

Municipal Wi-Fi Risks & Solutions

Amit Sinha, Chief Technology Officer, AirDefense, Inc.

Proliferation of Municipal Wi-Fi

The promise of pervasive wireless broadband access using license-free spectrum and commodity IEEE 802.11 based Wi-Fi networking gear is indeed enticing. While 802.11 is a local area networking standard, innovative mesh networking solutions using wireless backhubs allow coverage areas to be extended to city-wide deployments. According to an ABI research report published in March 2006, municipal Wi-Fi network coverage worldwide will grow from about 1,500 square miles in 2005, to 126,000 square miles by 2010. More than one million wireless mesh routers will be shipped in 2010 to support municipal Wi-Fi networks and the manufacturing revenues from those shipments will exceed US \$1.2 billion.

Threats to Municipal Wi-Fi Providers

Today, over 300 US cities are deploying or considering municipal Wi-Fi. Security is an afterthought in most of these deployments. City officials do not want the headaches and cost associated with supporting heterogeneous clients and security protocols. The City of Philadelphia was one of the first adopters of municipal Wi-Fi. In fact, according to the Wireless Philadelphia Business Plan, "...the more secure the network is, the more complicated the provisioning process can become. Open access in parks and public spaces should limit the provisioning requirement to confirmation of an acceptable use policy and disclaimer."

The established vulnerabilities of the IEEE 802.11 protocol coupled with the pervasive availability of municipal Wi-Fi makes it a perfect playground for hackers. Evil Twin and Wi-Phishing attacks that were restricted to hotspots can now proliferate city-wide. Hackers can lure unsuspecting corporate laptops to associate with soft Access Points (APs) that look and feel like municipal Wi-Fi using free and readily available tools.

Security Risks of Users and Enterprises Surrounded by Municipal Wi-Fi

More and more enterprises and independent operators find their air space being invaded by free, insecure and pervasive Wi-Fi. Established wired security paradigms such as content filtering and internet access policy enforcement break down with unrestricted and pervasive wireless access. Consider a scenario where a security sensitive Fortune 1000 company's office is present in an area with a municipal Wi-Fi deployment. An employee can bypass wired security and policy enforcement restrictions by simply connecting to the internet through a readily available municipal Wi-Fi node. Security compliance management becomes increasingly difficult. The employees can use external email servers, send instant messages, access forbidden sites, day trade, sell stuff on eBay, etc. – many of which could be against corporate internet access policies and were previously enforced using wired network controls. Such unrestricted access of enterprise computers to the public wireless networks can unleash a new security threat since they are bypassing established wired access security mechanisms such as network Firewalls, IPS, UTM, Spyware/Spam blockers, etc. Enterprise laptops can unwittingly reveal passwords and other confidential information over these insecure wireless networks. The company's security is reduced to being only as good as the security of the weakest PC and its user.

Enterprises with their own wireless LANs will run into co-channel interference from the municipal Wi-Fi network and wireless performance will degrade because there is no centralized frequency planning and RF management. Accidental or intentional associations of corporate laptops with municipal wireless nodes increase significantly causing larger attack surfaces that IT security must now worry about.

Solutions for the Enterprise and Municipal Wi-Fi Users

Mobile wireless devices are often the weakest link in the enterprise security infrastructure. Realizing that laptops and mobile workers are extending the edge of the corporate network is essential. Pervasive wireless networks such as municipal Wi-Fi are invading the enterprise perimeter itself. Firewalls and VPNs provide only limited protection to wireless devices from the rising threat of wireless Layer 2 attacks. Monitoring the air space and enforcing centralized policy for wireless access is required. AirDefense, the market leader in anywhere, anytime wireless protection, has a comprehensive solution to mitigate wireless threats. The AirDefense Enterprise product provides total protection of the enterprise wireless perimeter by monitoring the air space 24x7 using dedicated sensors capable of detecting and preventing rogue devices, unauthorized communications/connections, wireless attacks and enforcing wireless policy centrally. The AirDefense Personal product works in conjunction with firewalls and VPNs on laptops to prevent Layer 2 attacks and vulnerabilities while allowing enterprises to centrally monitor and enforce common wireless policies across the organization's laptops. Using AirDefense Personal enterprises can allow safe use of hotspots and municipal Wi-Fi. Independent municipal Wi-Fi users can guard themselves from Evil Twin and Wi-Phishing type attacks using AirDefense Personal.

Solutions for the Municipal Wi-Fi Providers

AirDefense Enterprise sensors can be used in conjunction with municipal Wi-Fi nodes to monitor and protect coverage areas. These sensors can detect malicious activity, rogue devices, identity theft, performance and connectivity problems, etc. The sensors can be used to terminate rogue devices and unauthorized connections on the municipal Wi-Fi network without disrupting regular service. They could even be used to terminate Evil Twins and Rogue APs that masquerade as legitimate municipal Wi-Fi nodes. The forensic capabilities of the AirDefense product can be used to historically troubleshoot performance and security issues while managing compliance and liability problems.

Further, municipal Wi-Fi operators can encourage their subscribers to use AirDefense Personal on their laptops as a Layer 2 Firewall to safeguard them from Evil Twin and Wi-Phishing attacks. This will reduce their support and liability problems as well.