Yui Kee Computing Ltd.

Newsletter

December 2009

Contents

Can Your Social Network Authenticate You?

<web-link for this article>

Roger Thomson, AVG's Chief Research Officer, has described how credit card companies are using information from social networks to authenticate customers in his blog. In short, his card was declined, he called his bank, and one of the "security questions" was about the age of his daughter-in-law, referred to by her maiden name. The only place Roger knows of a public link between them is Facebook, so it appears that (some) credit card issuers are utilising personal data from social networks for the purposes of authentication.

To find that a stranger knows something about us that we do not expect sends a shiver down our spine, yet the same information might be freely discussed in our circle of friends. It is the moment in the movie when the Bad Guy says to the victim, "We know where you live, and where your children go to school", the threat is implied, but strong. But what are the real issues?

Is It a Threat?

Credit card companies are respected financial institutions, not known for indulging in the sort of kidnapping and extortion that features in movies. A credit card company using social network data for authentication does not pose a physical risk.

What if the credit card company matched your friend's birthdays to your purchase records and their interests and hobbies? They could sell the information to a direct marketer, and you might receive, entirely "coincidently", a marketing message just when you were wondering what gift to get. This represents a serious shift in the balance of information between vendor and purchaser, and is, effectively, an attack on the Free Market.

Is It Reliable?

In the authentication process, multiple checks are made, so the reliability of a single question is less important, assuming the credit card company has correctly analysed the reliability of each question, and is using Bayes' Theorem to combine the results. Still, a question with 50% false positive and 50% false negative results would be worthless, so what will damage the reliability:

- Inaccurate social network data - your friend lied about their age, or mistyped something, or didn't update
- You don't know, or can't remember - will inability to keep a credit card become another affliction of the socially inept?
- Making the wrong connections - maybe you know two John Smiths

But there is another problem with the reliability, a problem that will become more severe as this type of questioning becomes more prevalent: there are intelligent adversaries. The criminals can try to harvest exactly the same information that the credit card companies are using, and provide it, real-time, to the low-level fraudsters so they can answer the "security questions" flawlessly. The criminals can probably develop their response more cheaply - they can copy or steal the credit card companies' software, and use stolen computer resources (botnets) to run them. Developing an expensive system that your opponent can defeat cheaply does not sound like a good strategy, and it is the customers who will ultimately pay.

Personal Data Privacy

Roger Thomson is in the USA, but Hong Kong and Europe have legislation on Personal Data Privacy. The details of the legislation differ, but the basis is six Data Protection Principles (DPP). A major difficulty in apply these to social network issues is that they assume a simple data subject/data user model that does not match the complexity of relationships on social networks.

Under DPP5, which requires data users to be open about their personal data policies and practices, the credit card companies probably need to say how they are using social networks.

By DPP3, which says that the data subject's permission is required before their data can be used for a new purpose, when your credit card company asks you about your daughter-in-law's age, you should refuse to answer because you do not have her permission to use her data to authenticate yourself. Of course, you then have the disadvantage of not being able to use your credit card.

We expect credit card companies to prevent fraud, and they can rely on us to not take good care of the cards, keep the PIN with the card, and all sorts of other, lazy security mistakes. In response, they introduce new security measures that do not require effort from us, but which may not be effective, sustainable or in our wider interests.

15th December 2009

Allan Dyer

David Harley, Director of Malware Intelligence, at ESET has posted an excellent article discussing Roger Thomson's experiences. In particular, David raises the scenario, not discussed above, of an attacker poisoning publicly available information. I think that is a possibility, but the extra work and risk would make it a much more targeted attack, against a high-value victim.

More Information

Now THIS is scary
About Roger Thompson
Views on the Review of the Personal Data (Privacy) Ordinance

Your Data and Your Credit Card

COFEE Break

<web-link for this article>

A month after Microsoft's free law-enforcement-only live forensics tool, COFEE, was posted to a file-sharing site, Graham Cluley's prediction that someone could write a tool that neutralises it (or wipes sensitive data) when it was used has been fulfilled. DECAF is a lightweight tool, reported to be written in Visual Basic 2005, that waits for COFEE's launcher to be executed, verifies the hash of the launcher and the presence of the COFEE USB, and then performs configurable actions. Possible actions include shutting down the computer, disabling devices, erasing data, events and caches.

One of the authors of DECAF claimed, "We want to promote a healthy unrestricted free flow of internet traffic and show why law enforcement should not solely rely on Microsoft to automate their intelligent evidence finding". Reinforcing DECAF's positioning as a demonstration, the End User License Agreement includes, "You will not use DECAF for illegal purposes", though criminals wanting to hide incriminating evidence from the Police are unlikely to obey such restrictions.

Allan Dyer, Yui Kee's Chief Consultant, commented, "the authors of DECAF have a point, the Police should not place too much trust on a single, automated tool. But most Police Forces know that already."

No doubt, a new version of COFEE that avoids recognition by DECAF, and that detects it in return, will be soon released.

More Information

Hackers declare war on international forensics tool
Regular or Decaf? Tool launched to combat COFEE

Schneier Classifies Social Networking Data

<web-link for this article>

Internationally renowned security technologist and author Bruce Schneier has published a Taxonomy of Social Networking Data on his blog. Bruce's divisions are:

- Service data. Data you give to the site in order to use it.
- Disclosed data. Data you post on your own pages.
- Entrusted data. Data you post on other people's pages.
- Incidental data. Data other people post about you.
- Behavioral data. Data the site collects about your habits.

This is a useful starting point for discussing data on social networks, and who should have what control over it. However, things can get complicated very quickly. Using Roger Thomson's credit card "security question" incident, discussed earlier in this issue, as an example, his credit card company (probably) used the existence of a link between two people to generate the "security question" about the contact's disclosed data. The link is a new category: jointly disclosed data - it cannot be seen until both parties agree, but the site (necessarily) knows in advance: when one party has sent the "friend request".

Blogger José Ignacio Orlicki has proposed a different taxonomy, based on the destination of the data.

More Information

A Taxonomy of Social Networking Data
Can Your Social Network Authenticate You?
Another Categorization of Social Networking Data

SMS and Social Networks: Beware of Scams

<web-link for this article>

Hong Kong's Telecommunications Regulator, OFTA, has agreed voluntary guidelines to control misleading charged SMSs with the five main telecom companies: CSL, SmarTone, 3, PCCW and Peoples. The move follows a damning report by the Consumer Council about 470 complaints it had received from January to November this year. Typical scams offered users a "free" service ("friend-seeking", "IQ test" or a "lucky draw") with concealed conditions - the users were subscribing to expensive SMSs charged to their phone-bill. One People's customer reported being charged HK$50 per message, and, when he refused the bill totalling HK$2000, he received a lawyer's letter and had his mobile service stopped.

Action on misleading messages has been slow, telecoms companies typically respond that subscribers should discuss it with the content providers directly, a PCCW representative said that it provided a platform for communication between content providers and users; and OFTA's initial reaction was that they didn't fall within its purview. However, the Consumer Council report, and subsequent pledge by the Secretary for Commerce and Economic Development Rita Lau Ng Wai-lan to crack down on unscrupulous practices led to the sudden drafting of the voluntary code.

The code includes four points:

- Messages to include notice they are chargeable, and when the chrages are invoked;
- Providing clear information about charges;
- Clear, easy to understand and use arrangements for unsubscribing or deregistering;
- Disputes over content services must not affect normal mobile phone services.

However, Samson Tam Wai-ho, LegCo member for the IT functional constituency, doubted that a voluntary code would be effective.

The misleading offers of services are often made online, and Hong Kong is not the only place where these scams operate. Michael Arrington has written about the lead-generation business model of application developers on social networks and the social gaming ecosystem of hell they form with advertisers. The offers sound eerily familiar: "IQ tests" and hidden, expensive subscriptions.

More Information

Message loud and clear
Consumers bound to get last word
Scamville: The Social Gaming Ecosystem Of Hell
Social Games: How The Big Three Make Millions

Gartner Advocates Security Dead-End

<web-link for this article>

A recent Gartner report by analyst Avivah Litan notes the recent surge in online banking fraud, and details some of the methods criminals are using to defeat strong authentication methods. It correctly identifies the insecure browser as the flaw to be addressed, but advocates server-based fraud detection to monitor transactions for suspicious behaviour as the solution.

Criminals attack strong authentication methods in a variety of ways. Authentication using one-time passwords or a token generating an authentication code might be compromised by a trojan in the browser that captures the user-id, password and code, and uses them immediately to make a fraudulent transfer, returning an error message to the victim. Or the trojan might silently change the destination and amount of the transfer. If the authentication uses out-of-band communications by phone, criminals might use call forwarding to intercept the validation call.

Server-based fraud detection monitors transactions for suspicious behaviour that might indicate that the transaction is automated. The speed of "typing", the navigation from login to the transaction page, or other clues might give away that a bot, and therefore fraud, is involved.

Could a trojan that captures keystrokes also note the cadence of the strokes, and use that when communicating with the bank's server? Criminals are likely to develop ways to make their transactions look more "normal", especially now there is a Gartner report instructing banks to look for the "abnormal". The benefits of a server-based fraud detection monitor are likely to be short-lived.

Our Chief Consultant suggested a solution to untrustworthy computers in an article for the IMIS Journal in 2004:

> *Perhaps trusted readers would be a solution. We could have a device with a screen, about the size of a PDA, with a built-in smartcard reader that probably plugs into a USB port. Its function would be simple: accept a text-only document through the USB connection, display it on the screen, and sign it using the inserted smartcard, returning the signature by the USB. Make the case tamper-evident, and publish the software for review. The Government would certify units; they would definitely not be updateable. This would make them immune to viruses, because they would have limited functionality: they can sign documents; they cannot change their own software. The primary design objective would be to make the functionality as simple as possible, so there will be fewer programming errors, and so the code will be easier to audit.*

More Information

Gartner: Hackers are defeating tough authentication
Avivah Litan
When and Where Strong Authentication Fails (by Avivah Litan)
Gartner's Avivah Litan on the online banking fraud surge
Trusted Readers in an Untrustworthy World

Strategic Commodities Import and Export Regulation Changes Take Effect 4th February 2010

<web-link for this article>

Hong Kong's Director-General of Trade and Industry has appointed 4th February 2010 as the date when the revised control list for strategic commodities, previously reported, comes into force. The amendment includes four changes to the regulations on Information Security products.

More Information

Commencement of the Import and Export (Strategic Commodities) Regulations (Amendment of Schedule 1) Order 2009
Hong Kong Amends Strategic Commodities Import and Export Regulations

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/