Geofencing could add security layer for mobile devices

Maria Korolov

Mar 3, 2015 4:00 AM PT

Geofencing technology -- tracking the location of a mobile device -- could offer an extra layer of security for enterprises trying to manage both company-owned and employee-owned devices. However, the technology can also raise worries about privacy and battery life.

Extra layer of security

Last fall, Romania-based CoSoSys Ltd. added geofencing to its mobile device management software, tracking location via GPS, Wifi and Bluetooth beacons.

But the first major use of the technology wasn't for companies tracking employees -- but for companies tracking visitors.

CoSoSys has customers in the high-tech industry who want to ensure that visitors can't take pictures when they enter particular secured areas. Typically, they ask visitors to leave their mobile devices at the door, to put tape over the camera lenses.

"Or visitors can agree to have a client installed that will make sure that those features are disabled based on the geofence," said CoSoSys founder and CEO Roman Foeckl.

This is particularly useful for frequent visitors, such as contractors, he said.

The system works because it doesn't just rely on the GPS location, but also uses local beacons to get a very precise idea of where the device is located.

A similar approach could work in Wall Street firms where a Chinese firewall is supposed to be in place between certain departments. The CoSoSys geofencing technology can tell which part of a building the employee is in.

"Is there certain data that is not supposed to be accessed on the device while they have the possibility to meet people from other areas?" he asked.

This is not currently a regulatory requirement, he added, but might soon become one as the technology becomes more commonly available.

A more common application is to use geofencing to control access.

"For example, it can be used to whitelist locations that authorized devices can be used from," said Talbot Harty, CEO at Fremont, Calif.-based DeviceAuthority, Inc. "We have a few government agency projects underway which use this capability."

Harty added that geo-fencing can be combined with other security elements, such as timing, to enforce more granular security restrictions.

For example, a device might be allowed to access an application only from a particular location, and only during working hours.

Companies that use tablets to hold sensitive information could also benefit. Say, for example, a company could use tablets to hold inventory data in a warehouse.

"Geofencing can be used to 'brick' a device if it leaves the premises," said David Goldschlag, SVP of Strategy at San Jose, Calif.-based Pulse Secure, LLC.

The convenience factor

Beyond restricting -- or allowing -- access, geofencing also offers the potential for some convenient, time-saving functionality.

"Employees could use location functionality to access client data for a client whom they are about to visit," said Philip Casesa, director of IT at Clearwater, Florida-based International Information Systems Security Certification Consortium. "Or they could be automatically connected to the corporate LAN when in proximity of a company facility."

And location tracking could also be useful if there was an emergency, and life-saving services needed to be dispatched to the employee's location, he added.

Geofencing could also be useful for corporate board meetings, said Brian Cleary, chief strategy officer at Boston-based bigtincan, a mobile content management company.

"Presentations or sensitive documents can be shared as board members walk into the meeting room, and then once they leave the designated perimeters, those materials can be removed from the device," he said.