Summit White Paper: PCI DSS in a post-TKIP World

Retailers must tighten Wi-Fi security

Akron Ohio, June 10, 2010 – TKIP, the encryption method once required on all Wi-Fi® devices, soon will be prohibited. A white paper from Summit Data Communications explains the implications for retailers that rely heavily on Wi-Fi and must be compliant with the Payment Card Industry Data Security Standard (PCI DSS).

"Retailers have relied on wireless local area networks since before the first Wi-Fi standards were ratified," said Chris Bolinger, Summit VP of Business Development and the paper's primary author. "TKIP is a key element of Wi-Fi security in many retail stores and distribution centers, but TKIP is not strong enough to satisfy PCI DSS requirements."

When the original Wi-Fi encryption mechanism of WEP was found to be vulnerable to attack, the Wi-Fi Alliance® created a security specification called Wi-Fi Protected Access®, with Temporal Key Integrity Protocol (TKIP) as its encryption method. Like WEP, TKIP uses RC4 encryption, but TKIP is designed to address vulnerabilities of WEP by encrypting each data packet with a different key, preventing key reuse during a session, and ensuring that the message is not altered in transit between sender and receiver.

In late 2008, two German researchers reported that a vulnerability in TKIP could enable an attacker to decrypt individual packets that are encrypted with TKIP. In mid-2009, two Japanese researchers reported that they had expanded on the German researchers' work and devised a way to mount a successful attack on TKIP. The latter report received a lot of media attention, with some articles claiming that TKIP can be cracked in less than one minute. In reality, neither of the reports demonstrated that a practical tool for cracking an actual TKIP key or deciphering TKIP-encrypted data packets is imminent.

The two reports, however, were enough to sound the death toll for TKIP. The Wi-Fi Alliance has announced that it is phasing out TKIP, first on infrastructure devices and then on client devices. Beginning January 1, 2011, TKIP will be prohibited in Wi-Fi infrastructure except as a component of WPA2®, the successor to WPA. In a few years, TKIP will be prohibited in any Wi-Fi CERTIFIED™ device.

"Retailers often use Wi-Fi client devices for a decade or longer," said Bolinger. "Devices manufactured before 2006 may not support WPA2. The Enterprise version of WPA2, with its robust, bidirectional authentication and strong encryption using AES-CCMP, now is a PCI DSS requirement for all wireless LANs and client devices that have access to credit card and debit card information. To protect themselves and their customers, retailers must move to WPA2-Enterprise."

The Summit white paper, "Wi-Fi Client Device Security and Compliance with PCI DSS", is available free of charge from the Summit Web site, www.summitdatacom.com.

About Summit
Summit Data Communications, Inc. is the *mobile* in today's mobile computers and other business-critical mobile devices. Summit's embedded Wi-Fi solutions provide secure, reliable connections in the challenging environments in which business-critical mobile devices operate, including factories, warehouses, ports, hospitals, and retail stores. For more information, visit www.summitdatacom.com.