Yui Kee Computing Ltd.

Newsletter

May 2008

Contents

Web Page Design Rap

<web-link for this article>

Get the message about web page design. Poetic Prophet (AKA The SEO Rapper) stars in a music video advocating web standards and proper design.

More Information

Design Coding

Questioning Password Resets

<web-link for this article>

Allan Dyer

A recent article and a website advocate improving the quality of "security questions" for web-based customer self-service password resets, but are any questions really suitable for global, inter-cultural use? Personally, any information about me that is memorable and I would be willing to tell to a website is probably not a secret, and if it is not memorable, I won't remember it either, making it useless as a "security question".

Below I list some of the questions that goodsecurityquestions.com claim are "good", with thoughts on their limitations. Of course, a developer can provide a choice of "good" questions for users to choose between at registration, but the number of choices suitable for particular users may be very restricted, once cultural, social or other factors are considered:

- **What was your childhood nickname?** Might be researchable from a friend's social networking page, the user may not realise that.
- **What street did you live on in third grade?** Culturally specific to North America... how old is "third grade"?

- **What is the middle name of your youngest child?** Limited to users with children with an odd number of names. The answer may change over time, when a new child arrives. Cultural perception may change the name order - am I Allan George Dyer, or DYER Allan George, which was my mother thinking when she registered?
- **What was your childhood phone number including area code? (e.g., 000-000-0000)** Don't try validating the number format, it is North American specific. I have no idea what the area code was for my home town when I was young, but I am fairly sure it is not the same now.
- **What was the name of your first stuffed animal?** Guess "Ted" or "Teddy" first. How large is the vocabulary of a 2-year old?
- **What are the last 5 digits of your driver's license number?** Which driver's license? My Hong Kong license number is the same as my Hong Kong ID card number, which is information I refuse to use for authentication. I cannot remember my UK driver license number, but I think it includes letters as well as digits.
- **What was the name of your elementary / primary school?** Easily researched from social networking sites.

So even "good" questions may be limited in their applicability. Developers should consider the risks involved for their application.

More Information

How to do password resets right
Examples of Security Questions

Ethics, Hacking and the Law: the Tipping Point

<web-link for this article>

Security researchers at TippingPoint DVLabs have made a nice little ethical dilemma for themselves. The Kraken trojan builds a botnet that is difficult to take down because, instead of using a hard-coded address for the control server(s), it uses a pseudo-random domain name generation algorithm that allows the zombies to search for control servers. The good guys therefore do not know which addresses to get taken down.

Pedram Amini and Cody Pierce at TippingPoint realised that this gave them an opportunity to "infiltrate" the botnet. They reverse-engineered the Kraken trojan and built their own, fake, control server that could successfully communicate using Kraken's encrypted protocol. When they registered some of the sub-domains Kraken is looking for, Kraken infected systems started contacting their fake server, asking for instructions. Over one week, about 25,000 infected systems contacted their fake server, an estimated 14% of the infected population.

TippingPoint can now issue instructions to those 25,000 machines, telling them to do anything from sending spam (as the botnet creators probably originally intended), wiping the machine, or, simply, uninstalling the Kraken client. This is now their dilemma: uninstalling the client would appear to be a benevolent act, should they do it?

On the plus side, about 25,000 users will find their computer and internet connection is faster, and there will be about 25,000 less machines sending spam or participating in DDoS attacks etc.

On the minus side, what if there are unintended consequences of the uninstallation? Dave Endler, director of TippingPoint, brought up the hypothetical case of what happens if the uninstallation accidentally crashes the target system? What if that target system is responsible for someone's life support?

Yui Kee Chief Consultant Allan Dyer commented, "The life support scenario is a bit extreme - why was such a critical machine unprotected and connected to the internet to get infected in the first place? However, we can substitute 'serious damage' without changing the discussion. I would take a probabilistic view: which has the greater probability of resulting in damage, uninstalling the malware without authorisation, or leaving it there for an indefinite period to be exploited by Kraken's developers, possibly downloading additional software with additional incompatibilities? Uninstallation seems less risky, and is therefore the ethical choice."

However, ethics is not the only consideration. In most jurisdictions, unauthorised modification of programs or data on a computer is a crime, so the uninstallation would be illegal, regardless of the fact that the installation was also illegal. Dyer commented, "Vigilantism can lead to chaos. So far, TippingPoint has done some good research and passive monitoring that may benefit their customers, and have uncovered a crime in progress. Isn't this the point where they should turn the results over to the Courts and the Police, to decide what happens next? There are great difficulties there too: firstly, with jurisdiction, but this is an area where we need to think, what should the appropriate course be, and how can we put in place the laws and cooperation to make that work."

The debate might be moot for the Kraken botnet - now that the infiltration has been publicised, Kraken's developers might be taking other actions.

More Information

Whitehats tackle The Great Botnet Dilemma
Botnet agent plays lost sheep to avoid detection
Kraken Botnet Infiltration
Kraken Infected IP Addresses
Owning Kraken Zombies, a Detailed Dissection

Data Leak Disease

<web-link for this article>

Allan Dyer

Hong Kong is suffering an epidemic of data leaks, and a serious of incidents in the Health Services are the latest to come to light. People and organisations handling sensitive data have had plenty of warning, starting with the public outcry at the leak from the Independent Police Complaints Commission in 2006. There was a strong reminder in September 2007 when the email passwords of various political parties and figures were revealed, and overwhelming public interest in the leaking of erotic photos stolen from Edison Chen's hard disc in February this year. However, despite these cases, many organisations have still not put strong measures in place to control leaks, only now is the Hospital Authority holding an emergency meeting to work out new guidelines.

The latest leaks reported have mostly involved the loss, or theft, of small memory devices: flash cards and USB drives:

- April 25 Tuen Mun clinic (665 patients)
- April 25 United Christian Hospital (26 patients)
- April 26 Kowloon Hospital reports data loss involving five patients
- April 28 Pamela Youde Nethersole Eastern Hospital reports data loss involving 50 patients
- April 30 Civil Service Bureau reports data loss involving 25 workers
- May 5 Hospital Authority reports data losses:

- three at Pamela Youde Nethersole Eastern Hospital (983 patients)
- two at Kowloon Hospital (43 patients)
- one at Queen Mary Hospital (3,000 patients)
- one at Tuen Mun Hospital (1,885 patients).

- May 6 Privacy Commission reveals data loss from Prince of Wales Hospital. May involve 10,000 patients.

In the Prince of Wales Hospital incident, a technician lost a USB drive, which was attached to her mobile phone, in a taxi. The data included patients' names, ID numbers and pathological tests, however, the technician was "not sure" if the data had been erased or not. There is no suggestion that the data had been securely erased by overwriting multiple times, so much of it could be recovered fairly simply. The description implies that much is wrong with hospital IT systems:

- The device was the technician's personal possession (why else was it attached to her mobile phone?), credit to the technician for using personal resources to get the job done, but why isn't the hospital providing the necessary resources?
- The data might have been erased, implying it was used as temporary storage, probably to transfer the files from one system to another. Why couldn't the transfer have been achieved via a network connection? Of course, networks also have vulnerabilities, but they can be protected by centrally managed solutions, and the exposure is for the limited time of transfer, not for the life of a USB device.

Hospital Authority chief executive Shane Solomon has announced that the authority would upgrade its system in seven to 10 days so that all downloaded information would be automatically encrypted and could only be read by the authority's computers. It is surprising that an IT department that, apparently, was unaware that its failure to provide suitable resources was forcing its users to use personal storage devices is able to roll-out an ambitious encryption scheme in such a short timescale. I wonder whether they have properly studied the impact this will have. Will Doctors find themselves unable to access patient data at critical times? With the keys distributed over so many thousand Authority computers, any serious attacker will still be able to access stolen data.

One idea to reduce the loss of data on mobile storage devices would be to use commercial anti-shoplifting technology. Issue staff with the USB drives they need, but tag them and install detectors at the hospital exits. The beeping when the devices leave the premises should remind staff, and inconvenience petty thieves. This could be used with or without encryption.

Ultimately, the Authority needs Information Security Management that supports the healthcare givers in their important work.

09th May 2008

More Leaks

Allan Dyer

The problem with writing about data leaks in Hong Kong at the moment is how to keep up with the new reports. In the day since writing the above section, HSBC has revealed that it "lost" a server containing personal data, and a member of Immigration Department staff inadvertently shared confidential Department files from his home computer. Additional details also confirmed some of the issues I speculated about.

The server went missing from the Kwun Tong branch of Hongkong and Shanghai Banking Corporation during a renovation, and the case was reported to the Police as theft on April 26. It contained name, account number and transactions of 159,000 customers, though the bank

reported that it was protected by "multiple layers of security which are regularly reviewed". One hopes that those layers include strong encryption (Triple-DES, AES or similar) of the sensitive data on disk. Once the server is in the physical possession of an attacker with reasonable time, measures such as physical locks and barriers, and logical access controls managed by the operating system are easily bypassed. The bits can be read from the physical media, and only encryption stands between the attacker and understanding of the data.

The Immigration Department incident involved a member of new staff who took old confidential files home to familiarise himself with working procedures. He said the classified files were put in folders that were not shared by the Foxy peer-to-peer sharing software. However, many users of the software are unaware that the default settings share the whole hard disk. The issue here appears to be that the staff was not properly briefed about handling confidential files, and a mis-placed trust in the security of the home (internet-connected) computer.

On the previous cases, the Hospital Authority is planning to upgrade computers and networks, to ensure that all its computers are connected to a single network, eliminating the need to transfer files using removable devices. It was confirmed that a worker used a removable device to transfer data from one computer to another within the same department, leading to the data leak when the drive was lost.

To say that these incidents are the tip of the iceberg is understating the problem, and it is not just Government departments and financial institutions. I recently had reason to transfer some files to an advertising media company, the method was ftp, the username was the same as the domain name and company name. It is easy to compile a list of mistakes:

- Unencrypted protocol: ftp
- Use of shared user account - no accountability of actions
- Weak password - while not as bad as, say, '12345', it was not strong
- No delete limitation - potentially, any user could delete files relating to dozens of projects

The data mostly related to old campaigns, so disclosure would not be a concern, but sometimes it would contain details of campaigns pre-launch, and the details might be extremely valuable to their client's competitors. Also among the files was a Resume, definitely a violation of the Personal Data Privacy Ordinance.

There is a widespread lack of a security culture that is putting huge amounts of data at risk of exposure or loss. Anyone reading this newsletter is probably already information security-aware, what can we do about all those with no concept of the problem?

More Information

Anonymity and Secrecy: Why Sin Chung Kai Should Apologise
Hong Kong Liberal Party Can Count but Sin Chung Kai uses Wife's Name in Password
Espionage and Arrest in Tor Sniff Case
Tor used for Man-in-the-Middle Attacks
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Why flawed privacy ordinance must be given more teeth
November - December 2006
Another data leak prompts security vow
HSBC boss says sorry over lost data server
Bank loses server
HSBC in further data loss

Humour: Bobby Tables Parks His Car

<web-link for this article>

Are automatic license plate scanners vulnerable to SQL injection exploits? The driver of this car knows.

More Information

Hackeando
Humour: Bobby Tables

Schneier Advocates Tougher Privacy Laws

<web-link for this article>

Bruce Schneier writes about the need for a "comprehensive data privacy law" in the latest issue of his monthly newsletter. He appears to be on the same wavelength as Hong Kong's currently toothless Privacy Commissioner, saying, "And we need more than token penalties for deliberate violations."

More Information

Our Data, Ourselves

False Positive Propagation Problem

<web-link for this article>

A recent article by Pedro Bustamante, a researcher at Panda Security, the Spanish Anti-Virus company highlights a problem with the automation of virus definition creation. Anti-virus companies have been increasing their use of heuristics and automation in sample collection, handling and analysis for many years. This has allowed them to keep up with the huge increase in the amount of malware being generated, but it also leads to an increase in false positives on programs that show some of the characteristics of malware. Worse, once a small number of anti-virus companies start detecting a program as malicious, the rest follow suite, perhaps without verifying that the program is, in fact, malicious. This is driven by the dual needs to provide the best protection to their customers by cooperating with "rival" anti-virus companies in sharing samples, and to always score "perfect" detection on tests performed by researchers who are also not checking exhaustively for false positives.

A case in point is the detection of game downloaders created by Fenomen Games, a company that creates and distributes games. The game downloaders have many of the features of trojan downloaders, such as the runtime-packing and their behaviour of connecting to the Internet, downloading something, executing it and exiting, so they often trigger heuristic detection. Mr. Bustamante has analysed some of these and not found anything malicious. Assuming that the analysis is correct, then AVIRA's description, saying it is a trojan, is wrong. On the other hand, Sophos' description, saying it is Adware or PUA (Potentially Unwanted Application), is arguably correct - in a business context, few employers would want their employees downloading and playing games.

Test results that do not clearly specify what was tested therefore have little value - how can you be sure they reflect your requirements?

More Information

Fenomen(al) False Positives

Data Leak Disease Spreads to Police?

<web-link for this article>

Hong Kong's Police Force are now the focus of concerns about unauthorised data leaks following the emailing of ten documents to the media. The documents appear to be confidential Police reports, and the email claimed they were downloaded using the peer-to-peer software Foxy. It has been noted in previous data leak cases that a default Foxy installation shares the user's entire computer, without clearly notifying the user.

The documents include a report on an anti-drug operation in a Kowloon West disco, including undercover agent aliases and other operational details. A Police spokesman has declined to confirm whether the files are genuine, and the technology crimes division is following up the case.

Sin Chung Kai, Legislative Councillor for the Information Technology sector, showed no restraint in commenting before the facts are known, saying it could be a hoax. Apparently demonstrating detailed knowledge of Police IT systems, he said, "The data would be stored in a standalone computer and would not be connected to the internet so it is difficult to see how it could be transferred". However, Hong Kong Police Inspectors' Association chairman Tony Liu Kit-ming had a different perspective, saying that the leak could be a result of officers taking work home, "It is common for frontline officers to write their reports at home and it poses risks to security, but they have too many things to be finished and working at home is the only way."

Previous high-profile data leak cases in Hong Kong have included Legislator Sin Chung Kai's email, the Independent Police Complaints Commission, various Hospitals, and celebrity Edison Chen.

28th May 2008

Inquiries have confirmed that the documents are genuine, and have identified three officers as responsible for the leaks. However, more confidential files were found on the internet yesterday, including a detailed police investigation report, a report on an appraisal of an officer and the job description of an ICAC officer. These are clearly not isolated incidents.

Discussion has focussed on the practice of using home computers to work on official documents, in violation of regulations, and the lack of computers available for junior officers. Ten constables might share a computer in a police station. Computers need not be expensive, charitable organisations are aiming to empower third-world school children with the One Laptop Per Child initiative. Perhaps senior Police officers should consider a "One Secure Laptop Per Constable" programme.

There is a lesson for all organisations: encouraging home working may be attractive for many reasons, but such a move has security implications, and enlarges the security boundary of the organisation. Cost savings may be less attractive when you need to budget for securing your employees' home computers.

More Information

Covert cops hit by leaks
Data Leak Disease
Hong Kong Liberal Party Can Count but Sin Chung Kai uses Wife's Name in Password
Privacy and Obscenity: Hong Kong's Showbiz Sex Scandal
Anonymity and Secrecy: Why Sin Chung Kai Should Apologise
Financial hub vulnerable as lax security raises risks

African Union Clamps Down on Advanced Fee Fraud?

<web-link for this article>

Spammers are staying creative in their attempts to trick fools out of their money. A recent message claims to be from the "MINISTERIAL COMMITTEE OF AFRICAN UNION GOVERNMENT" in Ghana, and starts:

This is to notify you that African union government have received complaints about being swindled off your money by our bad citizens in Africa. And world bodies have called to our notice to look into this menace that is eating deep and simultaneously undermines the name of Africa as a continent.

It goes on to say that the crimes will be investigated, and compensation will be released "without delay", please fill in some personal details. Quite why the African Union Government would need to use an Australian webmail account and would want a reply sent to a GMail account is unclear.

We guess that there will be some minor "handling fees" to pay before the compensation can be "released". The spammers appear to be working on the principle that people stupid enough to fall for an earlier scam are too stupid to learn caution when receiving unexpected email messages.

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/