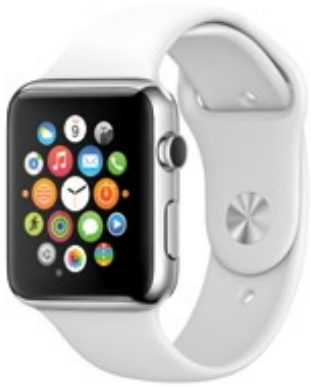
SPOTLIGHT ON SECURITYHow Secure Is the Apple Watch?



Apple Watch applications themselves could be a potential source of security problems. "The introduction of new app marketplaces presents an opportunity for scammers to ride the wave of excitement to peddle new malicious apps, craft lures related to the new service, and jump on consumer curiosity and lack of knowledge about the legitimate system," said Websense security analyst Carl Leonard.

By John P. Mello Jr.
03/19/15 4:31 PM PT

Apple typically has impeccable timing for its new product introductions, but that may not be the case with its new smartwatch.

In a gala event last week, the company announced model and pricing details for its Apple Watch. That came just six days after questions were raised about the security of its mobile payment platform. Those questions haven't gone away, and now they're also being asked about Apple's smartwatch.

Wearable computing devices like the Apple Watch are still new territory for cybercriminals, but as more of these gadgets hit the market, they'll start appearing on the radar of hackers.

That could be very soon, as 2015 is expected to be a watershed year for wearables. Shipments will jump 129 percent from last year to this year, with 43.2 million units expected to enter the market, Canalys predicted.

While Apple is keeping the nitty-gritty of its watch's security close to its vest, it is touting a unique skin sensor that provides a measure of security for the device.

"When you take off or put on the watch, you're required to enter a PIN, so there's some capacity there for multifactor authentication," said Steve Pao, general manager for security business at Barracuda Networks.

Jailbreaking the Apple Watch

An obvious point of attack on the watch is its wireless connection to an iPhone. That can be addressed without too much trouble, though.

"It can be mitigated to a large degree by putting application security measures on top of what the communication protocol security provides," Pao told TechNewsWorld. "It wouldn't be a tremendous burden to do that."

The Apple Watch applications themselves could be a potential source of security problems, noted Carl Leonard, principal security analyst at Websense.

"One thing to keep in mind is that the Apple Watch will pair with your iPhone to get new apps," he told TechNewsWorld.

"The introduction of new app marketplaces presents an opportunity for scammers to ride the wave of excitement tc peddle new malicious apps, craft lures related to the new service, and jump on consumer curiosity and lack of knowledge about the legitimate system," Leonard said.

New users should be watchful for malicious apps and only use reputable apps from the marketplace," he added.

Since the new watch and the iPhone are connected at the hip, the Apple Watch benefits from the strong security found in iOS, Apple's mobile operating system. However, users have been known to jailbreak Apple devices and disable the protections provided by iOS.

If that's done, Pao noted, "just as when you hack your iPhone, all bets are off."

Building a Geofence

Most security experts advocate using layers of defense to protect an organization's data. Firewalls can protect the perimeter, but additional defenses need to be in place to thwart threats that make it through the perimeter, and to squash threats originating from within an organization. Geofencing can be one of those additional layers.

Geofencing can add more context to the rights and privileges of users within an organization. For instance, if electronic patient records are limited to a department in a hospital, then an alert can be sent to the custodians of the records if someone should try to move them outside the designated area on a mobile device.

"Geofencing can complement security measures that are already in place," explained Roman Foeckl, CEO and founder of CoSoSys. "It will not replace them and take over as the primary driver of security."

With geofencing, rights and privileges can be assigned to a device based on where it is in a building or campus -- just as they can be assigned based on a person's official capacity within an organization.

"The device itself becomes aware of how it should behave if it's in or out of a geofenced area," Foeckl said.

Geofencing presently is most popular with forward-thinking companies that are concerned about protecting their intellectual property, but the market may expand in the future, he noted.

"Over the next few rears," Foeckl noted, "it could become a compliance requirement."

Breach Diary

- March 9. Nextep Systems, a vendor of point-of-sale solutions for restaurants, corporate cafeterias, casinos, airports and other food service venues, confirms it has been notified by law enforcement that some of its customer locations have been compromised.
- March 10. ACLU files lawsuit seeking to stop NSA's mass interception and search of Americans' Internet communications.
- March 10. Eleven suspects from the Detroit area indicted for stealing information from 5,514 Blue Cross Blue Shield of Michigan customers and using it to make fraudulent purchases around the nation.
- March 11. University of Pittsburgh Medical Center notifies employees that their federal income tax refunds will be delayed due to data breach last year in which personal information for some 62,000 workers was compromised by identity thieves.
- March 11. Indiana State Medical Association warns 39,090 clients that their private data may be at risk following "random" theft of a pair of backup hard drives being transported to an offsite storage location in February.
- March 12. U.S. Senate Intelligence committee approves the Cybersecurity Information Sharing Act, which expands liability protections for companies sharing information with the federal government.
- March 12. Reps. Peter Welch, D-Vt., and Marsha Blackburn, R-Tenn., introduce the Data Security and Breach Notification Act. A hearing on the bill before the House Energy committee is scheduled for March 18.
- March 12. Cisco's Talos Security Intelligence and Research Group reveals a bug in Google Apps has resulted in leakage of hidden whois data attached to more than 282,000 domains registered with the service over a two year period.

Upcoming Security Events

- March 20-21. B-Sides Salt Lake City. Sheraton Salt Lake City Hotel, Salt Lake City, Utah. Registration: before March 20, US$40; $50 at the door.

- March 24-27. Black Hat Asia 2015. Marina Bay Sands, Singapore. Registration: before Jan. 24, $999; before March 21, $1,200; after March 20, $1,400.
- April 1. SecureWorld Kansas City. Kansas City Convention Center, 301 West 13th Street #100, Kansas City, Missouri. Registration: open sessions pass, $25; conference pass, $75; SecureWorld plus training, $545.
- April 20-24. RSA USA 2015. Moscone Center, San Francisco. Registration: before March 21, $1,895; after March 20, $2,295; after April 17, $2,595.
- May 6-7. Suits and Spooks London. techUK, 10 Saint Bride St., London. Registration: government/military, $305; members, $486; industry, $571.
- June 8-10. SIA Government summit 2015. W Hotel, Washington, D.C. Meeting Fees: members, $595; nonmember, $795.
- June 8-11. Gartner Security & Risk Management Summit. Gaylord National, 201 Waterfront St., National Harbor, Maryland. Registration: before April 11, $2,795; after April 10, standard $2,995, public sector $2,595.
- June 16-17. Black Hat Mobile Security Summit. ExCel London, London, UK. Registration: before April 11, Pounds 400; before June 16, Pounds 500; after June 15, pounds 600.
- August 1-6. Black Hat USA. Mandalay Bay, Las Vegas, Nevada. Registration: before June 6, $1,795; before July 25, $2,195; after July 24, $2,595.

ECT

John Mello is a freelance technology writer and contributor to *Chief Security Officer* magazine. You can connect with him on Google+.