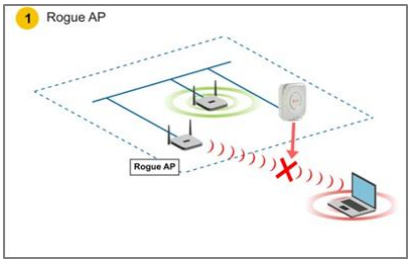
## WI-FI SECURITY

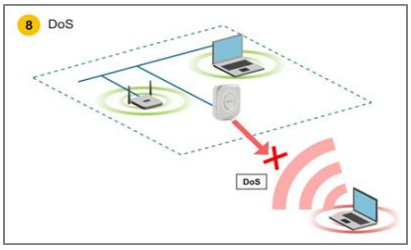
When developing your Wi-Fi strategy consideration should be given to the different types of threats that can occur over a Wi-Fi access network, from simple misconfiguration to focussed attacks. Wireless Intrusion Detection (WIDs) and Wireless Intrusion Protection (WIPs). We have listed here the most common types of threats to a Wi-Fi network. For further information and how Hughes can help prevent these types of attacked please call Hughes Europe on **+44 (0)1908 425 355**

### Rogue Access Point



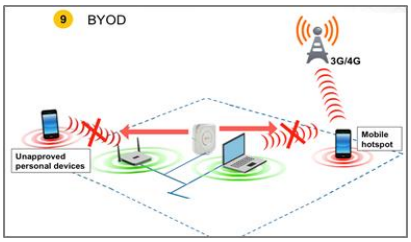

A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-the-middle attack

### Denial of Service (DOS)



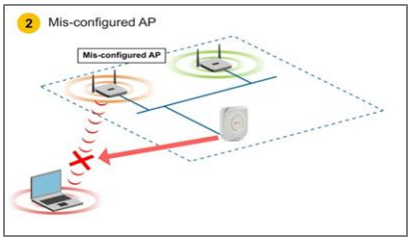

A Denial-of-Service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP)

### Bring Your Own Device (BYOD)



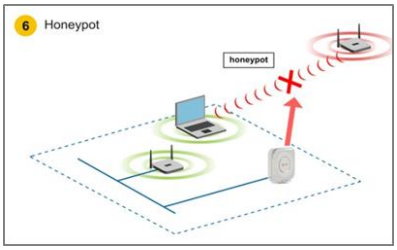

The BYOD trend is causing new security concerns for enterprise networks and data security. Corporate users (e.g. employees, contractors and visitors) are accessing network and data and bypassing corporate security controls using their personal Wi-Fi devices. This uncontrolled access can open backdoors into the enterprise network, leaking sensitive data, exposing the network to malware and potential malicious activity.

### Miss-configured Access Point




Threat to security due to incorrect settings on access points allowing unauthorised access to systems. This could be open access without passwords set or incorrect SSIDs set.

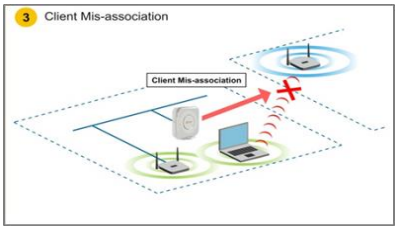
### Honey Pot / Man in the Middle




Normally, when a wireless client (PC, Laptop) is switched on, it will try to probe the nearby area for access points for a particular SSID (SSID is like a name for the network, which is advertised in order for users and clients to associate with the access points). In this scenario, if a hacker is nearby (perhaps in the car parking), he could use access points with high power (gain) antennas with the same SSID as the corporate network SSID and respond to such client probe requests with a valid probe response. As the wireless clients generally associate with an access point with the highest power (signal strength), it can get associated to the access point belonging to the hacker. A man-in-the-middle attack is an extension of the honeypot attack whereby the attacker entices computers to log into a computer which is setup as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic.

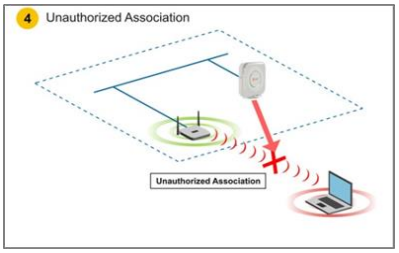
### Client Miss-Association

Wireless miss-association is a security vulnerability resulting from wireless connection (called as “association” in the 802.11 jargon) of wireless clients in the enterprise network to neighbouring APs. The miss-association can happen with or without the knowledge of the wireless client and the neighbouring AP. It creates avenue for enterprise security policy violations, and attacks on the enterprise network and the wireless client itself. Miss association is also called as “accidental association” or client “wandering”.



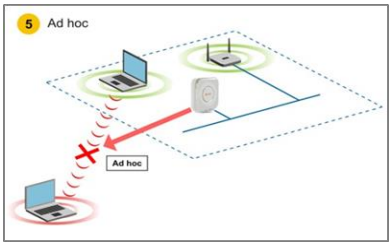

### Unauthorised Association

In an enterprise network environment, rogue access points installed by employees do not usually follow the network's standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired network. One of the major concerns that most wireless network administrators face is unauthorized associations between stations in an Access Control List and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information



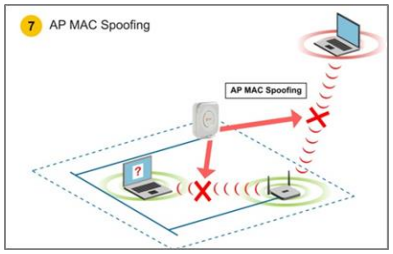

### Ad Hoc

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.



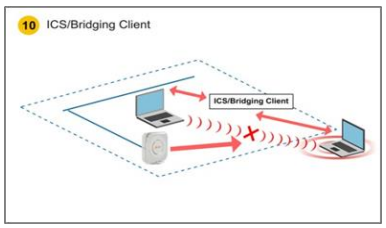

### Access Point MAC Spoofing

Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to only allow authorized computers with specific MAC IDs to gain access and utilize the network. However, a number of programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the cracker desires, and the cracker can easily get around that hurdle.




### Internet Content Sharing (ICS) Bridging Client

Network interface bridging and internet connection sharing (ICS) opens up security threats between devices. Virtual Wi-Fi creates a wireless hotspot by "bridging" communication between two wireless interfaces on a host -- one that is used for client operations and the other that is used for AP operations. Note that the AP mode operation is very similar to that of a network address translation (NAT) AP




## EXPERIENCE THE HUGHES DIFFERENCE

Part of Echostar a billion dollar global company and with offices in United Kingdom, Germany, and Italy, Hughes Network Systems Europe (Hughes Europe) is a market-leading provider of high-quality, resilient and cost-effective broadband networking and customer experience solutions to organisations throughout Europe. Combining the best of breed in terrestrial, mobile and satellite technologies with E-learning and Digital Media solutions and world-class Managed Network Services, for international delivery and multi-site integration Hughes Europe is uniquely positioned to meet the individual requirements of the distributed enterprise.

**For additional information, visit www.hugheseurope.com or call us on +44 (0) 1908 425 355**



Hughes Network Systems Europe Ltd
Hughes House
Rockingham Drive
Linford Wood East
Milton Keynes. MK14 6PD. UK