloud services are accessible over the internet from various devices, including desktop computers, laptops, smartphones, and tablets.

**3. Resource Pooling:** Cloud providers share and allocate computing resources among multiple users, enabling cost optimization and efficient resource utilization.

**4. Rapid Elasticity:** Cloud resources can be scaled up or down quickly and dynamically based on demand, allowing for flexible and automatic resource provisioning.

**5. Measured Service:** Cloud computing services are typically metered, and users are billed based on their actual usage of resources, such as storage, processing power, and data transfer.

**Deployment Models of Cloud Computing:**

1. **Public Cloud:** In a public cloud, cloud services are offered and managed by third-party providers over the internet. Resources are shared among multiple users and are usually more cost-effective for small and medium-sized businesses.
2. **Private Cloud:** A private cloud is dedicated to a single organization and is typically hosted on-premises or in a data center managed by the organization. Private clouds offer enhanced security and control over resources but may require higher upfront investments.
3. **Hybrid Cloud:** A hybrid cloud combines both public and private cloud infrastructures, allowing organizations to integrate and move workloads between the two environments. This offers flexibility and the ability to address specific business needs.

**Cloud Service Models:**

1. **Infrastructure as a Service (IaaS):** IaaS provides virtualized computing resources over the internet, such as virtual machines, storage, and networking. Users have control over the operating systems and applications but not over the underlying infrastructure.
2. **Platform as a Service (PaaS):** PaaS offers a complete development and deployment environment in the cloud, including operating systems, development frameworks, databases, and more. Developers can focus on building applications without managing the underlying infrastructure.
3. **Software as a Service (SaaS):** SaaS delivers software applications over the internet, which are hosted and maintained by the service provider. Users can access these applications through a web browser without the need for installation or local management.

Cloud computing has revolutionized the way businesses and individuals use and manage computing resources. It provides scalability, flexibility, cost savings, and accessibility to a wide range of applications and services. As a result, cloud computing has become a fundamental technology for various industries and has transformed the IT landscape.

***Internal Assessment Criteria and Weight***

* IAC0401 The importance of personal security is elaborated.
* IAC0402 Vulnerabilities in terms of personal security are listed and described.
* IAC0403 Measures to mitigate or counteract vulnerabilities are evaluated in terms of how effective they are with regard to cyber resilience.

***(Weight 20%)***

# KM-03-KT05 : Mobile Security 20%

**Topic elements to be covered include:**

* KT0501 Internet of Things and how it affects our daily lives
* KT0502 ‘Bring Your Own Device’ or BYOD and security risks
* KT0503 Keeping own device safe from cyber attacks
* KT0504 Recognize a strong password
* KT0505 Using the Guest Wi-Fi when using your own device
* KT0506 Keeping devices up to date
* KT0507 Only use reputable websites for downloads
* KT0508 The Internet of Medical Things
* KT0509 Security risks related to mobile devices
* KT0510 Using mobile devices safely

**KT0501 Internet of Things and how it affects our daily lives**

The Internet of Things (IoT) refers to the network of physical objects or "things" embedded with sensors, software, and connectivity that enables them to collect and exchange data over the internet. These interconnected devices can communicate with each other and with central systems, allowing them to share information and perform various tasks without the need for human intervention. IoT has a significant impact on our daily lives, transforming the way we interact with technology and the world around us. Here are some ways IoT affects our daily lives:

**1. Smart Homes:**

* IoT-enabled smart home devices, such as smart thermostats, smart lighting, smart security cameras, and smart appliances, allow homeowners to control and automate various aspects of their homes remotely. This includes adjusting the temperature, turning lights on or off, monitoring security, and managing energy usage, enhancing convenience and energy efficiency.

**2. Wearable Devices:**

* IoT has given rise to wearable devices like smartwatches and fitness trackers. These devices can monitor health metrics, track physical activities, and provide real-time feedback, helping individuals make informed decisions about their fitness and well-being.

**3. Healthcare:**

* IoT plays a vital role in modern healthcare, with connected medical devices like remote patient monitoring systems, smart medical wearables, and telemedicine platforms. These technologies allow healthcare providers to monitor patients' health remotely, offer personalized treatment plans, and improve medical outcomes.

**4. Transportation:**

* IoT is revolutionizing transportation with smart connected vehicles. IoT-enabled features like GPS navigation, vehicle diagnostics, and connected infotainment systems improve driver safety, optimize vehicle performance, and provide real-time traffic updates.

**5. Retail and Supply Chain:**

* IoT is reshaping the retail industry through smart inventory management, supply chain optimization, and improved customer experience. IoT devices help retailers track inventory levels, monitor product movement, and analyze customer behavior, leading to better stock management and enhanced shopping experiences.

**6. Industrial IoT (IIoT):**

* In the industrial sector, IoT is used for asset tracking, predictive maintenance, and optimizing manufacturing processes. IIoT enhances operational efficiency, reduces downtime, and enables better decision-making through data analytics.

**7. Agriculture:**

* IoT technologies are increasingly being used in agriculture to monitor crop health, soil conditions, and weather patterns. This data-driven approach allows farmers to optimize irrigation, manage resources efficiently, and improve crop yields.

**8. Environmental Monitoring:**

* IoT devices are deployed for environmental monitoring and conservation efforts. They help collect data on air quality, water levels, weather conditions, and wildlife tracking, aiding in the protection and preservation of natural resources.

**9. Smart Cities:**

* IoT plays a key role in the development of smart cities by integrating various technologies to enhance urban living. Smart city initiatives may include smart streetlights, waste management systems, traffic management, and public safety applications.

While IoT brings numerous benefits and conveniences, it also raises concerns about privacy, security, and data protection. As the number of interconnected devices continues to grow, addressing these challenges becomes crucial to ensuring the safe and responsible deployment of IoT technologies in our daily lives.

**KT0502 ‘Bring Your Own Device’ or BYOD and security risks**

Bring Your Own Device (BYOD) is a workplace policy that allows employees to use their personal devices, such as smartphones, laptops, and tablets, to access company resources and perform work-related tasks. While BYOD offers benefits such as increased productivity, employee satisfaction, and cost savings, it also introduces several security risks that organizations need to address. Here are some of the security risks associated with BYOD:

**1. Device Diversity:**

* BYOD policies introduce a wide range of device types and operating systems into the corporate environment. Managing security across diverse devices can be challenging, as different devices may have varying security features and vulnerabilities.

**2. Lost or Stolen Devices:**

* Personal devices used for work can be lost or stolen, potentially exposing sensitive company data to unauthorized individuals. Without proper security measures in place, data on these devices can be easily accessed.

**3. Data Leakage:**

* Employees may inadvertently or intentionally transfer sensitive company data from their personal devices to unauthorized locations, such as cloud storage services or personal email accounts, increasing the risk of data leakage.

**4. Lack of Device Management:**

* Organizations may have limited control over personal devices, making it difficult to enforce security policies, update software, and apply necessary patches, leaving devices vulnerable to exploitation.

**5. Malware and Security Threats:**

* Personal devices may not have the same level of security software or monitoring as company-owned devices. This increases the risk of malware infections and other security threats that could spread to the corporate network.

**6. Insecure Wi-Fi Networks:**

* Employees often connect their personal devices to various public Wi-Fi networks, which are typically less secure. This creates opportunities for attackers to intercept data and launch man-in-the-middle attacks.

**7. User Awareness and Training:**

* Employees may not be aware of the security risks associated with using their personal devices for work purposes. Without proper training, they may inadvertently engage in risky behavior, such as downloading untrusted apps or accessing malicious websites.

**8. Compliance and Regulatory Concerns:**

* BYOD introduces additional challenges for compliance with data protection regulations and industry standards. Organizations must ensure that data on personal devices is adequately protected and managed to meet legal requirements.

**Mitigating BYOD Security Risks:**

To address the security risks associated with BYOD, organizations can implement the following measures:

1. **BYOD Policy:** Establish a comprehensive BYOD policy that outlines security requirements, acceptable use guidelines, data handling procedures, and consequences for policy violations.
2. **Mobile Device Management (MDM):** Use MDM solutions to manage and secure personal devices. MDM enables organizations to enforce security policies, remotely wipe data, and control access to company resources.
3. **Encryption:** Implement encryption for data at rest and data in transit to protect sensitive information on personal devices.
4. **Strong Authentication:** Require strong authentication methods, such as multi-factor authentication, to enhance the security of device access.
5. **Regular Updates and Patching:** Ensure that devices are up-to-date with the latest software and security patches to minimize vulnerabilities.
6. **Network Security:** Implement strong network security measures, such as VPNs, to protect data transmitted between personal devices and the corporate network.
7. **Employee Training:** Educate employees about the risks of BYOD and provide training on secure device usage and best practices.
8. **Separation of Personal and Corporate Data:** Encourage employees to segregate personal and work-related data on their devices to minimize the impact of potential security incidents.

By implementing these security measures and taking a proactive approach to BYOD security, organizations can strike a balance between the benefits of BYOD and the protection of sensitive company data.

**KT0503 Keeping own device safe from cyber attacks**

Keeping your own device safe from cyber attacks is crucial to protect your personal data, privacy, and digital identity. Here are some essential tips to enhance the security of your device:

**1. Keep Software Updated:**

* Ensure that your device's operating system, applications, and security software are up-to-date. Regular updates often include security patches to fix vulnerabilities that could be exploited by cyber attackers.

**2. Use Strong Passwords and Authentication:**

* Use strong, unique passwords for all your online accounts and devices. Consider using a password manager to generate and store complex passwords securely. Enable two-factor authentication (2FA) wherever possible for an extra layer of security.

**3. Be Cautious with Email and Messages:**

* Avoid clicking on links or downloading attachments from unknown or suspicious sources, as they may contain malware or phishing attempts. Be wary of unsolicited emails or messages asking for personal information.

**4. Install and Maintain Security Software:**

* Use reputable antivirus and anti-malware software on your device. Keep it updated and perform regular scans to detect and remove any potential threats.

**5. Use Secure Wi-Fi Connections:**

* Be cautious when using public Wi-Fi networks, as they may be insecure and prone to eavesdropping. Whenever possible, use a virtual private network (VPN) to encrypt your internet traffic and protect your data.

**6. Secure Physical Access:**

* Keep your device physically secure and avoid leaving it unattended in public places. Use a strong password or biometric authentication to lock your device when not in use.

**7. Be Wary of App Installations:**

* Download apps only from official app stores or trusted sources. Read reviews and check app permissions to ensure they are legitimate and not requesting unnecessary access to your data.

**8. Backup Your Data:**

* Regularly back up your important data to an external storage device or a secure cloud service. This will help you recover your data in case of a ransomware attack or device failure.

**9. Enable Find My Device (or Similar Feature):**

* Many devices offer a feature to locate, lock, or remotely wipe the device in case it is lost or stolen. Ensure that this feature is enabled and properly configured.

**10. Educate Yourself about Cybersecurity:**

* Stay informed about common cyber threats and best practices for online safety. Understanding potential risks can help you recognize and avoid potential security pitfalls.

**11. Be Cautious with Social Media:**

* Be mindful of the information you share on social media platforms, as cybercriminals may use this information for social engineering attacks or identity theft.

By following these security practices, you can significantly reduce the risk of falling victim to cyber attacks and maintain a safe and secure digital environment for yourself and your personal data.

**KT0504 Recognize a strong password**

A strong password is one that is designed to be difficult for others to guess or crack, making it more secure and less susceptible to unauthorized access. Here are the characteristics of a strong password:

**1. Length:** A strong password should be long, typically at least 12 characters or more. Longer passwords are generally harder to crack through brute force attacks.

**2. Complexity:** It should include a mix of different character types, such as:

* Uppercase letters (A-Z)
* Lowercase letters (a-z)
* Numbers (0-9)
* Special characters (e.g., !, @, #, $, %, etc.)

**3. Unpredictability:** Avoid using easily guessable information, such as common words, names, or phrases. Instead, use random combinations of characters.

**4. Unrelated to Personal Information:** Do not use personal information, such as your name, birthdate, or common words associated with you or your life.

**5. Unique for Each Account:** Use a different password for each online account you have. This way, if one password is compromised, your other accounts remain secure.

**6. Not a Dictionary Word:** Avoid using single words found in dictionaries or commonly used passwords. Dictionary attacks can easily crack such passwords.

**7. Avoid Common Patterns:** Stay away from common password patterns like "123456," "qwerty," or "password." These are among the most commonly used and easily guessable passwords.

**Examples of Strong Passwords:**

* H@ppy3P!zz@
* Tr1umPh$!D9
* 5ecur1ty#N0w
* J%5bMvD&L@p

Creating strong and unique passwords for each of your accounts is crucial for maintaining your online security. While strong passwords can be harder to remember, consider using a reputable password manager to securely store and manage your passwords. This way, you can have complex, unique passwords for all your accounts without the need to memorize them all. Remember to also enable two-factor authentication (2FA) where available for an added layer of security.

**KT0505 Using the Guest Wi-Fi when using your own device**

Using the Guest Wi-Fi when using your own device can be a good security practice, especially when you are in public places, hotels, or other locations where you are not familiar with the network's security measures. Here are some reasons why using the Guest Wi-Fi for your own device is recommended:

**1. Network Segregation:**

* Guest Wi-Fi networks are typically segregated from the main or private networks used by the organization or establishment. This separation helps protect your device from potential threats or attacks directed at the main network.

**2. Limited Access:**

* Guest Wi-Fi networks often have restricted access to certain resources and services. Your device will have limited access to other devices on the network, reducing the risk of unauthorized access to your device.

**3. Isolation from Other Devices:**

* Using the Guest Wi-Fi helps isolate your device from other devices on the network. This isolation provides an additional layer of protection against potential malware or attacks that could spread through the network.

**4. Less Risk to Your Private Network:**

* When you connect your device to a Guest Wi-Fi, you are not exposing your private home or work network to unknown or potentially unsafe environments.

**5. Reduced Attack Surface:**

* Using the Guest Wi-Fi means your device will have limited access to the internet and specific services. This reduces the potential attack surface, making it harder for cybercriminals to target your device.

**Best Practices When Using Guest Wi-Fi:**

While using the Guest Wi-Fi is generally safer than connecting to unknown public networks, it's essential to follow some best practices to ensure your device's security:

1. **Use HTTPS:** Whenever possible, access websites using HTTPS connections to encrypt your data and protect it from eavesdropping.
2. **Avoid Sensitive Transactions:** Refrain from conducting sensitive transactions, such as online banking or accessing confidential information, while connected to the Guest Wi-Fi.
3. **Disable Sharing and Network Discovery:** Turn off file sharing and network discovery on your device to prevent unauthorized access from other devices on the network.
4. **Stay Updated:** Keep your device's operating system, applications, and security software up-to-date with the latest patches and updates.
5. **Enable Firewall:** Ensure that your device's firewall is enabled to block unauthorized access attempts.
6. **Use a VPN (Virtual Private Network):** If you need to access sensitive information or conduct secure transactions, consider using a reputable VPN service to encrypt your internet traffic.

By using the Guest Wi-Fi and following these best practices, you can enhance the security of your own device and reduce the risk of potential cyber threats when connecting to public networks.

**KT0506 Keeping devices up to date**

Keeping devices up to date is a critical aspect of maintaining their security and overall performance. Manufacturers regularly release updates, also known as patches or software updates, to address security vulnerabilities, fix bugs, improve functionality, and enhance compatibility. Here are some reasons why keeping devices up to date is essential:

**1. Security Patches:**

* One of the primary reasons to keep devices up to date is to apply security patches. Cybercriminals continuously search for vulnerabilities in operating systems and software to exploit them. By updating your device, you ensure that known security flaws are fixed, reducing the risk of your device being compromised by malware or hackers.

**2. Bug Fixes:**

* Software updates often include bug fixes that address issues and glitches in the current version. These fixes can improve the stability and reliability of your device, preventing crashes or malfunctions.

**3. Performance Improvements:**

* Updates may also include performance enhancements that optimize the device's speed and responsiveness, leading to a smoother user experience.

**4. Compatibility:**

* Keeping your device up to date ensures compatibility with new applications, services, and hardware. Older software versions may not work properly with the latest technologies and features.

**5. Feature Updates:**

* Some updates bring new features and functionalities to your device, improving its capabilities and providing additional options for users.

**6. Device Longevity:**

* Regular updates can extend the lifespan of your device. By addressing security issues and maintaining optimal performance, you can delay the need for a new device purchase.

**Tips for Keeping Devices Up to Date:**

1. **Enable Automatic Updates:** Most devices offer an option to enable automatic updates. Turning this feature on ensures that your device receives the latest updates without manual intervention.
2. **Check for Updates Regularly:** If automatic updates are not available or not preferred, make a habit of checking for updates regularly and installing them promptly.
3. **Update All Software:** In addition to the device's operating system, remember to update all installed applications, including web browsers, antivirus software, and other third-party software.
4. **Backup Your Data:** Before performing major updates, back up your important data to ensure it is safe in case anything goes wrong during the update process.
5. **Verify Software Updates:** Only download and install updates from official sources or the device manufacturer's website. Avoid clicking on suspicious update prompts or downloading updates from unknown sources.
6. **Update Firmware and Drivers:** For devices like routers, printers, and other peripherals, check for firmware and driver updates from the manufacturer's website.
7. **Obsolete Devices:** Be aware that older devices may eventually reach the end of their support life, and manufacturers may stop releasing updates for them. In such cases, consider upgrading to a newer device with ongoing support.

By following these practices, you can ensure that your devices remain secure, perform optimally, and stay compatible with the latest technologies and applications.

**KT0507 Only use reputable websites for downloads**

Using reputable websites for downloads is an essential cybersecurity practice that helps protect your devices from malware, viruses, and other security threats. Downloading files from untrustworthy or malicious websites can expose your device to various risks, including potential data breaches, ransomware attacks, and identity theft. Here are some guidelines for ensuring safe downloads from reputable sources:

**1. Download from Official Websites:**

* Whenever possible, download software, applications, or files directly from the official website of the developer or publisher. Official websites are more likely to provide legitimate and safe downloads.

**2. Use Trusted App Stores:**

* For mobile devices, download apps only from official app stores like Google Play Store for Android devices and the App Store for iOS devices. These app stores have strict security measures in place to minimize the risk of malicious apps.

**3. Avoid File-Sharing Websites:**

* Be cautious about downloading files from peer-to-peer (P2P) or file-sharing websites. These platforms may not have proper security checks, and the files shared there can be infected with malware.

**4. Check Website Security:**

* Before downloading from a website, ensure that it uses a secure HTTPS connection. Look for the padlock icon in the website's URL address bar, indicating that the connection is encrypted and secure.

**5. Read User Reviews and Ratings:**

* If available, read user reviews and ratings for the software or files you intend to download. Positive reviews from reputable sources can provide assurance about the download's legitimacy.

**6. Avoid Pop-up Ads and Clickbait:**

* Be cautious of websites with excessive pop-up ads, flashy banners, or sensational clickbait content. These may be signs of untrustworthy sites attempting to lure users into downloading malicious content.

**7. Use Antivirus and Security Software:**

* Install reputable antivirus and anti-malware software on your devices. These security solutions can help detect and block potential threats during the download process.

**8. Keep Software Up to Date:**

* Ensure that your device's operating system, web browsers, and other software are up to date with the latest security patches. Updated software is less vulnerable to known security flaws.

**9. Be Cautious with Email Attachments:**

* Avoid downloading email attachments from unknown or suspicious sources. Cybercriminals may use phishing emails to distribute malicious files.

**10. Verify Digital Signatures:**

* For downloadable software or files that offer digital signatures, verify the authenticity of the signature to ensure it has not been altered or tampered with.

By adhering to these best practices and exercising caution when downloading files, you can reduce the risk of falling victim to malware or other cyber threats. Remember that an ounce of prevention is worth a pound of cure when it comes to cybersecurity.

**KT0508 The Internet of Medical Things**

The Internet of Medical Things (IoMT) is a subset of the broader Internet of Things (IoT) concept that specifically refers to the network of medical devices, sensors, software, and applications connected to the internet within the healthcare industry. IoMT is revolutionizing healthcare by introducing innovative technologies and solutions that enhance patient care, improve efficiency, and enable better health outcomes. Here are some key aspects and applications of the Internet of Medical Things:

**1. Medical Devices and Sensors:**

* IoMT encompasses a wide range of medical devices and sensors that can collect and transmit patient data to healthcare providers and medical systems. These devices include wearable health trackers, smartwatches, connected medical devices (e.g., glucose monitors, blood pressure monitors), and implantable devices.

**2. Remote Patient Monitoring:**

* IoMT enables remote patient monitoring, allowing healthcare professionals to monitor patients' health conditions in real-time, even outside of traditional healthcare settings. This continuous monitoring helps detect early signs of health issues and improves chronic disease management.

**3. Telemedicine and Telehealth:**

* IoMT plays a crucial role in telemedicine and telehealth services. Through secure video conferencing and remote consultations, patients can receive medical advice and treatment from healthcare providers without the need for in-person visits.

**4. Health Data Analytics:**

* IoMT generates vast amounts of health-related data. Advanced analytics and machine learning algorithms can process this data to gain valuable insights, predict disease patterns, and improve personalized patient care.

**5. Enhanced Patient Engagement:**

* IoMT devices and apps promote patient engagement by providing individuals with access to their health data and personalized health insights. This empowers patients to take a more active role in managing their health.

**6. Wearable Health Technology:**

* Wearable health devices, such as fitness trackers and smartwatches, are popular examples of IoMT applications that monitor physical activity, heart rate, sleep patterns, and more. These devices encourage healthier lifestyles and wellness tracking.

**7. Efficient Healthcare Delivery:**

* IoMT streamlines healthcare delivery processes by automating routine tasks, reducing administrative burdens, and enabling seamless data sharing between healthcare providers, leading to improved patient care coordination.

**8. Predictive Maintenance of Medical Devices:**

* IoMT can facilitate predictive maintenance for medical equipment, ensuring that critical devices are in good working condition and minimizing downtime.

**9. Security and Privacy Concerns:**

* The implementation of IoMT raises security and privacy concerns due to the sensitive nature of health data. It is crucial for healthcare organizations to implement robust security measures and adhere to strict data protection regulations.

While the Internet of Medical Things offers tremendous opportunities for healthcare advancements, it also requires careful consideration of security, data governance, and regulatory compliance to ensure patient safety and privacy. When implemented responsibly, IoMT has the potential to transform healthcare delivery, enhance patient outcomes, and improve the overall quality of healthcare services.

**KT0509 Security risks related to mobile devices**

Mobile devices have become an integral part of our daily lives, and with their increased usage comes a range of security risks. Here are some of the key security risks related to mobile devices:

**1. Lost or Stolen Devices:**

* One of the most common risks is the loss or theft of a mobile device. If the device is not adequately protected, unauthorized individuals can gain access to sensitive data, personal information, and potentially exploit the device for malicious purposes.

**2. Data Breaches and Unauthorized Access:**

* Mobile devices often store a significant amount of personal and sensitive data, such as emails, contacts, passwords, and financial information. If a device is compromised, this data can be exposed, leading to identity theft or financial fraud.

**3. Malware and Mobile Attacks:**

* Mobile devices are susceptible to malware, including viruses, ransomware, and spyware. Malicious apps, phishing links, and infected websites can all lead to the installation of malware on the device, putting data and privacy at risk.

**4. Unsecured Wi-Fi Networks:**

* Connecting to unsecured public Wi-Fi networks exposes mobile devices to potential man-in-the-middle attacks. Cybercriminals can intercept data transmitted over the network and steal sensitive information.

**5. Outdated Operating Systems and Apps:**

* Devices with outdated operating systems and applications may have known security vulnerabilities that can be exploited by attackers. Regular software updates are essential to patch these vulnerabilities.

**6. Jailbreaking and Rooting:**

* Jailbreaking (iOS) or rooting (Android) a device to gain access to restricted features can bypass built-in security measures, making the device more vulnerable to attacks and malware.

**7. Phishing Attacks:**

* Phishing attacks are prevalent on mobile devices, where users may be more susceptible to clicking on malicious links or providing sensitive information to fake websites or apps.

**8. Untrusted Apps and App Permissions:**

* Downloading apps from unofficial sources or granting excessive permissions to apps can compromise the device's security and privacy. Some apps may contain malware or collect user data without consent.

**9. Insider Threats:**

* Mobile devices used within an organization can be a source of insider threats if employees accidentally or intentionally leak sensitive data or compromise security practices.

**10. Physical Access Attacks:**

* Physical access to a mobile device can lead to unauthorized data access. Devices left unattended or not adequately locked can be exploited by malicious individuals.

**11. BYOD (Bring Your Own Device) Risks:**

* When employees use personal devices for work purposes (BYOD), it can lead to potential security challenges for organizations, as they have less control over the security of personal devices.

To mitigate these security risks, it's essential to implement best practices such as using strong passwords, enabling biometric authentication, encrypting data, installing reputable security software, keeping devices and apps up to date, avoiding unsecured Wi-Fi networks, and being cautious with app downloads and website interactions. Raising awareness about mobile security among users is also crucial in safeguarding personal and sensitive data on mobile devices.

**KT0510 Using mobile devices safely**

Using mobile devices safely involves following a set of best practices to protect your personal data, privacy, and security. Here are some essential tips to ensure safe mobile device usage:

**1. Use Strong Passwords or Biometric Authentication:**

* Set strong passwords or use biometric authentication (fingerprint, face recognition) to unlock your device. Avoid using easily guessable passwords, and enable two-factor authentication (2FA) for an extra layer of security.

**2. Keep Software Updated:**

* Regularly update your device's operating system, apps, and security software to ensure you have the latest security patches and bug fixes.

**3. Be Cautious with App Downloads:**

* Download apps only from official app stores (Google Play Store for Android, App Store for iOS) to minimize the risk of downloading malicious apps. Read user reviews and check app permissions before installation.

**4. Secure Your Wi-Fi Connections:**

* Use secure and trusted Wi-Fi networks. Avoid connecting to public, unsecured Wi-Fi networks, and use a Virtual Private Network (VPN) when accessing sensitive information over public Wi-Fi.

**5. Encrypt Your Device and Data:**

* Enable device encryption to protect your data in case the device is lost or stolen. Many devices offer built-in encryption options.

**6. Use Mobile Security Software:**

* Install reputable antivirus and anti-malware software on your mobile device to detect and prevent malicious threats.

**7. Be Cautious with Personal Information:**

* Avoid sharing sensitive personal information, such as your social security number or financial details, through text messages or email.

**8. Regularly Backup Your Data:**

* Back up your important data to a secure cloud service or an external storage device. Regular backups help safeguard your data in case of device loss, damage, or malware.

**9. Be Wary of Phishing Attacks:**

* Be cautious of suspicious emails, text messages, or app notifications that ask for personal information or contain malicious links. Avoid clicking on unfamiliar links.

**10. Set Device Lock Screen Timeout:**

* Set your device to lock automatically after a short period of inactivity to prevent unauthorized access.

**11. Disable Bluetooth and Wi-Fi When Not in Use:**

* Turn off Bluetooth and Wi-Fi when you are not using them to minimize the risk of unauthorized connections.

**12. Avoid Rooting or Jailbreaking:**

* Avoid rooting (Android) or jailbreaking (iOS) your device, as this can bypass security measures and expose your device to additional risks.

**13. Be Mindful of App Permissions:**

* Review app permissions carefully and only grant access to the necessary functions required for the app to function properly.

**14. Enable Find My Device:**

* Enable the "Find My Device" or similar feature to remotely locate, lock, or erase your device if it gets lost or stolen.

By following these safety tips, you can significantly reduce the risks associated with using mobile devices and protect your personal information from potential threats. Stay informed about the latest cybersecurity practices and stay vigilant while using your mobile device to ensure a safer digital experience.

***Internal Assessment Criteria and Weight***

* IAC0501 The importance of mobile security is elaborated.
* IAC0502 Vulnerabilities in terms of mobile security are listed and described.
* IAC0503 Measures to mitigate or counteract vulnerabilities are evaluated in terms of how effective they are with regard to cyber resilience.

***(Weight 20%)***

# KM-03-KT06 : Password protection 15%

**Topic elements to be covered include:**

* KT0601 Password and elements of a strong password
* KT0602 Identify commonly used passwords
* KT0603 Authentication methods
* KT0604 Multifactor authentication
* KT0605 Understand why personal information should not be used in a password
* KT0606 The hash process and how it can be used in a cyber-attack
* KT0607 Password managers

**KT0601 Password and elements of a strong password**

A strong password is essential for protecting your online accounts and sensitive information from unauthorized access. A strong password should be difficult for others to guess or crack while being easy enough for you to remember. Here are the elements of a strong password:

**1. Length:**

* A strong password should be sufficiently long. Aim for at least 12 characters or more. Longer passwords are generally harder to crack through brute force attacks.

**2. Complexity:**

* A strong password should include a mix of different character types, increasing its complexity and security:
  + Uppercase letters (A-Z)
  + Lowercase letters (a-z)
  + Numbers (0-9)
  + Special characters (e.g., !, @, #, $, %, etc.)

**3. Avoid Dictionary Words:**

* Avoid using single words found in dictionaries, as they are more vulnerable to dictionary attacks. Instead, consider using a combination of unrelated words or create a passphrase.

**4. Avoid Common Patterns:**

* Avoid using common patterns or sequences like "123456," "qwerty," or "password." These are among the most commonly used and easily guessable passwords.

**5. Unpredictability:**

* A strong password should be unpredictable and not easily associated with you or your personal life. Avoid using information such as your name, birthdate, or family members' names.

**6. Unique for Each Account:**

* Use a different password for each online account you have. Reusing passwords across multiple accounts can lead to severe consequences if one account gets compromised.

**7. Avoid Personal Information:**

* Refrain from using easily accessible personal information, such as your phone number, address, or favorite sports team, as part of your password.

**Examples of Strong Passwords:**

* 5Tr@wbeRry$P@rkL3
* P@ssw0rd$M@keMeH@ppy
* D0g$L0ves2Pl@y&JumP!

Creating strong and unique passwords for each of your accounts is crucial for maintaining your online security. While strong passwords can be harder to remember, consider using a reputable password manager to securely store and manage your passwords. This way, you can have complex, unique passwords for all your accounts without the need to memorize them all. Remember to also enable two-factor authentication (2FA) wherever possible for an added layer of security.

**KT0602 Identify commonly used passwords**

Commonly used passwords are often simple, easily guessable, and widely used by many people. These passwords are highly discouraged because they pose a significant security risk, making it easier for attackers to breach accounts. Here are some examples of commonly used passwords:

1. 123456
2. password
3. 123456789
4. qwerty
5. 12345678
6. abc123
7. letmein
8. admin
9. iloveyou
10. welcome
11. monkey
12. 1234567
13. 1234567890
14. passw0rd
15. football
16. 123123
17. login
18. princess
19. sunshine
20. password1

These passwords are easily guessed because they follow simple patterns, use sequential numbers, or contain commonly used words. To maintain strong security for your accounts, avoid using these passwords or any variations of them. Instead, use complex, unique passwords that include a mix of upper and lowercase letters, numbers, and special characters. Consider using passphrases, which are longer and more memorable combinations of words or phrases that are difficult for attackers to crack. Also, consider using a reputable password manager to generate and store strong passwords for your various accounts securely.

**KT0603 Authentication methods**

Authentication methods are techniques or processes used to verify the identity of a user or entity trying to access a system, application, or network. Authentication is a crucial aspect of cybersecurity and ensures that only authorized individuals can access sensitive information. Here are some common authentication methods:

1. **Password-Based Authentication:**
   * The most common form of authentication where users provide a username and password to gain access. As mentioned earlier, using strong and unique passwords is essential to ensure security.
2. **Multi-Factor Authentication (MFA) / Two-Factor Authentication (2FA):**
   * MFA or 2FA adds an extra layer of security by requiring users to provide two or more authentication factors. These factors can include something they know (password), something they have (a smartphone or hardware token), or something they are (biometric data like fingerprints or facial recognition).
3. **Biometric Authentication:**
   * Biometric authentication uses unique physical or behavioral characteristics of a person, such as fingerprints, facial features, iris or retinal scans, voice recognition, or even behavioral patterns like typing speed, as a means of verification.
4. **Token-Based Authentication:**
   * In token-based authentication, a physical or virtual token is used to generate one-time passcodes (OTPs). The token can be a hardware device or a mobile app. The user provides the OTP along with their password to complete the authentication process.
5. **Certificate-Based Authentication:**
   * Certificate-based authentication uses digital certificates to verify the identity of the user. The user's device or browser presents a digital certificate, which is signed by a trusted Certificate Authority (CA), to prove its authenticity.
6. **Single Sign-On (SSO):**
   * SSO allows users to log in once with a single set of credentials and then access multiple applications or systems without needing to log in again. It enhances user convenience while ensuring security and reducing password fatigue.
7. **Smart Cards and Smart Tokens:**
   * Smart cards and smart tokens are physical devices that store authentication credentials securely. Users insert the card or token into a reader to authenticate themselves.
8. **Knowledge-Based Authentication (KBA):**
   * KBA involves answering specific questions or providing personal information that only the legitimate user should know. However, KBA can be less secure, as personal information can be obtained through social engineering or data breaches.
9. **Pattern-Based Authentication:**
   * Pattern-based authentication uses gestures or patterns drawn on a touch screen as a means of authentication, commonly found in mobile devices.
10. **Location-Based Authentication:**

* Location-based authentication uses the user's geographic location as a factor in the authentication process. It can help detect unusual login attempts from unfamiliar locations.

Different authentication methods offer varying levels of security and convenience. Organizations often combine multiple authentication methods to create a robust and layered security approach to protect sensitive data and systems.

**KT0604 Multifactor authentication**

Multi-factor authentication (MFA), also known as two-factor authentication (2FA), is a security mechanism that requires users to provide two or more distinct authentication factors to verify their identity. It adds an extra layer of security beyond traditional password-based authentication, making it more challenging for unauthorized individuals to gain access to sensitive accounts or systems. The three primary authentication factors used in MFA are:

1. **Something You Know:**
   * This factor is typically a password or a Personal Identification Number (PIN). It is something that only the legitimate user should know and is the first line of defense in the authentication process.
2. **Something You Have:**
   * This factor involves possession of a physical or virtual token or device that generates one-time passcodes (OTPs) or access codes. The token can be a hardware device (e.g., security key) or a software-based app (e.g., authenticator app on a smartphone).
3. **Something You Are:**
   * This factor involves biometric authentication, where unique physical or behavioral characteristics of the user are used to verify their identity. Biometric factors may include fingerprints, facial recognition, iris or retinal scans, voice recognition, or behavioral patterns like typing speed.

To complete the authentication process with MFA, the user must provide at least two of these factors. For example, they may enter their password (something they know) and then use their smartphone to generate a one-time passcode (something they have) through an authenticator app.

Benefits of Multi-Factor Authentication (MFA):

* **Enhanced Security:** MFA significantly reduces the risk of unauthorized access and helps protect against password-related attacks like brute force or credential stuffing.
* **Protection Against Stolen Credentials:** Even if an attacker manages to obtain a user's password, they still need the second factor (e.g., smartphone) to gain access, making it much more challenging for them to succeed.
* **Compliance Requirements:** MFA is often required or recommended by industry standards and regulations to enhance data security and privacy.
* **Improved User Trust:** MFA provides users with confidence in the security of their accounts and information, promoting better trust with service providers.
* **Adaptability:** MFA can be implemented across various platforms and applications, offering versatile protection for different systems and services.

As cyber threats continue to evolve, adopting multi-factor authentication has become increasingly important for individuals and organizations to safeguard sensitive information and prevent unauthorized access to critical systems and data.

**KT0605 Understand why personal information should not be used in a password**

Using personal information in a password is highly discouraged due to the significant security risks it poses. Personal information is often easily accessible or discoverable, making it vulnerable to various cyber threats. Here are the reasons why personal information should not be used in a password:

1. **Predictability:** Personal information, such as your name, birthdate, or the names of family members, is relatively easy for attackers to guess or obtain through social engineering techniques or public records. Using such predictable information makes passwords weak and vulnerable to brute force attacks.
2. **Data Breaches and Social Engineering:** In today's interconnected world, data breaches are common. If you use personal information in your passwords, it becomes easier for attackers to exploit the information leaked in data breaches to gain unauthorized access to your accounts.
3. **Phishing Attacks:** Cybercriminals often use phishing emails to trick users into revealing personal information or login credentials. If your password includes personal information, you might inadvertently provide it to attackers who pose as legitimate entities.
4. **Password Cracking Tools:** Cybercriminals use sophisticated password cracking tools that can quickly go through combinations of personal information, dictionary words, and common patterns to crack passwords.
5. **Public Information on Social Media:** Many people share personal information on social media platforms, such as their birthdate, favorite sports teams, or pet names. This information can be used to guess or crack passwords.
6. **Lack of Complexity:** Using personal information alone in a password may not meet the complexity requirements set by various websites or services. Passwords should include a mix of characters (uppercase, lowercase, numbers, and special characters) to be more secure.

To create strong and secure passwords:

* Avoid using any personal information, such as your name, birthdate, or addresses.
* Use a mix of characters (uppercase, lowercase, numbers, and special characters).
* Create long passwords (at least 12 characters) that are difficult to guess.
* Consider using passphrases, which are longer and easier to remember than traditional passwords but provide increased security.
* Use different passwords for each of your accounts to avoid a domino effect if one password is compromised.
* Consider using a reputable password manager to generate and securely store complex passwords for your various accounts.

By avoiding the use of personal information in passwords and following best practices for password creation, you can significantly enhance the security of your online accounts and protect your sensitive information from cyber threats.

**KT0606 The hash process and how it can be used in a cyber-attack**

The hash process is a cryptographic technique used to convert data of any length into a fixed-size string of characters, typically represented in hexadecimal format. This fixed-size output is known as a hash value or hash code. Hashing is commonly used for various purposes in cybersecurity and data integrity, such as storing passwords securely, validating data integrity, and generating unique identifiers.

**The Hash Process:** The hash process involves the following steps:

1. **Input Data:**
   * The process starts with the input data, which can be any piece of information, such as a password, file, or message.
2. **Hash Function:**
   * A hash function is applied to the input data to generate a hash value. The hash function takes the input data and performs mathematical operations on it to produce a fixed-size output.
3. **Hash Value:**
   * The output of the hash function is the hash value. It is a unique representation of the input data, and even a slight change in the input data results in a significantly different hash value.
4. **Fixed Size:**
   * Hash functions always produce a fixed-size output, regardless of the size of the input data. For example, SHA-256 (Secure Hash Algorithm 256-bit) produces a 256-bit hash value.
5. **Irreversibility:**
   * Hashing is a one-way process, meaning it is computationally infeasible to reverse the process and obtain the original input data from the hash value. This property ensures that sensitive information remains secure.
6. **Collision Resistance:**
   * A good hash function should have collision resistance, meaning it is highly improbable for two different inputs to produce the same hash value. Collisions weaken the security of hashing, especially for applications like password storage.

**Use of Hashing in Cyber Attacks:**

1. **Password Cracking:**
   * In password cracking attacks, attackers obtain a hashed version of user passwords (e.g., from a compromised database). They then use various techniques, such as dictionary attacks or rainbow tables, to guess the original passwords that correspond to the hash values. This is why using strong hash functions and employing techniques like salting (adding random data to the input before hashing) are crucial for securely storing passwords.
2. **Data Integrity Attacks:**
   * In data integrity attacks, attackers modify data but want to maintain the same hash value to avoid detection. To achieve this, they need to find a collision, i.e., a different piece of data that produces the same hash value as the original data. However, finding collisions for secure hash functions is computationally challenging.
3. **Hash Extension Attacks:**
   * In hash extension attacks, attackers try to append or prepend data to an existing hash value in such a way that the new data, when hashed, matches the original hash value. This can potentially lead to privilege escalation or data tampering in certain applications.

To mitigate the risks of hash-related cyber attacks, it is essential to use strong and well-established hash functions, implement proper salting for password storage, and be aware of potential vulnerabilities associated with hash extensions and collisions. Additionally, staying up-to-date with the latest cryptographic standards and practices helps ensure the security of hash-based applications.

**KT0607 Password managers**

Password managers are software tools designed to securely store and manage passwords and other sensitive information, such as login credentials, credit card details, and personal notes. They provide a convenient and secure way to manage numerous passwords for different online accounts without the need to remember them all. Here's how password managers work and their key features:

**How Password Managers Work:**

1. **Secure Password Storage:** Password managers use strong encryption algorithms to securely store passwords and sensitive data. The user only needs to remember a master password, which grants access to the encrypted vault.
2. **Password Generation:** Password managers can generate strong and complex passwords for users, ensuring the use of unique and secure passwords for each account.
3. **Auto-fill and Auto-login:** Password managers can automatically fill in login credentials on websites and apps, streamlining the login process.
4. **Browser Extensions and Mobile Apps:** Password managers offer browser extensions and mobile apps for seamless integration across devices and platforms.
5. **Cloud Sync:** Many password managers offer cloud synchronization, allowing users to access their passwords and data across multiple devices.
6. **Two-Factor Authentication (2FA):** Some password managers support 2FA, adding an extra layer of security to the master password.

**Key Features of Password Managers:**

1. **Password Generation:** Generate strong and unique passwords for each account.
2. **Password Storage:** Securely store passwords and sensitive data in an encrypted vault.
3. **Auto-fill and Auto-login:** Automatically fill in login credentials on websites and apps.
4. **Form Filling:** Store and auto-fill personal information in online forms.
5. **Secure Notes:** Store and protect sensitive notes or information securely.
6. **Security Audit:** Analyze and identify weak or reused passwords.
7. **Browser Integration:** Support for popular web browsers for easy access and auto-fill functionality.
8. **Multi-Device Sync:** Synchronize passwords across multiple devices securely.
9. **Two-Factor Authentication (2FA):** Enhance security with 2FA for the master password.

Popular Password Managers:

1. LastPass
2. Dashlane
3. 1Password
4. Bitwarden
5. Keeper
6. NordPass
7. RoboForm
8. Enpass

Benefits of Password Managers:

* Improved Security: Password managers help create and manage complex, unique passwords, reducing the risk of password-related attacks.
* Convenience: Users only need to remember one master password to access all their passwords.
* Time-saving: Auto-fill and auto-login features save time when logging into websites and applications.
* Data Organization: Password managers help keep sensitive information organized and accessible.

While password managers enhance password security, it's essential to maintain the security of the master password and enable 2FA whenever possible. Regularly update the password manager software to ensure you have the latest security features and improvements. By using a reputable password manager, users can significantly improve their online security and reduce the risks associated with weak or reused passwords.

***Internal Assessment Criteria and Weight***

• IAC0601 Password protection to mitigate or counteract vulnerabilities is evaluated in terms of how effective they are with regard to cyber resilience.

***(Weight 15%)***

# REFERENCES

1. Improving Usability of Password Management with Standardized Password Policies. Retrieved on 2012-10-12.
2. *"Electronic Authentication Guideline" (PDF). nist.gov. USG. Retrieved 9 April 2020.*
3. *Statt, Nick (7 August 2017). "Best practices for passwords updated after original author regrets his advice". The Verge. Retrieved 9 April 2020.*
4. *Grassi Paul A. (June 2017). SP 800-63B-3 – Digital Identity Guidelines, Authentication and Lifecycle Management. NIST.* This article incorporates text from this source, which is in the public domain*.*
5. *"Password Complexity Requirements". The Bug Charmer. September 7, 2012.*
6. *"How long should passwords be?". The Bug Charmer. June 20, 2016.*
7. *John D. Sutter (August 20, 2010). "How to create a 'super password'". CNN. Retrieved August 31, 2016.*
8. *"The problems with forcing regular password expiry". IA Matters. CESG: the Information Security Arm of GCHQ. 15 April 2016. Archived from the original on 17 August 2016. Retrieved 5 Aug 2016.*
9. *"BYOD and Increased Malware Threats Help Driving Billion Dollar Mobile Security Services Market in 2013". ABI Research. 2013-03-29.*
10. *Kasmi C, Lopes Esteves J (13 August 2015). "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones". IEEE Transactions on Electromagnetic Compatibility.*
    * *Andy Greenberg (14 October 2015). "Hackers Can Silently Control Siri From 16 Feet Away". Wired.*
11. *McCaney, Kevin (7 May 2012). "'Unknowns' hack NASA, Air Force, saying 'We're here to help'". Retrieved May 7, 2012.*
12. *Michael SW Lee; Ian Soon (2017-06-13). "Taking a bite out of Apple: Jailbreaking and the confluence of brand loyalty, consumer resistance and the co-creation of value". Journal of Product & Brand Management.*