



MEDIA ALERT

Media Contacts: Lorraine Kauffman-Hall, for AirPatrol Corp., 704-882-0443, lhall@attainmarketing.com

AirPatrol Teams Up with CSI to Uncover Advanced Wi-Fi Attacks

New Video Production Unveils Invisible Threats to Corporate Networks and Data

CSI 2007, Washington DC, Nov. 5, 2007 – AirPatrol Corporation, the most trusted authority on wireless threats to wired and wireless networks, today announced its work with the Computer Security Institute (CSI), publisher of the world's most widely quoted research on computer crime, to uncover wireless security threats introduced by laptops in the enterprise. In a flagship video production entitled “CSI in Motion: the Hidden Wireless Threat”, CSI and AirPatrol unveiled potential attacks to both wired and wireless networks posed by Wi-Fi-enabled notebooks. As part of the video, AirPatrol demonstrated the first set of tools that completely protects against schemes like Wi-Phishing by tracking notebooks and wireless activity in an enterprise, giving businesses the power to shut down unauthorized users on the spot.

“CSI’s take is that wireless networks remain vulnerable to fairly easy attacks and enterprise-connected notebooks with wireless capabilities can open potentially serious security holes,” said Robert Richardson, Director of the Computer Security Institute. “Our work with AirPatrol on our just-launched “CSI in Motion” program shows how hackers can use the simple connection of a wireless notebook to a wired network to open up an entry point into a corporation’s most sensitive data – and what companies can do to stop them.”

Wi-Phishing is an insidious form of Wi-Fi attack that can occur without detection by the user. In a Wi-Phishing attack, the hacker sets his trap using a wireless router with a commonly used service set identifier (SSID) such as “linksys” or “tmobile” to lure laptops into automatically connecting with a bogus network as soon as they are in range. If this happens while the employee is connected to the corporate network through a wired Ethernet port, the hacker not only has an IP connection to the attacked laptop, but is also in a position to bridge from his fraudulent wireless network to the user’s corporate network – at which point the hacker has access behind the firewall.

Today, there is strong evidence that supports the fact that wireless attacks are being used to perpetrate network breaches and serious cybercrimes. Insufficient WLAN security has been blamed for the TJX breach of some 94 million cards. The recently released 2007 CSI Computer Crime and Security Survey reported that the "abuse of wireless network" as one of nineteen different kinds of security attack or incident, up from last year and ranking ahead of nine other categories.

“WiPhishing and other attacks not only increase the likelihood of a security breach, but also can place today’s businesses in violation of regulatory policies and industry directives, such as Gramm Leach Bliley Act (GLBA), Sarbanes-Oxley Act (SOX), and Payment Card Industry (PCI),” said Nicholas Miller, CEO of AirPatrol. “Our work with CSI demonstrates potential Wi-Fi risks and shows how Air Patrol's toolset can provide a virtual shield around the physical perimeter of an office space, enabling businesses to view actual wireless policy breaches in the field and pinpoint the location of the laptop causing the problem to within a few feet.”

AirPatrol will be showcasing its advanced location-based security tools at CSI 2007. In addition, Nicholas Miller, a well known wireless security expert, will be addressing CSI 2007 attendees to show how businesses are at risk today and what steps they should take to protect against the dangers posed by the widespread use of wireless laptops now flooding the workplace.

[Click here - or go to \[www.Gocsi.com\]\(http://www.Gocsi.com\) - to view “CSI in Motion: The Hidden Wireless Threat”.](#)

About AirPatrol Corporation

AirPatrol Corporation, the most trusted authority on wireless threats to wired and wireless networks, offers a comprehensive suite of location-based wireless solutions that enable companies to keep pace with the expanding requirements of an increasingly mobile world. Based on an expert understanding of real-world industry needs, AirPatrol delivers the innovations that businesses depend on to confidently deploy, manage and protect networks against present and future wireless threats. Customers and partners include leading mobile innovators, Fortune 100 enterprises and high-profile government agencies around the globe. AirPatrol is a privately held company with offices in the US, Canada and Europe. For more information, please visit the company’s website at www.airpatrolcorp.com.