Yui Kee Computing Ltd.

Newsletter

December 2010

Contents

The Camera Never Lies?

<web-link for this article>

Russian developer of computer forensics tools and services ElcomSoft has announced that it has cracked digital camera manufacturer Canon's image verification scheme.

In the scheme, Canon cameras embed verification data in photos they take, and sign it. The data includes the GPS location, date and time the photo was taken. Anyone can subsequently use Canon's OSK-E3 verification kit to check the signature and therefore prove where and when the photo was taken.

ElcomSoft claims that it has extracted signing keys from Canon digital cameras, used the keys to sign an altered image and successfully validated the fake photo with the OSK-E3. ElcomSoft has posted a selection of amusingly modified photos that they say the OSK-E3 will validate.

The OSK-E3 is available from Amazon for US$658.40, a small price for verifying the location of the USSR's moon landing.

Dmitry Sklyarov of ElcomSoft went into the details of the exploit in his presentation at the CONFidence 2.0 conference on 30th November. He described how he analysed the camera firmware to locate the obfuscated signing key and that the key is the same for all camera of the same model, but different in different models. He can therefore generate verification data for any camera where the key for the model is known. Saying that Canon could do nothing about this flaw for existing models, he recommended that, for future models, Canon should implement the signing calculation in a cryptoprocessor which does not expose the secret key; prevent the camera from running non-Canon's code to avoid illegal usage of the cryptoprocessor; and hire people who really understand security.

Dmitry Sklyarov is previously known for his presentation on Adobe's eBook Security at the DEF CON convention in Las Vegas in 2001, and his subsequent arrest by the FBI for distributing a product designed to circumvent copyright protection measures, under the terms of the Digital Millennium Copyright Act, following a complaint by Adobe. This may be why he chose CONFidence 2.0 in Prague, Czech Republic to present his findings on this occasion.

More Information

Canon Original Data Security System Vulnerability
Forging Canon Original Decision Data
Canon Original Data Security System Compromised: ElcomSoft Discovers Vulnerability
Canon OSK-E3 Original Data Security Kit for the Canon 1D Mark III
OSK-E3 Original Data Security Kit
Cryptographers crack system for verifying digital images

The Professional Commons holds Open Forum on Privacy

<web-link for this article>

The Professional Commons held an Open Forum on "Review of Personal Data (Privacy) Ordinance" on 9th December, with Government and Privacy Commissioner representatives speaking. The ongoing review of the Personal Data (Privacy) Ordinance is a hot topic of public policy in Hong Kong at the moment, and this was a further opportunity for discussion.

Ms Adeline Wong, Under Secretary for Constitutional and Mainland Affairs, HKSAR Government, explained the proposed amendments from her department, and Mr. Henry Chang, Information Technology Advisor and Mr. Wilson Lee, Chief Personal Data Officer, both of the Office of the Privacy Commissioner for Personal Data responded. Mr. Charles Mok, Vice Chairperson of the Professional Commons moderated the event. The discussion was continued by a panel consisting of Mr. Ian Christofis of PISA, Mr. SC Leung of IT Voice and Mr. Allan Dyer, our Chief Consultant, speaking in his personal capacity.

Some of the topics included special provisions regulating Direct Marketing, making disclosure for profit or malicious purposes an offence, whether breach notification should be voluntary or mandatory, regulation of Data Processors, Sensitive Personal Data, a Do Not Call list for Person to Person phonecalls, criminal investigations and source disclosure. Mr. Dyer's speech is included in this newsletter.

The consultation period for the report on the Public Consultation will end on 31st December 2010. There will be another opportunity to question Mr. Henry Tang at a Hong Kong Computer Society event on 13th December.

More Information

Open Forum on "Legislative Proposal of Personal Data (Privacy) Ordinance"
The Professional Commons
Views on the Review of the Personal Data (Privacy) Ordinance
Privacy Laws to be Tightened
A Dialogue on OCT and Personal Data Privacy

Views on the PDPO Legislative Proposal

<web-link for this article>

This is the speech made by Yui Kee Computing Chief Consultant Allan Dyer at the The Professional Commons' Open Forum on Privacy.

I think the biggest issue with this Legislative Proposal is what is left out. I'm talking about the complex relationships between Copyright, Privacy, Obscenity and Free Speech. The Information Age has changed things in ways we do not yet fully understand, and our laws on all of these cannot cope.

For example, when intimate pictures are published, what could or should be done? Credit to Edison Chen for raising this err... point. Under our current legislation, there is no protection for

the subject of the pictures. The photographer has copyright, but is copyright appropriate? Copyright is a contract between the creator of an artistic work and Society: the creator gets time-limited rights to make money, and Society gets the work in the long run, but intimate pictures are not intended to be published.

My thought is that the Data Protection Principles fit this case very well. Take a look at Principle 3 - *personal data should be used for the purposes for which they were collected or a directly related purpose*, so distributing to strangers on the internet is forbidden, unless the subject gives permission. That matches how I would like the law to protect this type of information. The problem, however, is enforcement. All the Privacy Commissioner can do at the moment is to issue an "enforcement notice", then, if the offence is repeated, the offender can be prosecuted. Why do you need to leak private information TWICE – once it is leaked it stays leaked.

Once a leak has happened, the damage is done. Therefore there must be a deterrent punishment. What surprises me is that the Commissioner has even shied away from issuing an enforcement notice – I'm talking about the results of the investigation into the Octopus Rewards Program. In that case, the information was sold to third parties for millions of dollars, yet apparently it was not likely that a contravention would continue.

So now we come to economics: information can be worth money. Who has a supermarket loyalty card? Do you realise how much valuable information about your family's shopping habits you are giving out? Of course, it is a trade, I get 0.2% discount, they get to know more about how I shop than I know. Hong Kong is known for its free market economy, but, any economist will tell you, markets are efficient when buyers and sellers have the same level of information. If I was a supermarket, I would be planning to put RFID chips in the loyalty cards, and update the prices as you approach the shelves.

It is not just supermarket economics. I predict a crisis in the health insurance market. All insurance is based in ignorance: neither the insurer nor the insured knows what is going to happen, so the insurer sets the premium according to the probabilities. Too much knowledge destroys that, and medical science and information technology are providing that knowledge. Already, genetic factors involved in many diseases are known, and more are being discovered and DNA sequencing is becoming cheaper. Will we be required to provide a genetic sample when we apply for health insurance, and some people get very low premiums (they are not at risk), and others get unaffordable premiums? DNA is personal information, how much more personal can you get? Do we want privacy laws that prevent insurers demanding a sample? What if an insurer takes your enquiry form and carefully processes it to recover DNA from the sweat left by your fingers?

One of the things the consultation asked was whether "sensitive" data should be given greater protection. I don't think you can divide data by sensitivity. It depends on how the data is used. I constantly shed DNA, as dead skin cells, without worrying, until someone uses my DNA to decide my health insurance premium. I do not find my HK ID card number to be embarrassing, I hold birthday parties, and even tell people my mother's maiden name. These are not items of information that need to be kept secret. Until, of course, some idiot who knows nothing about security decides that they can be used to authenticate my identity for something, like activation of my credit card or access to my phone records.

I would like to see this mis-use of personal data as supposedly "secret" authentication tokens stamped out. The practice always was insecure, but we have increasing repositories of shared personal information that can be searched by strangers. I'm talking about social networks. A friend posts a remark about how much fun their had at your birthday party, and suddenly a criminal has the last piece of information they need to mis-use your credit card.

We need a review that takes a holistic view of how laws should control the Information Society we are building.

Scotland's New Privacy Principles

<web-link for this article>

Scotland is introducing privacy principles to control the amount of personal information collected by public-sector organisations. They are:

Proving identity or entitlement: people should only be asked for identity when necessary and they should be asked for as little information as possible

Governance and accountability: private and voluntary sectors which deliver public services should be contractually bound to adhere to the principles

Risk management: Privacy Impact Assessments should be carried out to ensure new initiatives identify and address privacy issues

Data and data sharing: Organisations should avoid creating large centralised databases of personal information and store personal and transactional data separately

Education and engagement: Public bodies must explain why information is needed and where and why it is shared

They are likely to become a benchmark for all public bodies in the UK. The principles take the Personal Data Protection principles laid down by the OECD, and used in legislation such as Hong Kong's PDPO, to a more specific, operation level, actually specifying that people should only be asked for identity when necessary, and risk management should be considered.

Yui Kee Chief Consultant, Allan Dyer, commented, "Some Government departments in Hong Kong would do well to look at these, for example, the eTAX hotline asks for a caller's HKID card number when the problem is pre-login on their website."

More Information

Privacy principles to improve public confidence
Scottish privacy principles could become UK benchmark
Scotland unveils privacy principles
Mind your own: Scotland unveils privacy principles
Views on the Review of the Personal Data (Privacy) Ordinance

A Truely Honest Privacy Policy

<web-link for this article>

Author Dan Tynan has published a neat privacy policy at open exchange IT website ITworld. He's open-sourced it too, so you can use it on your own site. It's hilarious.

More Information

The first truly honest privacy policy
Views on the Review of the Personal Data (Privacy) Ordinance

Enforcing Privacy

<web-link for this article>

Our Chief Consultant Allan Dyer's further thoughts on the Consultation Report on Review of Personal Data (Privacy) Ordinance:

In my previous submission, I dismissed Proposal 4, concentration of the additional power of prosecution in the Privacy Commissioner, but that was before I knew the consequences of the existing arrangement. If I understand correctly, the procedure now is for a complaint to be made to the Privacy Commissioner, who investigates and decides whether there is a criminal

offence. If there is, a complaint must be made to the Police, who then investigate the offence. The investigation is duplicated.

Quite how ridiculous this procedure is can be appreciated by considering a member of the public discovering a dead body. The equivalent procedure would be for the person to call a pathologist to conduct an autopsy, and, only if the pathologist considered there was a possible crime, would the Police be called.

The repetition of the investigation, after a delay, is likely to substantially lower the success rate. Potential witnesses will be discouraged by the waste of time repeating their statements, and recall of facts will be impaired by the delay. The initial investigation might even obliterate significant evidence before the second investigation is conducted, the only way to ensure against this would be to have equally-skilled forensic investigators in the initial investigation, thus ensuring that the repetition doubles the cost.

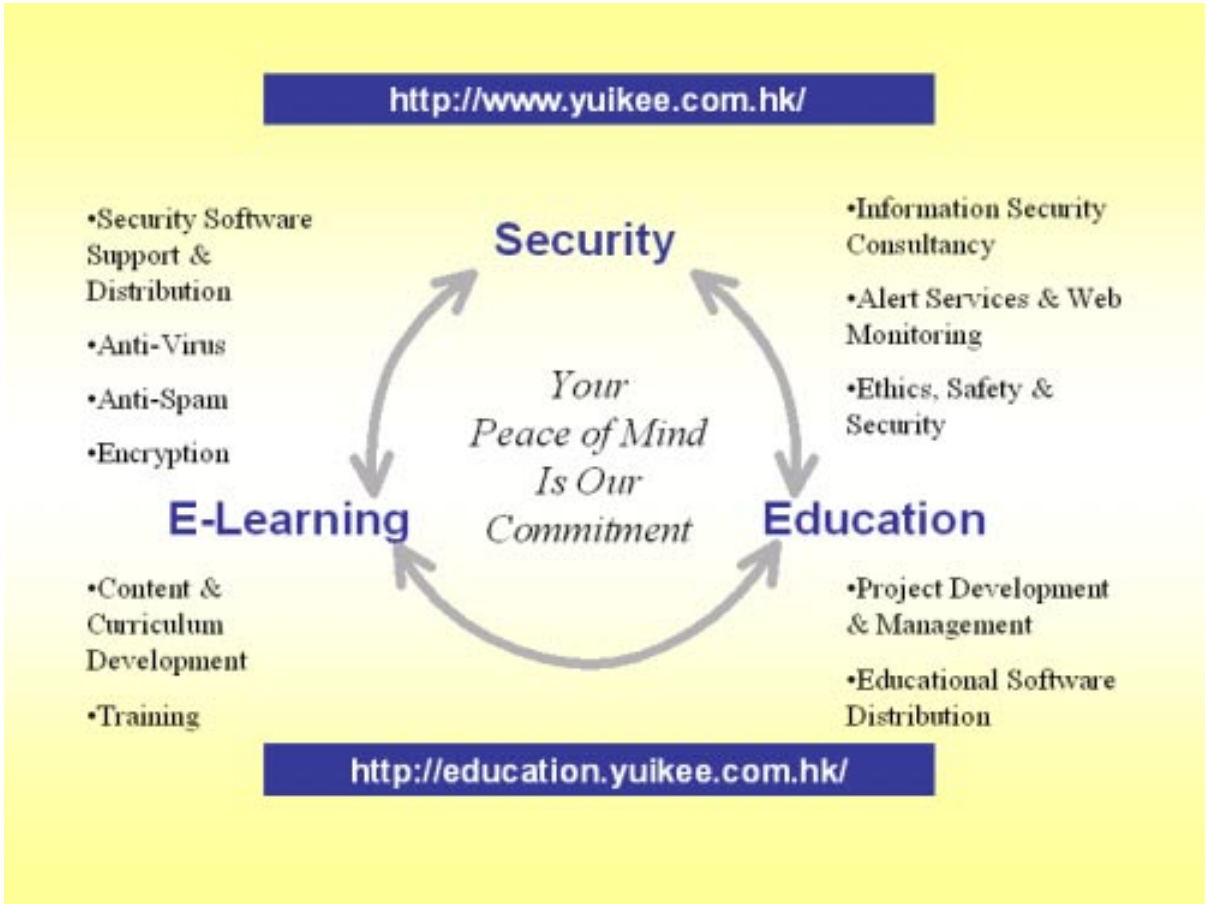
Any complaint by a member of the public of an possible crime should be handled by the Government in an efficient, transparent and effective manner. Duplicating the investigation does not achieve this.

More Information

Views on the Review of the Personal Data (Privacy) Ordinance

YUI KEE
銳基電腦顧問有限公司
Anti-Virus, Network Security & Education

Suite C & D, 8/F, Yally Industrial Building
6 Yip Fat Street, Wong Chuk Hang, Hong Kong
Tel: 2870 8550 Fax: 2870 8563
E-mail: info@yuikee.com.hk
http://www.yuikee.com.hk/


http://www.yuikee.com.hk/
Security
•Security Software Support & Distribution
•Anti-Virus
•Anti-Spam
•Encryption
•Information Security Consultancy
•Alert Services & Web Monitoring
•Ethics, Safety & Security
Your Peace of Mind Is Our Commitment
E-Learning
Education
•Content & Curriculum Development
•Training
•Project Development & Management
•Educational Software Distribution
http://education.yuikee.com.hk/