ELCOMSOFT
PROACTIVE SOFTWARE

ElcomSoft Discovers Vulnerability in Nikon's Image Authentication System

Moscow, Russia – April 28, 2011 – ElcomSoft Co. Ltd. researched Nikon's Image Authentication System, a secure suite validating if an image has been altered since capture, and discovered a major vulnerability in the manner the secure image signing key is being handled. In turn, this allowed the company to extract the original signing key from a Nikon camera. The vulnerability, when exploited, makes it possible to produce manipulated images with a fully valid authentication signature. ElcomSoft was able to successfully extract the original image signing key and produce a set of forged images that successfully pass validation with Nikon Image Authentication Software.

ElcomSoft has notified CERT and Nikon about the issue, and prepared a set of digitally manipulated images passing as originals when verified with Nikon's secure authentication software. Nikon has provided no response nor expressed any interest in the existence of the issue.

About Nikon Image Authentication System

Combined with digital signature modules featured in Nikon's top of the line digital SLRs, the purpose of Nikon Image Authentication Software was to enable users determine whether an image has been altered after being shot. By Nikon's claims, the system was to provide proof of image authenticity for the purpose of law enforcement and government agencies, insurance companies, businesses, and news agencies. As demonstrated by ElcomSoft, claims made by two major digital camera vendors, Canon and Nikon, have so far not lived up to the hype.

Background

Credibility of photographic evidence may be extremely important in a variety of situations. Courts, news agencies and insurance companies may accept digitally signed photographs as valid evidence. If such evidence is forged, consequences can be severe. The most famous fakes include cases of fraud committed by enthusiast photographers, photo journalists, editors, political parties, and even the US Army.

To address the issue, major manufacturers of photographic equipment such as Canon and Nikon developed their own proprietary versions of image authentication systems. In 2010, ElcomSoft performed a security analysis of Canon's proprietary image authentication system. Similar to Nikon's, the system was supposed to prove image authenticity in the eyes of the media, law enforcement, government, and business organizations. As demonstrated by ElcomSoft, a major security flaw exists in Canon's implementation, which has not been addressed in any way even today, after half a year after discovery.

Almost half a year later, ElcomSoft has discovered that a similar vulnerability exists in digital SLR cameras manufactured by Nikon. The existence of this vulnerability proves that image authentication data can be forged, and thus Nikon Image Authentication System cannot and shall not be relied upon. As a consequence, successful image verification as reported by Nikon Image Authentication Software cannot be used as a proof of authenticity.

The Issue with Nikon's Security System

When designing a digital security system, it is essential to equally and properly implement all parts of the system. The entire system is only as secure as its weakest link. In the case of Nikon's Image Authentication System, the company has not done at least one thing right. The ultimate vulnerability lies in the way the image signing key is being handled. As the signing cryptographic key is handled inappropriately, it can be extracted from the camera as shown by ElcomSoft researchers. After obtaining the signing key, one can use it to sign any picture, whether or not it's been altered, edited, or even computer-generated. The signed image will then successfully pass as a valid, genuine piece when verified by Nikon Image Authentication Software.

The vulnerability exists in all current Nikon cameras supporting Nikon Image Authentication, including Nikon D3X, D3, D700, D300S, D300, D2Xs, D2X, D2Hs, and D200 digital SLRs.

ElcomSoft will share some technical details on one of the security conferences in near future. Full detail will not be disclosed in the interests of public responsibility. The vendor and CERT Coordination Center have been notified of the issue. While ElcomSoft has contacted most Nikon's branches, including Nikon USA, Nikon Europe and Nikon Japan, the company provided no meaningful response and did not appear concerned about the issue in the least.

ElcomSoft has performed the extraction of the signing key, and, as a proof of concept, prepared a set of forged images that pass as fully genuine. The fakes successfully passing validation with Nikon Image Authentication Software are available at http://nikon.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

Manipulated images successfully passing validation by Nikon Image Authentication Software are available at http://nikon.elcomsoft.com