Canon Original Data Security System Compromised: ElcomSoft Discovers Vulnerability

Moscow, Russia – November 30, 2010 - ElcomSoft Co. Ltd. has discovered vulnerability in Canon Original Data Security, a verification system to provide image data verification features intended to authenticate image originality. The vulnerability allows extracting the original signing key from a Canon digital camera and using the key to put an authenticity signature to a photo or any digital image, which will be validated as an original and authentic.

The vulnerability discovered by ElcomSoft questions the authenticity of all Canon signed photographic evidence and published photos, and effectively proves the entire Canon Original Data Security system useless.

Background

Canon Inc. introduced its Original Data Security system as means to securely verify credibility of image data and prove image originality. A supported Canon digital SLR signs pictures taken with the camera with a secure digital signature. Image verification data becomes embedded in every image shot with the camera, allowing to verify the authenticity and originality of an image with utmost accuracy. Unfortunately, this is not the case, according to recent findings by ElcomSoft, a leading information security company.

The Original Data Security system was intended to ensure that images, taken with a compatible Canon camera, are unaltered in any way and contain the original valid GPS data. The system was designed to prove image originality as well as time and place of the capture. The intent of the system was to protect the integrity of images shot as evidence. According to Canon official announcement, the credibility of photographic evidence is directly linked to its legitimacy when making legal decisions. The Canon data security system is being used by world leading news agencies including Associated Press as effective means to ensure that each agency's photo manipulation policies are enforced.

Today, ElcomSoft has proven the system to be far from bullet-proof. The company was able to extract signing keys from Canon digital cameras, use the keys to sign an altered image and successfully validate fake photos with Canon Original Data Security Kit (OSK-E3).

"The entire image verification system is proved useless", says ElcomSoft CEO Vladimir Katalov. "*It is hard to underestimate the significance of our discovery. The authenticity guarantee advertised by Canon data security system is truly worthless. If one company was able to produce fake images indistinguishable from originals, how do we know that others haven't been doing this for years? ElcomSoft demonstrated that any photographic evidence authenticated by the Canon system is just as insecure as pictures not secured by the system."*

ElcomSoft has published a series of manipulated images that will successfully validate with Canon Original Data Security Kit (http://www.canon.co.jp/imaging/osk/osk-e3/index.html). The images are available at http://canon.elcomsoft.com/.

About ElcomSoft Co.Ltd.

Founded in 1990, ElcomSoft Co.Ltd. develops state-of-the-art computer forensics tools, provides computer forensics training and computer evidence consulting services. Since 1997, ElcomSoft has been providing support to businesses, law enforcement, military, and intelligence agencies. ElcomSoft tools are used by most of the Fortune 500 corporations, multiple branches of the military all over the world, foreign governments, and all major accounting firms. ElcomSoft and its officers are members of the Russian Cryptology Association. ElcomSoft is a Microsoft Gold Certified Partner and an Intel Software Partner. More information at http://www.elcomsoft.com/

ElcomSoft offers a series of manipulated photos that will successfully validate with Canon Original Data Security Kit at http://canon.elcomsoft.com/.