ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Analyzes 17 Smartphones' Secure Password Managers, Finds No Security

ElcomSoft Co. Ltd. analyzed 17 popular password management apps available for Apple iOS and BlackBerry platforms, including free and commercially available tools, and discovered that no single password keeper app provides a claimed level of protection. None of the password keepers except one are utilizing iOS or BlackBerry existing security model, relying on their own implementation of data encryption. ElcomSoft research shows that those implementations fail to provide an adequate level of protection, allowing an attacker to recover encrypted information in less than a day if user-selectable Master Password is 10 to 14 digits long.

Finally, 7 out of 17 products store users' passwords unencrypted or encrypted so poorly that they can be recovered instantly. "*Using the right encryption algorithm is not enough*", says Andrey Belenko, ElcomSoft Chief Security Researcher. "*It only takes one weak link to ruin the entire security model. Some of the tools would have a better chance to pass our security test if they were about 10,000 to 20,000 times more secure in terms of password recovery speed. Some other tools are completely hopeless and should be avoided at all costs*."

"*Our research proved once again that IT security requires more than just programming skills*", comments Dmitry Sklyarov, ElcomSoft IT Security Analyst. "*With open-source strong-crypto libraries everyone and their dog can write a password keeper, claiming their product offering secure protection – which is not really the case. A good security model takes the whole system into account including the user himself – and not just the strength of the encryption algorithm alone*".

Background

Passwords should be long and complex. The same password should not be used for different services, no matter how complex that password might be. Those are valid requirements often demanded by corporate security policies. However, these requirements create a challenge of remembering dozens of complex passwords, something an average human being is not very good at.

Password keepers, or password management apps, are applications designed to facilitate storing and management of passwords on mobile platforms such as Apple iOS and BlackBerry. Password keepers are a matter of convenience, offering a centralized storage and quick access to all user's passwords and pieces of sensitive information such as credit card data. Typically, access to user's passwords is protected with a single master password.

© 2012 ElcomSoft Co. Ltd.

Microsoft Partner
Gold Independent Software Vendor (ISV)

intel Software Partner

In an ideal world, password keepers would provide cryptographically strong, difficult to break protection of sensitive information against unauthorized access. They would utilize each platform's security model, building an extra layer of protection on top of it to safeguard what's considered to be the most sensitive bits of information. Indeed, most password keepers, especially those provided by BlackBerry themselves, claim a high level of security citing the use of industry-standard encryption algorithms such as AES-256 or Blowfish.

Since the apps are entrusted with sensitive data, the questions arise about how secure they really are. The research analyzed whether password managing applications are utilizing security mechanisms provided by mobile OS and whether they add any additional security on top of that by performing an in-depth analysis of as many as 17 popular password keepers.

The Research

Both platforms being analyzed, BlackBerry and Apple iOS, feature comprehensive data security mechanisms built-in. Exact level of security varies depending on which version of Apple iOS is used or how BlackBerry users treat memory card encryption. However, in general, the level of protection provided by each respective platform is adequate if users follow general precautions.

The same cannot be said about most password management apps ElcomSoft analyzed. Only one password management app for the iOS platform, DataVault Password Manager, stores passwords in secure iOS-encrypted keychain. This level of protection is good enough by itself; however, that app provides little extra protection above iOS default levels. Skipping the complex math (which is available in the original whitepaper), information stored in 10 out of 17 password keepers can be recovered in a day – guaranteed if user-selectable master password is 10 to 14 digits long, depending on application. What about the other seven keepers? Passwords stored in them can be recovered instantly because passwords are either stored unencrypted, are encrypted with a fixed password, or are simply misusing cryptography.

Interestingly, BlackBerry Password Keeper and Wallet 1.0 and 1.2 offer very little protection on top of BlackBerry device password. Once the device password is known, master password(s) for Wallet and/or Password Keeper can be recovered with relative ease.

Recommendations

Many password management apps offered on the market do not provide adequate level of security. ElcomSoft strongly encourages users not to rely on their advertised security, but rather use iOS or BlackBerry built-in security features.

In order to keep their data safe, Apple users should set up a passcode and a really complex backup password. The unlocked device should not be plugged to non-trusted computers to prevent creation of pairing. Unencrypted backups should not be created.

BlackBerry users should set up a device password and make sure media card encryption is off or set to "Encrypt using Device Key" or "Encrypt using Device Key and Device Password" in order to prevent attackers from recovering device password based on what's stored on the media card. Unencrypted device backups should not be created.

The full whitepaper is available at http://www.elcomsoft.com/download/BH-EU-2012-WP.pdf

About ElcomSoft Co. Ltd.

Established in 1990, ElcomSoft Co.Ltd. is a global industry-acknowledged expert in computer and mobile forensics. The company provides tools, training, and consulting services to law enforcement, forensics, financial and intelligence agencies. ElcomSoft pioneered and patented numerous cryptography techniques, setting and exceeding expectations by consistently breaking the industry's performance records. ElcomSoft is Microsoft Gold Independent Software Vendor, Intel Software Premier Elite Partner, member of Russian Cryptology Association (RCA) and Computer Security Institute.

© 2012 ElcomSoft Co. Ltd.