Icon Labs Announces the Smart Home Security White Paper

Security for the Smart Home – Who is Responsible?

WEST DES MOINES, IOWA, UNITED STATES, September 24, 2013 /EINPresswire.com/ -- Icon Labs Announces the Availability of the Smart Home Security White Paper

Icon Labs provides security for the smart home and the internet of things

Security for the Smart Home – Who is Responsible?

West Des Moines IA, Sept. 24, 2013

Icon Labs (http://www.iconlabs.com), a leading provider of embedded networking and security technology, today announced the availability of a new white paper – "Security for the Smart Home – Who is Responsible?"

As smart home technology moves from the lab to the marketplace, home security, surveillance and control functions will now be exposed to the Internet through Smart Home gateways and management systems. Are these systems really ready for the cyber-attacks that will undoubtedly ensue? And who is responsible for ensuring these devices are safe from attack?

Security is clearly a requirement for the smart home. The smart home may now include home video surveillance systems, home security systems and door locks that can be accessed remotely, and these systems must be protected from hackers.

Since the homeowner who is using smart home devices cannot install security software onto the device, the responsibility for security falls squarely onto the shoulders of the OEMs who build the device. Security for embedded devices has to be built into the device itself. All too often though, OEMs push off the responsibility for the security of the device to the operating system running on the device. They argue that the OS is responsible for the security of the device. Or even worse, that security is either not a requirement or provides no competitive advantage and therefore can be ignored.

So who is really responsible? Download and read this white paper at http://www.iconlabs.com/security-for-the-smart-home-whitepaper/

“The only way to ensure smart home security is through the coordinated effort of everyone involved in the development and use of the product,” says Alan Grau, President of Icon Labs. “By starting with base security within the essential components of the device, each additional layer of manufacturer, integrator and user can build upon it and makes it less likely that someone – the end user or the network provider – will accidentally leave open the door to attack.”

The new Icon Labs Floodgate at Home solution protects home premises equipment against the growing number of Internet-based attacks. By stopping communication from unapproved devices, Floodgate at Home blocks unauthorized access, protects against automated hacking drones, and can even prevent the device from being discovered by hackers.

About Icon Laboratories, Inc.

Icon Labs is a leading provider of embedded software for device security, device protection and networking management, including the award winning Floodgate Defender. Founded in 1992, Icon Labs is headquartered in West Des Moines, Iowa. For more information, visit www.iconlabs.com, send email to info@iconlabs.com, or call 1.888.235.3443 (U.S. and Canada) or 515.226.3443 (International).

Mark Shapiro
SRS Tech PR
619 249 7742
email us here
