PHYS ORG

Location spoofing possible with WiFi devices

April 14 2008

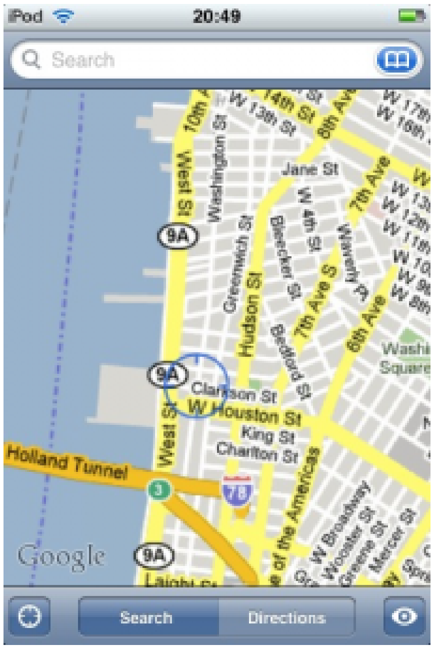

Image credit: ETH Zurich

Apple iPhone and iPod (touch) support a new self-localization feature that uses known locations of wireless access points as well as the device's own ability to detect access points. Now ETH Zurich researchers have demonstrated that positions displayed by the devices using this system can be falsified, making the use of this self-localization system unsuitable in a number of security- and safety-critical applications.

In January, Skyhook Wireless Inc. announced that Apple would use Skyhook’s WiFi Positioning System (WPS) for its popular Map applications. The WPS database contains information on access points throughout the world. Skyhook itself provides most of the data in the database, with users contributing via direct entries to the database, and requests for localization.

ETH Zurich Professor Srdjan Capkun of the Department of Computer Science and his team of researchers analysed the security of Skyhook's positioning system. The team's results demonstrate the vulnerability of Skyhook's and similar public WLAN positioning systems to location spoofing attacks.

When an Apple iPod or iPhone wants to find its position, it detects its neighbouring access points, and sends this information to Skyhook servers. The servers then return the access point locations to the device. Based on this data, the device computes its location. To attack this localization process, Professor Capkun's team decided to use a dual approach. First, access points from a known remote location were impersonated. Second, signals sent by access points in the vicinity were eliminated by jamming. These actions created the illusion in localized devices that their locations were different from their actual physical locations.

Skyhook's WPS works by requiring a device to report the Media Access Control (MAC) addresses that it detects. However, since MAC addresses can be forged by rogue access points, they can be easily impersonated. Furthermore, access point signals can be jammed and signals from access points in the vicinity of the device can thus be eliminated. These two actions make location spoofing attacks possible.

Professor Capkun explained that by demonstrating these attacks, the team hoped to point out the limitations, despite guarantees, of public WLAN-based localization services as well as of applications for such services. He said: "Given the relative simplicity of the performed attacks, it is clear that the use of WLAN-based public localization systems, such as Skyhook’s WPS, should be restricted in security and safety-critical applications."

See more details at: www.syssec.ch/press/location-s … -the-iphone-and-ipod

Source: ETH Zurich

Citation: Location spoofing possible with WiFi devices (2008, April 14) retrieved 25 April 2024 from https://phys.org/news/2008-04-spoofing-wifi-devices.html