Yui Kee Computing Ltd.

Newsletter

July 2007

Contents

Renaming Passwords

Passwords are recognised as the easy and cheap-to-implement method of authentication, but their disadvantages are low security and the continual running costs of users forgetting them. Many alternatives have been proposed, and one that has gained recent attention is "Passfaces", designed and sold by Passfaces Corporation. How does it really compare to passwords?

In the Passfaces system, users are required to remember a series of faces, and select them from a grid of other faces when they log in. In the demonstration on the Passfaces website, guests are asked to remember one face from each of three grids of nine faces. This is an easy task, and the demonstration works acceptably. However, this only provides $9^3 = 729$ combinations, or about 9.5 bits of entropy. Assuming English provides 1.3 bits of entropy per character, this is equivalent to an eight-letter English password, which, as it would be vulnerable to a dictionary attack, would be considered very weak.

Of course, the strength could be increased by using a longer sequence of faces, but would that still be easy to use? What if every website you logged in to required remembering a long sequence of faces?

The Passfaces website also claims, "When used with a simple password, Passfaces provides a second factor in a two factor authentication process". This is simply wrong: passfaces and passwords are both *something you know*, and therefore constitute a **single** factor of authentication.

One scientific usability study of Passfaces at UCL had mixed results, the number of failed logins was drastically reduced by Passfaces, but the number of reminder requests (directly affecting helpdesk calls and costs) was not. The study also noted that Passfaces took significantly longer on low-powered hardware.

So, if you want a *something you know* authentication method that requires higher processing power than passwords, and might be easier for users, but which is not stronger than passwords, Passfaces might be what you are looking for.

More Information

Firm aims to phase out passwords
Welcome to passfaces
Try Passfaces: Demonstration
Face in the Crowd
Are Passfaces More Usable Than Passwords? A Field Trial Investigation

Anti-Virus Companies in Legal Battle

Russian anti-virus developer Kaspersky Lab is suing Chinese competitor Rising Tech Co. Ltd. for unfair competitive practices in an escalating dispute between the companies. The dispute started when Kaspersky mistakenly identified components of Rising's software as malicious in May 2007. Rising responded by claiming that Kaspersky had twenty-two false positives during a six-month period and showed contempt for Chinese users. Kaspersky responded with the lawsuit. Rising has upped the stakes by releasing another announcement accusing Kaspersky of another six false positives in two weeks.

The case will be heard in the Tianjin No.1 Intermediate People's Court at the end of July 2007.

Allan Dyer commented, "It is disappointing to see two good anti-virus companies, and AVAR members, mud-slinging like this. The fact is anti-virus software cannot be perfect, and we can expect occasional flaws to get through the testing process. Two other anti-virus companies have had recent false positives for components of the Chinese version of Windows. Those flaws had an immediate, detrimental, effect on end-users. A false positive on a rival anti-virus product will only effect users with both products installed - which probably means they are testing professionals. Kaspersky made mistakes, and quickly fixed them, Rising apparently took affront because their own software was mis-identified. Please can everyone calm down and get back to serving the users?"

More Information

Kaspersky(China) sues Rising
Antivirus Vendors Head to Court
半年内 22 次重大误杀 卡巴斯基蔑视中国用户
“误杀之王” 卡巴斯基 近两周又爆 6 次重大误杀
Rising responds to Kaspersky lawsuit, alleges that Kaspersky made six recent blunders
卡巴斯基回应查杀瑞星卡卡：一切为了用户安全
AVAR
Kaspersky sues Rising over unfair competitive practices
“误杀事件”升级 卡巴斯基起诉瑞星
Tianjin No.1 Intermediate People's Court

Developers Should Build-In Security

In the July/August 2007 Editorial of Visual Systems Journal, Editor Mike James raises the problem of increased security breaking existing applications, specifically, Windows Firewall preventing a WMI application from working. Our Chief Consultant, Allan Dyer responds:

"Security is Everyone's Business". Specifically, developers have a responsibility to consider and implement security when designing and building their applications. Too many systems are built using the "get it working first, secure it later" approach, which leads to many of the security disasters we see today.

The application in question was designed to contact other computers across a (possibly hostile) network, apparently without thought on who or what would be allowed to make connections, or how those connections would fit network security policies. Windows Firewall is a method for implementing the security policy of your organisation; don't blame it when it refuses to let you break the rules your organisation chose. Why didn't the security team know that RPC was a required service before they decided to deploy Windows Firewall with a configuration that blocked it? There does need to be more communication between the application and security teams, so the issues can be discovered and resolved at an early stage.

MSDN does have an article specifically addressing the Windows Firewall settings needed for WMI. I found them with a search for "WMI firewall".

I appeal to developers to design in security from the beginning, the "get it working first, secure it later" approach creates difficult security problems for the future.

14th July 2007

Mike James responded, agreeing about the dangers of the "get it working first, secure it later" approach, but pointing out that in XP SP2 the firewall is on by default and blocks WMI, the user doesn't make a choice and doesn't even know about it; and the instructions in "Windows Firewall settings needed for WMI" do not work.

On the first point, end users don't have the expertise to understand the implications of XP SP2 and its defaults, but end users aren't deciding to use WMI, either. As a default for end users, blocking a service that they are not using is a sensible precaution. It is probably the corporate IT department that is using WMI, and they should have the expertise to predict what happens when XP SP2 is deployed, or at least test it before they roll it out. And, as a developer, you should be aware of the services your application is using, and the security implications.

I am not saying this is easy, you are using WMI on top of DCOM on top of RPC, and it is the features of RPC that make it difficult to secure. However, the problem of securing RPC is well–known, at least in security circles - I have a book on Firewalls published twelve years ago that discusses the problem. Why have developers continued building on RPC without improving the security during those years? Presumably, security was not a priority for them - "secure it later". It **is** later, and we have to face the conflicting requirements created by leaving security out of the design requirements.

On the second point, the easy answer is, "Blame Microsoft". On the other hand, this is an excellent opportunity for Microsoft to demonstrate how seriously they are taking security nowadays by promptly fixing this.

I can't say what considerations the team that decided on the Windows Firewall defaults considered, but blocking a group of services that are not normally used or needed by ordinary users seems reasonable. Maybe they could have provided clearer information about the choices for IT departments and developers.

More Information

Visual Systems Journal
Connecting to WMI Remotely Starting with Vista

Hidden Costs of Government Reorganisation

On 1 July 2007, the Hong Kong Policy Bureaux of the Government Secretariat were reorganised. The Education and Manpower Bureau (EMB) was split into the Education Bureau (EDB) and the Labour and Welfare Bureau. This brought with it a domain name change for the Bureau's website and email addresses: emb.gov.hk to edb.gov.hk. The Government, naturally, is managing the change carefully: the old website displays a notice about the change, and the old email addresses are currently forwarded, and a change notice is sent back to the sender.

However, third parties will have to correct email addresses in their address books and mailing lists, and links on their websites, in many cases, manually. Wasting time. Many links will never be updated; they will go dead when the EDB decides it is time to switch off the old domain name.

Back in 1998, Tim Berners-Lee pointed out Cool URIs don't change. Government structure appears to change frequently, the functions do not. Why not use domain names that reflect the functions instead of the transitory bureaux, education.gov.hk instead of edb.gov.hk?

More Information

Education Bureau Notice
Education Bureau
Cool URIs don't change

Magical Information Security

From an information security perspective, the latest Harry Potter film left out the most magical part of the book, Harry Potter and the Order of the Phoenix. In the film, Alastor "Mad-Eye" Moody reveals the secret location of the group's headquarters using his staff, but, in the book, Harry has to read a note from Professor Dumbledor before he can become aware of its existence. This is because it is protected by the Fidelius Charm, which, as previously noted prevents transitive betrayal of trust.

Such a Charm could provide the perfect defence against virus spread, make unbreakable DRM, and totally eliminate software piracy. Imagine, you would need to receive a personally-signed license from Bill Gates before you could use Windows, and you couldn't copy or resell the capability! It is the software developer's dream... the nightmare is signing all those licenses.

The power and subtlety of the Fidelius Charm is incredible to anyone who thinks about information flow, and the film, unfortunately, is less magical for having left it out.

More Information

Potter and Security

Elk Cloner a Quarter-Century Old

The first personal computer virus, Elk Cloner, which spread on Apple II computers, is 25 years old this month. It is thought a 15-year-old high school student from Pittsburgh released it in July 1982. However, the idea of self-replicating code can be traced to a 1947 paper on self-replicating automata by John von Neumann, and the term computer virus was not used until about 1983 by Frederick Cohen.

More Information

Computer virus turns 25
Comments on ‘Computer virus turns 25’
John von Neumann

Remember to take those Security Precautions

Or you risk loosing customer confidence, as this photo shows.

More Information

Airport Security ftw!

Child Safety and Educational Video Websites

Yui Kee recently bid for a contract to build a website to host videos as an educational resource for teachers, parents and children. The bid was unsuccessful, but our proposal included a discussion of the child safety issues the project raised. We have decided to published an edited version of that discussion here, to promote careful consideration of the issues:

When this issue was raised in the briefing session, the response mentioned obtaining parental consent for including the videos on the site. While it is right that parental consent should be obtained, it does not constitute sufficient action on child safety. Firstly, it may not be *informed* consent. Parents may not appreciate the potential of the internet to magnify this type of threat, and parents will tend to trust that the School and the EMB have studied the issue and taken all reasonable precautions before asking for consent. Secondly, obtaining parental consent without taking all reasonable precautions is passing the problem to a party that is less able to deal with it – parents who understand the problem will refuse consent, their children will be safe but will be excluded from some of the benefits of the site; parents who do not understand the problem will give consent, and their children will be at risk. The Schools and the EMB have a responsibility to protect all children in their care, not just the children of informed parents.

Regrettably, the world is not a safe place, even for children, and the communications revolution of the internet that has brought so many benefits has also provided new opportunities for criminals and undesirables. Of particular concern is the use of online information by paedophiles. In the context of this project, we have preliminarily identified three areas of concern:

1. Salacious use of videos. Paedophiles would regard videos of children, especially if they featured sportswear or swimsuits, as arousing and a large collection of such material would be highly attractive to them.
2. Stalking. A paedophile might use videos from the site to select and research potential victims. Being chosen to demonstrate a technique in a sport would be a strong indication that the child was interested in that sport, and incidental features might indicate friends or other interests. The information might be used to engineer a meeting, or gain the trust of the victim.
3. Negative Publicity. If videos from the site were discovered in a paedophile's collection, the media could highlight the involvement of the site, the school and the EMB in enabling the activities of paedophiles.

Considering these threats, it should be remembered that paedophiles are not restricted to a particular location, race or educational background. Some are highly educated and technically competent, they are quite capable of developing sophisticated techniques and instructing the less able in how to use them. With the internet, distance is not a barrier, and, even though the proportion of paedophiles in the population is low, the numbers and capability of those that might cooperate to access and make “best” use of an attractive resource could be very high.

The approach to this issue we propose is a combination of Awareness, Restriction, Discouragement and Traceability.

Awareness

Teachers will upload the videos, so the teachers should be made aware of the issues and given guidelines with the aim of making the content less useful or attractive to paedophiles. The guidelines should be developed in collaboration with experts in this field. Some preliminary suggestions are:

1. Reduce identifiability. Choose a shot that does not show faces clearly in preference to one that does.
2. Remove unnecessary personal information. Avoid full names, or don't use names at all.
3. Consider the background and incidental details both when taking the shot and when choosing which shot to use. Incidental details might help with identification; background figures might be identifiable or inappropriate.

Restriction

The policy should be to restrict the site to *bona fide* users, only teachers should upload and only teachers, students and parents should download. Realistically, considering the school population of Hong Kong and a requirement for ease of use, this is unachievable, inevitably user access credentials will be lost, shared, and disclosed. Still, ongoing effort and resources should be allocated to enforcing the restrictions, as this will reduce the number of accounts available for misuse.

The restrictions should include:

1. Verification of status. Account applications should be referred to the relevant school administration for confirmation.
2. Expiry. Accounts should be disabled when the user leaves the school.
3. Monitoring. Logs should be analysed for patterns of misuse – e.g. simultaneous access from different locations.
4. Investigation and action. Violations should be investigated and appropriate action taken.

One interesting possibility is using Hongkong Post eCert as a login credential. This would make account application and subsequent login easier for existing eCert holders – the registration process could be simplified, and they would not have to remember *another* password to access the site. It would also simplify verification of status – the school could check the HKID number against their records and be sure that the user had the correct eCert. If an applicant using an eCert falsely claimed to be a teacher, pupil or parent, that would be obvious, and the digitally signed application would be strong evidence of their lie.

Discouragement

Awareness, Restriction and Traceability do not prevent misuse, so the objective of discouragement is to warn paedophiles that they will get caught with the intention of persuading them to choose not to use the resources. This will take the form of notices on Child Safety, stating that logs of downloads are kept and suspected misuse will be investigated etc. This will also reassure legitimate users that precautions are being taken. However, the notices should not contain details of the precautions that could be used to circumvent them.

Traceability

The objective of traceability is to facilitate investigations. This includes *features omitted for obscurity*. These could then be used in combination to trace those responsible for misuse. *features omitted for obscurity* kept as confidential as possible.

The Personal Data Privacy Ordinance should also be considered. *omitted* and linked user records constitute personal data, and must be handled in accordance with the law, including

considerations of security and data retention. The vast majority of records will be of entirely innocent actions. It is our opinion that child safety is more important that privacy, but ways should be sought to safeguard both.

Kaspersky Slams Symantec's Privacy Control

Kaspersky Lab, has released its latest analytical article, "Modern Security Suite solutions: methods for protecting confidential data" by Nikolay Grebennikov, deputy director of the Department of Innovative Technologies. The article examines how confidential data can be stolen, and methods used to protect such data.

The article takes the example of a well-known Trojan program, and examines the methods used by Norton360 and Kaspersky Internet Security 7.0 to protect confidential data from theft by the Trojan.

The author concludes that the most effective method for protecting confidential data is one that is based on analyzing application activity and tracking suspicious activity. According to Grebennikov, Kaspersky Internet Security 7.0 provides better protection for confidential data.

More Information

Modern Security Suite solutions: methods for protecting confidential data
Summary of Modern Security Suite solutions: methods for protecting confidential data

Hong Kong Police Smash eBay Fraud Gang

Hong Kong Police arrested eight suspects in pre-dawn raids of twenty premises on 26th July following investigations triggered by a complaint by eBay HK, several months ago. The gang are believed to have made HK$5 million by offering electronic goods on eBay that were never delivered.

Jenny Yip, eBay Communication Manager said, "Online fraud is an industry-wide problem globally. The industry is working hard to combat the problem." The gang made over 2000 transactions, many with customers from Britain and the United States. Senior Superintendent Man Chi-hung, of the Commercial Crime Bureau warned fraud "could happen anywhere and anytime in any corner of the world".

More Information

Police hold gang over eBay scam worth millions

BIND 9 DNS server Vulnerability and Patch Announced

Amit Klein, security researcher and CTO of Trusteer, has released details of a BIND 9 cache poisoning issue. The vulnerability makes pharming attacks feasible against unpatched BIND 9 caching DNS servers. Internet Systems Consortium Inc., the developers of BIND, have released BIND 9.4.1-P1, which fixes the problem.

All sites that utilise BIND are advised to upgrade.

More Information

Internet Systems Consortium, Inc.
BIND Vulnerabilities
BIND 9 DNS Cache Poisoning (Amit Klein)
SANS Internet Storm Center: BIND Updates Available
SANS Internet Storm Center BIND cache poisoning vulnerability details released

[US-CERT Vulnerability Note VU#252735 ISC BIND generates cryptographically weak DNS query IDs]
[US-CERT Vulnerability Note VU#187297 ISC BIND does not correctly set default access controls]
[Users urged to patch serious hole in BIND 9 DNS server]

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/