IBM Hosted Vulnerability Management Service
Get a free security scan for your company.
Try VMS now
replay

Tweet 100 Like 8 Share 4 Permalink

Security Fail: Apple iOS Password Managers

Claims of military-grade encryption on smartphones are vastly overstated by almost every maker of Apple iOS password safes, say researchers at Black Hat Europe.

By **Mathew J. Schwartz** InformationWeek
March 16, 2012 11:01 AM

To riff on the old Steve Martin joke about cats: Do you have a password manager on your mobile device? Do you trust it?

Anonymous: 10 Facts About The Hacktivist Group

(click image for larger view and for slideshow)

If so, that trust may be misplaced. Speaking Friday at Black Hat Europe in Amsterdam, two security researchers from Elcomsoft detailed a study they'd conducted of 13 Apple iOS password managers (a.k.a. password keepers, wallets, or safes). Only one of the tested products, however, had properly implemented strong crypto.

"Most people who develop password keepers, I believe they're very good programmers, but they need to study security," said Elcomsoft's Dmitry Sklyarov.

The sole exception they found in testing a sample of popular apps was Strip Lite, a free password manager from Zetetic. Strip Lite computes an encryption key using 4,000 iterations of PBKDF2-SHA1, together with a per-database salt (random bits). All this makes it very difficult to crack the password it generates, which means that the app does a good job of securing passwords.

[The mobile ecosystem has a lot of growing up to do. Read more at Mobile's Cryptography Conundrums.]

Elcomsoft's Andrey Belenko also said that a $10 product they tested called mSecure "seems not bad," in part because of its use of Blowfish encryption.

The researchers studied a total of seven free applications and six paid ones. On the free front, Sklyarov dubbed three of the apps–iSecure Lite Password Manager, Secret Folder Lite, and Ultimate Password Manager Free–as the "unsafe triplets." All three use the exact same underlying software code but have a different name and graphical user interface, and all store their master passwords in unencrypted form on the device, which makes retrieving the password a trivial matter. Other free applications studied were Keeper Password & Data Vault (from Callpod), My Eyes Only–Secure Password Manager (Software Ops), Password Safe–iPassSafe free version (from Netanel Software), and Zetetic's Strip Lite.

For paid applications, the researchers Googled "top password keepers for iOS" and picked six that looked popular: 1Password Pro (Agilebits, $15), DataVault Password Manager (Ascendo, $10), LastPass for Premium Customers ($1/month), mSecure Password Manager (mSeven Software, $10), SafeWallet–Password Manager (SBSH Mobile Software, $4), and SplashID Safe for iPhone (SplashData, $10).

More Security Insights

Webcasts
- Exposing the Money Behind Malware
- Is Your Vulnerability Management Program Irrelevant? Recommended Steps To Turn Vulnerability Management Into An Effective and Necessary Part of Your Security Process.

More >>

White Papers
- 5 Things You Need to Know About BYOD
- Fighting Fraud with IP Geolocation

More >>

Reports
- Research: State of the IT Service Desk
- Database Defenses

More >>

Get InformationWeek Daily

Don't miss each day's hottest technology news, sent directly to your inbox, including occasional breaking news alerts.

RELATED WEBCASTS

What's this?

- Exposing the Money Behind Malware
- Is Your Vulnerability Management Program Irrelevant? Recommended Steps To Turn Vulnerability Management Into An Effective and Necessary Part of Your Security Process.
- The IBM End-to-End Mainframe Security Solution Overview

More >>

THIS WEEK'S ISSUE

- Subscribe to InformationWeek
- Subscribe to Digital
- Read the Cover Story
- Download This Issue

Back Issues

The researchers began their testing project after a British law enforcement agency asked Elcomsoft how hard it would be to crack a SplashID database password, which the agency had encountered during an investigation. SplashID Safe for iPhone appears to be one of the three most popular password safes for the iPhone, with about a half million users.

On the positive side, the researchers found that SplashID Safe uses Blowfish, for which password experts have spent less time developing cracking tools. On the negative side, SplashID Safe uses a hard-coded key to encrypt a user's master password, thus making that master password instantly recoverable to anyone who can access the device and get past the iOS passcode entry requirement (if it's been enabled). In other words, the software may store passwords, but it effectively fails to secure them.

Based on their research, in fact, the researchers said that the single best way to secure passwords or any other data on an iOS device is to enable the iOS security feature that requires a passcode to be entered to unlock the device. "Always use a passcode for iOS devices, and use something more complex than the standard four-digit passcode, because ... a four-digit passcode can be brute-forced in less than two hours for any device before the iPhone 4S," said Belenko.

The security situation improved with the iPhone 4S, the iPad 2, and the new iPad, because all password-cracking attempts must be done on the device itself. This greatly slows attackers because "there are no publicly available exploits that can be utilized to recover the passcode," according to Belenko. (For older devices, the iOS passcode hash can be recovered, transferred to another computer, and then subjected to a brute-force attack.) "Of course, do not jailbreak the device, because you're making the ecosystem more open, but you're also making it more open for bad guys," he said.

That iOS security technique aside, why did so many password safe apps fail at security? For starters, many of the tested products use AES encryption, and password researchers have created AES-cracking tools optimized for the ultra-fast graphics processing unit (GPU) now built into most computers. Combined with the poor crypto implementations seen in almost every tested product, the use of GPUs allows attackers to–in many cases–test millions of possible passwords per second, and for some password managers up to 20 million passwords per second. For comparison's sake, when attempting to crack passwords for Microsoft Office 2007 documents, attackers can currently test only about 5,000 passwords per second.

Belenko said that he himself had been using 1Password Pro, which may be the most-installed password manager for Apple iOS. But he ceased using it after testing the application's cryptography. "When we recovered my master password in five seconds? That was a moment," he said.

Meanwhile, some password managers encrypt passwords by using the cryptographic hash function MD5. Callpod's Keeper Password & Data Vault, for example, claims to have "military-grade encryption"–thanks to MD5–which it says means that "you can trust that no one else will have access to your most important information." Except that MD5 must be used properly, since researchers have devoted extensive resources to defeating it. "MD5 is like a platform for testing skills on GPU acceleration," said Sklyarov.

For Keeper Password, however, GPU cracking isn't even required, since the product fails to salt its MD5 passwords. That means that an attacker could simply reference rainbow tables–lists of the password equivalent for any given hexadecimal hash–which are freely available on the Internet. "Type the hexadecimal hash in Google, and in many cases you will find the password value in less than a second," said Skylarov.

The same weak crypto that makes it easy to test millions of possible passwords per second also means that users would need relatively long passwords–typically, 14 characters or more in length–if they want to make their password uncrackable by an attacker in less than 24 hours. Of course, almost no one will use a password of that length, given the usability challenge of reliably entering so many characters via a touch screen. As a result, most real-world password safe master passwords are relatively easy to crack.

In response to a question from the Black Hat audience about whether these password manager cryptography problems had been shared–per responsible disclosure guidelines–with the relevant developers, the Elcomsoft researchers said they'd declined to notify vendors. "We don't think this will provide any benefit because this isn't a bug, this is architecture," said Belenko.

In other words, the applications don't have code-level errors that can be patched. Rather, most of their developers appear to have failed to understand how to properly implement cryptographic features. "It's very bad for the industry: security that doesn't provide security isn't a very good thing," Belenko said. "If you don't really need the password manager, we'd probably recommend that you don't use it."

InformationWeek is conducting a survey to determine the types of measures and policies IT is taking to ensure the security of the full range of mobile assets on cellular, Wi-Fi, and other wireless technologies. Upon completion of our survey, you will be eligible to enter a drawing to receive an 32-GB Apple iPod Touch. Take our Mobile Security Survey now. Survey ends March 16.

4 **Comments, join the conversation**

Related Reading

News

Commentary

Second LulzSec Sony Hacker Suspect Arrested

6 Password Security Essentials For Developers

SPECIAL ISSUE

- **Subscribe to InformationWeek**
- **Subscribe to Digital**
- **Read the Cover Story**
- **Download This Issue**

Back Issues

RELATED WHITEPAPERS

What's this?

- 5 Things You Need to Know About BYOD
- Advanced Threat Report: What You Need to Know About the Latest Cyber Attacks and How to Protect Your Organization
- Software-Based Authentication Delivers More Reliable and Less Costly Security

More >>

FEATURED RESOURCES

Complimentary Dummies Books

- IT Availability & Performance Monitoring
- Data Deduplication
- VM Data Protection
- BPM
- Private cloud
- Systems Engineering for Dummies

RELATED REPORTS

What's this?

- Research: State of the IT Service Desk
- Will IPv6 Make Us Unsafe?
- Database Defenses

More >>

VIDEO

WATCH: 5 Elevator Pitches,

WATCH: The Most Interesting IT Guy In The

WATCH: What Not To Do To Prevent Ending

MobileIron Distributes Enterprise Apps, Simplifies Android

Mobile's Cryptography Conundrums

More News»

Most Popular

On the Web

5 Dropbox Security Warnings For Businesses

Getting Started With Full Disk Encryption

How Anonymous Are Your Online Posts?

New Protocols Secure Layer 2

More Popular»

Slideshow

Video

Secret Spy Satellite Takes Off: Stunning Images

12 Epic Tech Fails Of 2011

InformationWeek Analytics Presents: The Best of Interop 2011

15 Budget Busting Technology Projects

More Slideshows»

NetSuite CEO Hit Val ... World ... Up In B ...

View All Videos

Like

Login or Register to Comment

Real-time updating is **paused**. (Resume)

Showing 4 comments

Sort by oldest first

clurey606

The app developers should have been contacted prior to the release of this document. There are many statements here which are not accurate and oversimplified.

3 months ago Permalink Flag as inappropriate Like Reply

Khad Young I work for AgileBits, and I love you.

I though it may be prudent to post the email that we sent Matthew earlier which includes a link to our response for the benefit of those following along at home.

—

Hi Matthew, it's good to see tech publications bringing up the topic of security in the mobile space. It's a tough nut to crack in some key ways.

We read your piece and our co-founder wrote a response about how we approach some of these issues as well as some of our plans for updates in the future, including 1Password 4. Could you take a look and let me know if you have any questions?

http://blog.agilebits.com/2012...

I think some of our comments here could serve as a response to some of the issues brought up by Elcomsoft's white paper, but please let me know if you have any questions you would like to ask me or others at AgileBits. We're here to listen and help.

Thanks again, Matthew.

—
Khad Young
Forum Choreographer, AgileBits
http://agilebits.com/support

3 months ago Permalink Flag as inappropriate Like Reply

Stephen Lombardo

I'm one of the developers of STRIP, the password manager that was favorably reviewed by the presenters. This paper was especially important because it exposed a range of serious issues, from apps that don't even encrypt data, to real flaws in crypto implementations. These findings have sparked a lot of interest in STRIP because of it's resilience to password cracking (we've released converters from other less-secure programs, like SplashID : http://getstrip.com/switch).

That said, the premise holds that, regardless of the application used, numeric PIN numbers are not safe. The choice of password is thus very important and a key factor in the overall security of any encryption system, and there just isn't enough entropy in a numeric passcode to render brute force attacks infeasible. With a fast GPU an 8 digit numeric PIN could take a few hours to crack, yet an 8 character random alphanumeric password with meta-characters would take thousands of years.

3 months ago Permalink Flag as inappropriate Like Reply

AmazonMAL

Hello, I am not a security expert, just have a question. Keeper is updating to version 5 soon and they say "We are increasing the encryption levels of the master password and data storage to add additional protection for our users. For those of you who are technically savvy, all password hashes will be encoded with BCrypt, supported with 128-bit AES for all symmetric ciphers."
Will this make the product more secure? Using on device with IOS pass codes.

4 months ago Permalink Flag as inappropriate Like Reply

Subscribe by email RSS

XML Subscribe to RSS

RESOURCE LINKS

How To Architect, Deploy And Manage Your Storage Infrastructure
Cloud Connect ? Cloud technologies, platforms and opportunities
Get Today's Hottest Tech News, Direct To Inbox - Subscribe now!
No Jitter – Daily blogging and analysis of enterprise IP-telephony
Click here for a whitepaper on Information Security
Get Expert Coverage Of Consumer Tech In Business On BYTE
Government IT Intelligence, Direct To Your Inbox - Subscribe Now!
Healthcare IT Intelligence, Direct To Your Inbox - Subscribe Now!
Premier Research App For IT Pros - TechWeb Digital Library
Register Today For The Most Timely Security Insights

Live National Broadcast & Lunch Event – October 9, 2012
Expert IT: Accelerate Big Data and Cloud with Expert Integrated Systems
InformationWeek events

UBM TechWeb

Enabling People and Organizations to Harness the Transformative Power of Technology

CIOs & IT Professionals
Black Hat
BYTE
Cloud Connect
Dark Reading
Enterprise 2.0
Enterprise Connect
Enterprise Efficiency
HDI
InformationWeek
InformationWeek 500
InformationWeek 500 Conference
InformationWeek Events
InformationWeek Global CIO
InformationWeek Healthcare
InformationWeek India
InformationWeek Reports
InformationWeek SMB

Software Developers
Dr. Dobb's
Dr. Dobb's M-Dev
Dr. Dobb's Journal
Dr. Dobb's Update
TechWeb.com

Web & Digital Professionals
Internet Evolution
Online Marketing Summit
TechWeb.com

Government Officials
GTEC Ottawa
InformationWeek Government
TechWeb.com

Vertical Markets
Advanced Trading
Bank Systems & Technology
CreateYourNextCustomer
InformationWeek Government
InformationWeek Healthcare
Insurance & Technology
Light Reading / Telecom
The CMO Site
Wall Street & Technology

Game Industry Professionals
Gamasutra.com
Game Developers Conference (GDC)
Independent Games Festival
Game Developer Magazine
GDC Europe
GDC China

Global Communications Service Providers
4G World
Heavy Reading
Heavy Reading Insiders
Pyramid Research
Light Reading
Light Reading India
Light Reading Mobile
Light Reading Cable
Light Reading Europe
Light Reading Asia
Ethernet Expo
TelcoTV
Tower Summit
Light Reading Live & Virtual Events
Webinars

Most Popular
Cable Catchup
Cloud Connect Blog
Digital Life
Evil Bytes
InformationWeek Reports
Interop Blog
Monkey Bidness
Over the Air
Personal Tech
The Philter
Valley Wonk

Interop
Mobile Connect
Netw ork Computing
No Jitter
TechWeb.com
The BrainYard

Game Career Guide
Game Advertising Online

UBM TechWeb Reader Services

About UBM TechWeb Advertising Contacts Technology Marketing Solutions Contact Us Feedback

Reprints TechWeb Digital Library / White Papers TechWeb Events Calendar TechWeb.com

Terms of Service | Privacy Statement | Copyright © 2012 UBM TechWeb, All rights reserved.

InformationWeek Home News Commentary Video Slideshows Software Security Cloud Mobility Social Business
Personal Tech Hardware Windows Global CIO Government Healthcare Financial SMB

About Us Contact Us Customer Support Current Issue Back Issues Site Map Reprints Editorial Calendar