Securing Wireless Hotspots
http://www.cert-in.org.in/

Description

Wi-Fi is now becoming a necessary requirement in a variety of areas like airports hotels , coffee shops, libraries, and restaurants. With the increasing use of smartphones and the deployment of 4G (long-term evolution-LTE) mobile networks, people are preferring publicly accessible wireless networks over other network accesses. Concerns about the security of public WiFi hotspots and other Wi-Fi accesses are increasing since it threatens the confidentiality and integrity of user data. As attacks specifically targeted at stealing user data increase, sophisticated attacks are becoming common in today's news. In this document the best practices for securing public hotspot implementations are given along with suggested network architectures.

1. Security Best Practices for Service Providers

Protect network against unauthorized use of services

- Authenticate the Users with Authentication protocols like 802.1x,RADIUS and EAP (EAP -PAX,EAP-PSK,EAP-TLS ,EAP-TTLS ,EAP -FAST,EAP -POTP,EAP -1KEVs) in the authentication Gateway for authentication of the credentials that include digital certificate ,user name(s) and passwords,secure tokens etc.
- Implement Access Point (AP)/ Wireless LAN Controller (WLC) devices that do rogue threat detection, assessment, location tracking & mitigation, by scanning, detecting & containing rogue Access Points & ad-hoc networks.
- Enable management frame impersonation detection by the Wireless APs.
- Secure network services using authentication and access controls and filter these services as far as possible : Network Services such as Dynamic Host Configuration Protocol(DHCP), Domain Name System DNS, Authentication Authorization, and Accounting (AAA),
- Simple Network Management Protocol (SNMP), SYSLOG, Network Time Protocol (NTP), Internet Protocol Security (IPSEC) must only communicate with other network services based on a specific and restricted list of addresses or subnets
- Network services must be configured with authentication credentials such as certificates, shared passwords or similar,

if supported, when communicating with other network service providers

- Configure Access lists to explicitly allow devices that are authorized peers on the network.
- Access to network services must be filtered by a firewall
- Authenticate and encrypt all protocols on the network e.g. Control And Provisioning of Wireless Access Points (CAPWAP), Open Shortest Path First (OSPF) etc. and use secure management protocols like SSH (Secure Shell), HTTPS for all control traffic
- Use a centrally controlled wireless Intrusion Detection/Prevention Systems (IDS/IPS) to monitor for unauthorized access and to detect rogue and misconfigured wireless devices. Enable historical logging of wireless access that can provide granular wireless device information and store event logs and statistics . Enable IPS features to automatically disable rogue wireless devices. Ensure the IPS signature set is regularly updated as new threats are discovered.
- Coordinate and correlate wireless logging events with other networking devices within the environment. Implement processes and policies that include regularly reviewing and acting on the data provided by the IDS/IPS.Regularly test the security of the wireless network using the best available intrusion Detection systems , Wardriving tools.

Protect the network against DoS attacks making services unavailable

- Use control plane policing to police the traffic going to the device CPU. This would include rate limiting all control traffic like SNMP/ ICMP/Routing protocol traffic etc, and using access lists to explicitly define which devices can send packets to this device.
- Monitor the resource utilization on the devices eg. CPU, memory, CAM tables at all times to quickly detect any attacks.
- Disable all unneeded services on the devices like ICMP redirects, ICMP unreachable, IP source routing etc. that can be used to launch an attack.
- Have a consistent MTU on the network to avoid any unnecessary fragmentation and reassembly on the devices.
- Use devices that can do intrusion detection on DoS attacks through the use of signatures.
- Data plane DoS attacks can be mitigated by monitoring through

Netflow and identifying attacks, and black-holing/ scrubbing them through specialized devices.

- Protect the confidentiality of user data on the network
- Detect rogue APs and contain them by using the genuine APs to scan & detect rogue ones.
- Deploy Wireless infrastructure that can detect any breakage into the network devices and identify the attacker and rogue files.
- Encrypt traffic wherever possible eg using DTLS over CAPWAP & IPSec.
- Protect all control services like DNS, DHCP, User databases behind firewalls by using IDS/ IPS systems.
- Explicitly allow devices that can access the backend systems using access lists and firewall policies.
- Use secure methods of accessing this information from the backend systems.
- Maintain logs for any triggers/ alarms/ login failures.
- Enforce strict control over port spans.
- Use end to end IPSec for additional user security on the data plane for application security.

Protect the network devices against unauthorized access

- Harden the device using the security guidelines of the organization
- Create a hierarchy of users who can access the network and ensure there is role based access such that only authorized personnel can make critical changes on the network.
- Enforce access lists on the devices to allow the subnets from which users can access the devices.
- Use secure management protocols like HTTPS & SSH.
- Allow a limited number of users to login concurrently into the device.
- Log all failed attempts at login through a logging server and monitor the logs regularly.
- Use AAA and have command level authorization & accounting for users.
- User security & user tracking
- Design networks to allow service access after authentication either through a web portal or based on SIM.
- Use Two Factor authentication for all network/ service access.
- Allow service access to the user by authenticating against credentials that are verifiable eg. using Phone numbers and one

Time Passwords (OTPs).

- Maintaining a verified user database for voucher based access at the point of sale of the vouchers.
- Using unique public IP addresses for end users or by maintain NAT logs for private & public IP address mappings for all sessions.

2. Security Best practices for users

- Always ask the owner of the Wi-Fi hotspot for the correct network name and password You should ensure that the web pages you visit are https encrypted where possible. You can check this by looking for https at the start of the URL address bar, or for the security padlock sign.This indicates that the website, and that particular page, has a valid digital certificate and up-to-date SSL/TLS encryption, thus making Man-in-the-Middle (MiTM) attacks much less likely.
- Patching and updating software on a regular basis is an essential security practice, especially when it comes to Wi-Fi.You should keep your web browser, software and antivirus solution up-to-date to fix bugs, while an up-to-date antivirus engine will scan, detect and remove the latest threats.
- Public Wi-Fi networks should not be used to access email, online banking and credit card accounts, or any other sensitive data for the matter.
- Make sure your laptop, tablet or smartphone are set to manually select a Wi-Fi network, rather than having it automatically connect. Also, turn off sharing and Wi-Fi capabilities when the wireless is not in use, as this cut downs possible avenues for cybercriminals to exploit. You should also remember to tell your phone or tablet to "forget" certain networks if they are no longer in use or required, as this could mean your device will automatically reconnect when back in range.
- Consider a virtual private network (VPN): This is a safe way of surfing the web in an encrypted manner.VPN solutions provide encryption and security across public networks, as well as masking your IP address so that opportunities for phishing are dramatically reduced.
- Enable two-factor authentication where possible. 2FA is increasingly seen as the future of authentication and it is wise for anyone using a hotspot. This per-website step adds an extra layer of protection for public password-sniffing hackers to try and overcome.
- Logout when finished and Turn off Wi-Fi if not in use.

References

1. Enterprise Wireless Fidelity Implementations Using Port Based Network
2. Access Control (IEEE 802.1X) - International Journal of Computer Science, and Telecommunications [Volume 3, Issue 7, July 2012] www.ijcst.org/Volume3/Issue7/p20_3_7.pdf
3. http://www.welivesecurity.com/2015/09/02/10-steps-staying-secure-public-wi-fi/
4. www.cisco.com