securityinformed.com
Making The World A Safer Place

Farpointe Data Alerts Its Partners To Encrypt Wireless Access Control Systems

Published on 29 Jun 2017

Farpointe Data, the access control industry's trusted OEM partner for RFID solutions, alerted its access control manufacturer, distributor, integrator, dealer, and specifier partners about the potential impact on their businesses of the settlement of Edenborough v. ADT LLC, Case No. 3:16-cv-02233, in the U.S. District Court for the Northern District of California. Referred to as the ADT Hacking Vulnerability Class Action Lawsuit, ADT will pay $16 million to settle five hacking vulnerability class actions because of claims that ADT's wireless security systems were vulnerable to hacking because ADT failed to include any encryption within them.

Failing To Implement Good Cybersecurity Practices

"This settlement comes on top of the U.S. Federal Trade Commission, through court actions, holding Wyndham Worldwide, a hotel chain, and D-Link, a wireless router and IP camera

manufacturer, responsible for failing to implement good cybersecurity practices," emphasizes Scott Lindley, Farpointe Data president. *"It's become very clear. If you are involved in any type of security, including electronic access control equipment, you can be liable if you don't provide adequate cybersecurity safeguards. That includes encryption which is readily available."*

According to Lindley, *"All modern contactless smart card credentials support cryptography but legacy credential technology may not. Look for terms such as 3DES, AES (which the government uses to protect classified information), TEA and RSA."*

Secure Smart Credentials

Security professionals should always consider more secure 13.56 MHz smart credentials over 125 KHz proximity cards. "Mifare," a technology from NXP Semiconductors, is a leading brand of contactless smart IC. The newest Mifare standard, DESFire EV1, includes a cryptographic module on the card, adding an additional layer of encryption to the card/reader transaction. DESFire EV1 protection is especially important for customers wanting to use secure multi-application cards for access management, public transportation, or closed-loop e-payment.

Another valuable option is Valid ID, an anti-tamper feature for contactless smartcard readers, cards, and tags. Embedded, it adds yet an additional layer of authentication and integrity assurance to traditional Mifare smartcards. Valid ID helps verify that sensitive access data programmed to a card or tag is indeed genuine and not counterfeit.

"Whether you need to guard against state sponsored terrorists or the neighborhood teen from hacking the electronic access control systems that you implement and use, security today starts with encryption," warns Lindley. *"But, that's just a beginning. To take steps that will further hinder hackers, ask for your manufacturer's Cybersecurity Vulnerability Checklist."*

You may also be interested in...

Farpointe Data Urges Channel Partners To Add Anti-hacking Measures To...

Wiegand over-the-air protocol is no longer secure due to its original obscure and non-standard nature Farpointe Data, the...

Farpointe Data Releases First RFID Cybersecurity Vulnerability Checkli...

Farpointe Data, the access control industry's trusted global partner for RFID solutions, has just posted the first radio frequency identific...