

Electronic litigation systems – a comparison of security issues between web-based litigation and traditional paper based methods

Pauline German

Abstract

This paper looks at the increasing use of web-based litigation management systems, particularly from the aspect of security. It compares them with the traditional paper-based systems. The author concludes that such systems have vulnerabilities that are not readily apparent and although technologies such as PKI go some way to address them, they are not the complete answer.

Introduction

Litigation-management systems are specialized forms of software that essentially “wrap” a computer database system. They can replace more traditional paper-based methods of document handling, including tasks such as storage, retrieval, modification and distribution. In Australia, these are primarily seen as a tool to aid legal professionals in discovery, but their ability to easily store and maintain differing types of documents, such as audio, video, spreadsheets and email, makes them a versatile tool for the handling of evidence at all levels; more so in the USA, this is expanding to include electronic filing/lodgement and presentation before the courts. This paper focuses on security aspects of the Australian experience, firstly providing an overview of computer database systems and their advantages. A comparison of the web-based litigation systems with the more traditional paper-based systems then follows. Finally some further security issues relating to computer systems in general are discussed.

An Overview of Computer Database and Management Systems

Document storage and retrieval can be accomplished via a myriad of technologies and systems, both electronic and physical. However, there are three broad levels of classification for these types of technologies:

1. the traditional usage of paper files (“hard-copy”), folders and filing cabinets;

2. the conversion of materials into electronic media and storage in computer files and folders; and,
3. conversion into electronic media, tagging and storage in a computer database.

Although they are more complex, modern computer databases offer several major advantages.

- Index generation allows fast (virtually instant) cross-referencing of material. This allows for the rapid searching of a document set or an entire database, something that may take hours with a simple (but large) set of computer files or even days in the case of physical hard-copy files.
- The storage of metadata (not to be confused with the inherent metadata within an electronic document), allows the filer to tag relevant information with each piece of data, automatic creation of specialized access and modification histories and generation of accounting information, if required.
- Concurrent access allows multiple users access to the same documents at the same time, and works in hand with some form of version-tracking to keep data modifications from different users valid and synchronized (the “data integrity” problem). Workflow bottlenecks due to one researcher having documents needed by another are hence removed. This is a huge advantage, allowing access from various (perhaps remote) sites simultaneously.
- The ability to set various access levels for different users allows an organization to manage who has rights to modify, view or delete data at a much finer level than through traditional systems. Access is available at all times the database is running¹.

As with all electronic systems, backup and restoration of documents is far more practical than with hard-copy storage, and can be virtually instant. Conversely however, the possibility of accidental data destruction is also greater, so the requirement for an effective backup system really is imperative².

Although it is possible (and in some cases desirable) to use an existing database product and have it customized in-house, there is a growing requirement for ready-made litigation-specific management systems, following the trend in the manufacturing, local government and administration sectors, where large amounts of highly specialised documents and diagrams are routinely handled. The benefits of these systems arise from the above-mentioned functionalities of

¹ Adelman, S., Moss, LT., & Abal, M., “Data Strategy”, 2005, Addison Wesley Professional

² ibid

the underlying database, combined with a graphical user interface that 'conceptually' makes sense to the legal professional, hiding the intricacies of information technology and the specialised semantics of database management from the user.

Litigation Management Technologies

The traditional litigation document management cycle involves:

- the lodgement of particulars with the court;
- the collection of relevant documentary evidence and communication of such to the other parties ("discovery");
- distribution and analysis of the documents by the legal team;
- the presentation of the documents in court; and,
- the archiving of the documents post-case.

Filing and Lodgement Security Issues

The activity of lodging claims and particulars with the court is overwhelmingly done in the traditional manner of personally getting the relevant documents typed up, physically signed by the relevant parties, taken to the particular court, stamped and filed. There are numerous security concerns that can be raised with such a model, but a hundred years or more of use has led to general acceptance of the system. On the face of it, there is no way for the court officer to verify that the signatories are who they purport to be; in the case of multiple copies for service to other parties, it is difficult (and time consuming) to verify that each is a faithful reproduction of the other, and there is opportunity for the tampering, loss, misplacement or destruction of the documents once lodged. Actual episodes of these examples appear rare however, and the system is no less secure than any financial or business transaction³.

Following the USA's experience, there are now several Australian courts that allow electronic filing of documents. For example, in Western Australia, r12(1) of the Magistrates Court (General Rules) has recently approved "eLodgement"⁴. This essentially removes the need to physically appear at the courts to lodge the documents. They are sent via the internet (through a web service) to the court

³ Judicial Conference 2001 [internet] URL: <http://www.usdoj.gov/criminal/cybercrime/commento.htm>.

⁴ eLodgement [Internet] URL: <http://www.magistratescourt.wa.gov.au/content/eLodgement>, accessed 19/08/06.

and an electronic receipt (or “stamp”) is returned as proof of lodgement. In the fully-realised system, the documents would then be electronically copied and filed, and could even be electronically sent to the relevant court officials. Service to other parties is still problematic; many people in the community do not have a web “presence”, that is they can not be found over the internet, and physical service of the copies is still required. However, there are still several advantages to this system:

1. Copying and backing-up of the documents is trivial.
2. Copies can be guaranteed to be exact (computer protocols such as MD5 checksum⁵ can be used to ensure a copy is a byte-for-byte replica of the original).
3. Transfer of documentation is instant.
4. All parties have equal access to the particular court’s system (distance and locality is no longer an issue).
5. Documents in the public domain can be easily made public by publishing them on the Web.

The last two points embraces the concept of “open justice”, allowing for fairer access to the court process and greater accountability. However, there is also the competing need for privacy, and the tension between the two has evoked much discussion. The US Judicial Conference in 2001⁶ noted that,

“Historically, a common law right has existed ‘to inspect and copy public records and documents, including judicial records and documents’⁷. Court records are presumptively open to the public for the express purpose of assuring that the public can monitor the integrity of the judicial system. That right is not to complete and unfettered access, but is a rebuttable presumption of openness. In the cases that discuss the right to public access, there is no declaration that access must be provided with state-of-the-art tools. Instead, the message is that where there is a determination that information should be available for review, access to the information should be provided.”

The commentators further noted that the traditional safeguards of the paper-based system were eliminated by things such as open internet access. The problems associated with having to physically attend court to view documents have a benefit, in that simple “trawling” for useful data is an impracticality. However, with open internet access, marketing companies for example, could easily access large amounts of data that could be used for “improper purposes”⁸.

⁵ Internet Engineering Taskforce RFC 1321 [Internet] URL: <http://tools.ietf.org/html/rfc1321>

⁶ Judicial Conference 2001 [internet] URL: <http://www.usdoj.gov/criminal/cybercrime/commento.htm>.

⁷ *Nixon v. Warner Communications Inc.*, 435 U.S. 589 (1978)

⁸ Judicial Conference 2001 [internet] URL: <http://www.usdoj.gov/criminal/cybercrime/commento.htm>.

There are, of course, several security issues with this system that need to be addressed in order to maintain public confidence. There is still the issue of signatories and their identity, and the electronic model does not really address this any better than has the traditional system. The Federal Court Rules allow for a “facsimile” of a signature to be attached to a document⁹ (an “image” of the signature is pasted onto the document), but this does not ensure the originality of the document, as it can just as easily be electronically removed or edited. Similarly, there is the additional problem of identifying who is lodging the documents. Although rarely done, in the traditional model the court official can ask for identification of the individual presenting the documents. But how is this done electronically?

The web service that receives the lodgement is normally a secured site, using the “https” URI scheme. This is similar to the familiar “http” (HyperText Transfer Protocol) used for most web sites, but is encrypted using SSL (Secure Socket Layer) technology. In both systems, there is the concept of a “server” machine and a “client” machine. The “https” encryption serves two purposes. Firstly, it requires the client to have a username and password that it recognizes, thereby identifying the client. Secondly it ensures that the data being transmitted cannot be easily read; it is encrypted using a 128 bit code¹⁰. However, there are problems with this. Most web browsers will store the username/password pairs. This is usually done automatically, by the browser and the service swapping “cookies” between them that identify certain aspects of the requested transaction. The cookie is stored by the browser on the client’s machine, ready for the next time the same request is made. Therefore anyone with access to the client machine and the user’s account could also access the service and although it uses a secure protocol, “https” does not guarantee that the server itself is secure, just the message. The server may have already been “hacked” or have other security issues.

There is also still the problem of data destruction. Ultimately, the documents are stored as data on a physical hard-drive attached to a computer. These drives can (and often do) fail. Because electronic data can be so easily copied, most institutions back-up their data, by copying them to another hard-drive (either on the same machine or a different one) or to storage tape¹¹. This in itself can be a security concern. However, if the data is entered into a data-management system rather than a simple file, it will have the advantage of not being in an open text format and therefore difficult to de-cypher¹².

⁹ Federal Court Rules FCR O41 R7 [Internet] URL: <http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrumentCompilation1.nsf>, accessed 21/08/06.

¹⁰ Shea, B., “Have You Locked the Castle Gate? Home and Small-Business Computer Security”, 2002, Addison Wesley Professional, IN.

¹¹ Stallings, W., “Data and Computer Communications”, 3rd Ed, 1991, Macmillan Publishing, NY

¹² Adelman, S., Moss, LT., & Abal, M., “Data Strategy”, 2005, Addison Wesley Professional

Electronic Discovery and Security Issues.

The concept and practice of discovery varies somewhat between the USA on the one hand, and Australia and the UK on the other. In the latter, there is an onus on each party to present, *a priori*, any relevant documentary evidence to the other parties, regardless of whether such documentation supports or counters the case being made¹³. In Australia, any documentary evidence that is not privileged is subject to discovery. The traditional paper-based system requires the researcher to sift through hard-copy documents, tapes or videos, determine their discovery status, physically file the documents and make copies for the other parties of those that are relevant and without privilege. Mistakes can often be made, and documents may inadvertently be left out of the copies to other parties, particularly when there are many documents, and many parties. Security concerns revolve mainly around who has physical access to the offices, filing cabinets and files.

The web-based system has several important advantages. Firstly, there are all the usual advantages of the electronic document model mentioned previously; copies are virtually instant and limitless, verification of copies is possible, and access is possible either remotely or locally.

One important advantage however, involves the types of documents being discovered. Increasingly, documents that can be used in evidence are originally created or stored by the witness or client in electronic format. Following the decision in *Sony Music Entertainment (Australia) Ltd v University of Tasmania*¹⁴, Australian courts define a broad range of types of electronic data as “documents”. Hence music files, electronic access logs, backup tapes, video or word processing data can all be considered “documents” for the purposes of discovery. These types of documents typically hold a lot of additional information. An example would be a Word document, produced with Microsoft’s ubiquitous “Office” software. These documents consist of two main components; the user data that is typed in by the user, and the metadata that is generated by the program. In many cases, there can be more content in the metadata than in the data itself. It may hold information on how and when the document was edited, what was changed, what sources were used or contributed, and what date and machine it was created on. Simple filing of a hard-copy of the document will lose the metadata, as it is generally hidden. However, using a computer-based litigation system to store the document will preserve it for further analysis. Another example is the filing of audio or video. Copying traditional tape sources can lead to rapid degradation. Again, more and more of this type of documentary evidence comes originally in digital format, and can be more easily filed and copied using a computer management system. As a final example, consider

¹³ “Is Digital Different? Electronic Disclosure and Discovery in Civil Litigation”, Kenneth J. Withers

¹⁴ (2003) 198 ALR 367

emails. These primarily exist as digital data, and again the metadata associated with them (time of creation/arrival, bcc'd list etc) can be as important as the data itself.

A second advantage relates to the fact that web-based systems are by definition accessible via the web, and rely on a computer database in the backend. Members of the research team involved in the discovery process need not be in the same physical location, and due to the database's concurrency management, several can access the same document at the same time.

Once the documents required for discovery have been established, the communication to the other parties can also be done electronically. Rather than physically handing over files and files of paper, a CD or DVD can be presented to the other party. However, the format of this data needs to be agreed upon first, as there are literally thousands of different formats for the electronic storage of text, audio and video. In Australia, Federal Court PN 17 requires the parties to agree to a format prior to commencement and provides guidance on the type and layout of data to use¹⁵.

However, along with these advantages, web-based systems raise new problems regarding security, and unlike the traditional paper model, these issues are not always as obvious.

As with any software product, the ability to securely deploy litigation management systems within a legal organization is of paramount importance. Systems that allow network or Internet access are generally far more at risk than isolated machines with no network connection. However, in terms of deliberate forced access, it should be noted that a properly maintained and well-secured software system is as safe as the traditional measures of a locked office and security alarms, maybe even more-so. Almost all "hacking" incidents have involved systems that have not applied basic security protocols. In this sense, these incidents are more "crimes of opportunity", rather than the public perception that computer systems are inherently "unsecurable". The problem is really one of identifying the risks, as they are not readily apparent to the average user, and ensuring that users comply with some basic principles. Unfortunately, this last point cannot really be enforced. As a broad description, computer security issues for systems such as litigation-management can be viewed at several levels.

The base level, and the most obvious area for concern, is local user-access to the actual program. Valid users of the service will have a username and password pair. Access to the management system cannot occur without a valid pair. Additionally, different users may only have access to certain parts of the system. However, there are the usual concerns with users writing down their

¹⁵ Federal Court practice notes [Internet] URL: http://www.fedcourt.gov.au/how/practice_notes_cj17.htm, accessed 22/08/06.

passwords, or using simplistic ones that can be easily guessed. User-education is the only way to overcome these issues.

Local user-access to the computer is another area where security needs to be reviewed. Again, access is via a username/password pair, which is reasonably secure, although one should note that Windows machines may have a “guest” account that has no password and could allow access. It does not follow however, that these particular username/password pairs are the same as those above for accessing the program. The computer may allow access to other sets of users for running other programs. So it is possible that, if the computer running the management program also hosts the data storage for the system, a knowledgeable user that has access to the computer (but not the actual program) could access the underlying data directly, without going through the program itself. Although this data is normally encrypted, it can still be a security issue, as the unauthorized user could copy the data to a private machine and attempt to de-encrypt it at their leisure. This is a greater risk with Windows-based machines, as there is no robust system of file ownership and access, as exists on Unix-based systems¹⁶. One solution is to have a dedicated machine solely for the database’s storage requirements. Such a machine would not allow normal users to log on.

Web access to the computer presents a different set of problems. If a computer has access to the Internet, it must be understood that in general, it is a two-way access point. That is, others on the Internet may have access back to the computer. This is more-so in the case where computers are left on and attached to the Internet indefinitely. Networks generally run a multitude of services on the one network (for instance, email services, web-browsers and news services all on the Internet), with each type of service communicating with a specific “port” on the computer. For traditional reasons, all ports on a computer (and there can be thousands of them) are open by default. The Internet Engineering Task Force (IETF) sets the standards required for services on the Web¹⁷, and which ports are for use by which services. “Firewalls” are dedicated pieces of software that control the opening or closing of ports and alternatively, which Internet addresses are allowed to use them. Unfortunately, many computers on the Internet do not run firewalls, or do not have them configured properly. Unauthorised access through a port can allow a user to compromise the security of the machine by running their own small programs remotely (such as spyware or key-loggers).

Web access to the actual service (or program) also needs to be secured. Users trying to access a computer-based litigation system via the web are required to identify themselves. This is generally accomplished via Public Key Infrastructure (PKI) encryption systems. These systems are based on a public key (held by the client and server) and a private key (held only by the client). Only the user’s

¹⁶ Shea, B., “Have You Locked the Castle Gate? Home and Small-Business Computer Security”, 2002, Addison Wesley Professional, IN.

¹⁷ Internet Engineering Task Force [Internet] URL: <http://www.ietf.org/overview.html>, accessed 22/08/06.

private key can “unlock” the public one and thereby authorize access. The format of these keys is again governed by the IETF, using a standard known as X.509, as set by the International Telecommunication Union¹⁸. The keys are signed by a “Certification Authority” (CA), which is an organization authorized to produce and distribute such digital keys. The Australian Partnership for Advanced Computing (APAC) is one such authority¹⁹. The user must be initially physically identified (normally using traditional “100” point personal identification methods) to a “Registration Authority” (RA) before the CA will issue the keys. These “keys” are digital messages that are practically unbreakable (without the use of a supercomputer), however the user’s private key can in theory be used by anyone, so must be kept hidden and secure. As it is stored on a computer (it is not practical to write it out), this means having a secure computer (password protected)²⁰. As an additional protection, the private key can be encoded with its own passphrase, that must be entered to use it. Unfortunately as most people find authentication an annoyance, the majority of users often leave this blank²¹.

Although not a direct security concern, there is also the issue of data formats. Noting that source documents may be in wildly different formats, and the requirement (as per Federal Court PN 17) for a “standard” format to be agreed upon between parties, care needs to be taken to ensure that any data - particularly metadata - is not lost or corrupted during conversion to the agreed-upon formats.

Additionally, the ease with which electronic documents can be copied can itself cause problems. Because of this characteristic, most electronic documents go through multiple phases of editing during the creation process, with each phase being saved. It may therefore be difficult to confirm that the document in possession is really the final version, and not one of a multitude of drafts. This is particularly so if the document was found through a computer search or other forensic means.

Court use and Archival Security Issues

The use of computer-based systems is increasingly seen in Australian courts, essentially to help manage electronic evidence. Due to its ease of production, the volume of electronic documentary evidence may dwarf anything seen in the more traditional paper system, and a database system is the only effective way to deal with such cases.

¹⁸ International Telecommunications Union Task Group [Internet] URL: <http://www.itu.int/ITU-T/studygroups/index.html>, accessed 20/08/06.

¹⁹ APACgrid Certification Authority [Internet] URL: <http://www.vpac.org/twiki/bin/view/APACgrid/CAInterface>, accessed 20/08/06.

²⁰ Ferreira, L., et al, “Introduction to Grid Computing with Globus”, 2nd Ed, 2003, IBM

²¹ Thorsteinson, P., & Ganesh, A., “.NET Security and Cryptography”, 2003, Prentice Hall, NJ

In such systems, the Court and the parties can all “plug-in” to the central electronic data repository (via laptops, for instance) and view the same data. Additionally, the Court may see other notes or precedents. As these systems are often wireless, they need to be firmly secured, so that outside parties cannot access the data. The same security concerns as outlined above, apply here; authentication of the relevant parties at login, access to the database and importantly, differing access rights depending on the user’s status. Establishing “levels of access” was an important recommendation by the US Department of Justice at the 2001 Judicial Conference, with differing public access and litigant levels being recommended for civil cases, criminal cases and bankruptcy cases²². PKI technologies used with electronic databases can address these issues.

At the conclusion of the case, documents need to be archived. In the traditional paper-based system, this essentially means storage in a filing cabinet within a lockable room. The central problem with this system is that there is only one copy of each document in the archive, and that paper documents cannot be “regenerated”. Accidental damage, for instance due to water ingress or fire, fading due to age or smudging (particularly fax documents) can result in catastrophic loss. Unauthorised access to the files can occur for years without anyone’s knowledge.

With an electronic archival system, some of these issues are alleviated (for instance, any access to the data is immediately logged), but there are also other concerns. Because copying electronic data is a trivial exercise, several copies of an archive can be made, and kept in different locations. This redundancy protects against physical damage to a particular computer or the room it is housed in. It also provides some defense against hard-drive failure, as noted above. Additional backup can be made to tape, or to optical storage such as DVD or CD. However, then these items themselves need to be physically stored, and the problem reverts to the same situation as that of the paper-based system. And although a lot more data may be stored on optical media, they generally have a much shorter lifespan than paper – around two to five years for a burned CD²³. Magnetic tape lasts far longer (up to 30 or more years), but is slow to access and takes up more storage room.

There is also the problem of redundant formats. Written language changes very little over time and so paper documents remain understandable for centuries. But this is not so for electronic data. The data format used when the documents were archived, may no longer be readily available - consider trying to read a document made in 1990 with WordPerfect with today’s software.

²² Judicial Conference 2001 [internet] URL: <http://www.usdoj.gov/criminal/cybercrime/commento.htm>.

²³ Digital Storage [Internet] URL: <http://computerworld.com/hardwaretopics/storage/story/0,10801,107607,00.html>, accessed 21/08/06

The archiver needs, therefore, to regenerate the data periodically, ensuring that it is readily available, and it is in the organization's best interests to do so. Although relief from discovery can be granted if the task would be too "burdensome", in cases such as *BT (Australasia) Pty Ltd v State of New South Wales & Anor*²⁴ and *NT Power Generation Pty Ltd v Power and Water Authority*²⁵, the cost associated with restoring difficult-to-access backup data (in the form of old emails) was not considered to be a valid point on which to grant relief.

Further Issues

The use of PKI key pairs greatly reduces the risk of unauthorized access to data and services, but it is not totally without risk. A CA-based security system requires a chain of events to occur before access is granted, and is therefore only as secure as the weakest link in that chain. And there are a lot of links.

In the PKI model, the CA issues a certificate, but the risk is really still with the verifying service – it cannot know how stringently a user was vetted prior to issuing the keys. Secondly, as mentioned previously, there is a need for users to keep their private keys secure. But these are normally stored on a normal desktop machine, probably with several other user accounts on it and possibly an internet connection as well. The private key then only becomes as secure as the machine it is stored on. PKI vendors in the USA have lobbied for laws that prevent you from repudiating your private key signing, regardless of who actually uses it. These have been enacted in states such as Utah and Washington²⁶. This is in stark contrast to phone or internet transactions involving a credit card, where under the MOTO (Mail Order/Telephone Order) rules (as agreed by UNCITRAL – the United Nations Commission on International Trade Law and outlined at the Internet Law and Policy Forum²⁷) the merchant must prove that the user was the legal owner of the card.

On the other end of the connection, the web-service machine doing the verification uses a public key, not a "secret" or private one. It typically holds a list of public keys²⁸. If the server machine is compromised, an attacker can add their own "public key" to the list and it will be accepted as legitimate, intercepting the client's request²⁹.

Even if all transactions between the user and the web-service are correctly authenticated, there are a myriad of "spyware" packages that can be discretely

²⁴ [1998] FCA 363

²⁵ [1999] FCA 1623.

²⁶ Utah Uniform Electronic Transactions Act 46-4-205 [Internet] URL:http://www.ie.state.ut.us/-code/TITLE46/htm/46_02012.htm, accessed 21/08/06

²⁷ Internet Law and Policy Forum [Internet] URL: http://www.ilpf.org/groups/analysis_IEDSII.htm, accessed 21/0/06.

²⁸ Thorsteinson, P., & Ganesh, A., ".NET Security and Cryptography", 2003, Prentice Hall, NJ

²⁹ Schneier, B., "Secrets and Lies: Digital Security in a Networked World", 2000, Wiley and Sons, NY.

installed on a computer that will capture the screen image, keystrokes and activity data³⁰. Imagine something like this on a courtroom machine, with a wireless connection so that it could send the captured information out unnoticed.

More esoteric technologies, such as the purported TEMPEST (Transient Electromagnetic Pulse Emanation Standard) program³¹, which can capture stray radiation from a computer monitor and re-create the image it is showing, are probably impossible to completely shield against. Thankfully, if such technology exists, it is only in the hands of a very privileged few. Other capture technologies however, are more pervasive. For instance, most laptops or PDAs have infra-red ports for wireless communication. They are often left on, even when not in use. There are several hand-held IR scanners available that can detect such ports, and with little effort another computer or PDA could be programmed to communicate with the unsuspecting machine. The moral is to turn off all services that are not in use on a computer. But this requires a level of knowledge that is generally beyond the average computer user.

Conclusions

There is no doubt that web-based litigation systems offer important advantages to the legal profession; ability to handle electronic evidence, ease of copying and storage, and preservation of metadata are just a few. There are, however, some equally important security concerns, some that can be addressed by technology, and some that require a particular behavioural change on behalf of the user. Unlike the traditional paper-based model, many of these are not immediately obvious.

PKI digital signing and authentication techniques certainly improve the security of web-based transactions. But the digital key they rely on is still a point of weakness. Like physical keys, they can be lost or damaged. And worse, they cannot be taken with you – they are left in the same place on the computer, and are therefore no more secure than the computer itself. Users can add a passphrase to their private key, but most implementations of PKI will allow a blank passphrase. Enforcing the use of a passphrase that had to comply to a minimum standard for numbers and characters would certainly remove most of the problem, but few people want to remember “one more” password.

From the web-service’s point of view, digital keys do not really provide a secure identification. There can be three users called “John Smith” who have a private/public key pair to the service, but the service cannot know which one it is serving, or if it is someone else entirely who is using the key³². The PKI

³⁰ Virtual Screen Spy, from www.soft32.com, is freely available.

³¹ Various described, but see Canada’s CSE departmental paper, “Network Security, Analysis and Implementation” at www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg1-e.html.

³² Schneier, B., “Secrets and Lies: Digital Security in a Networked World”, 2000, Wiley and Sons, NY.

researchers' original idea to maintain a "phonebook" mapping users to keys was never implemented³³.

Username and password authentication for both the computer and the web service is a useful security strategy, but not without limitations either. Many computers will allow logon without a password, and for web-services, the browser used to connect to the service will often retain the username and password first entered by the user. Again, few people want to remember a long list of username and password pairs (and because different web sites have different rules for what constitutes a valid name/password, it is often impossible to use a "favorite" one), so they generally see this as an advantage. However, if someone else manages to gain access to the computer whilst the valid user is logged on, they can simply access the service by using the stored information in the browser. A knowledgeable user could even copy this information to another machine, or USB stick. The solution again requires additional effort from the user, by configuring the browser not to store passwords. If there was a general standard for what constitutes a web password, it may be easier for users to use just one or two passwords, and so the task of remembering them would be a little less burdensome. Additionally, secure browsers could be configured to refuse cookies, or secure web-services could refuse to acknowledge them.

As it is apparent that web-based technologies for tasks such as litigation management are here to stay, it will be important to address these issues at an international standards level. User education on the security issues that are spawned by particular behaviours will be the most important step in this process.

³³ Ibid.

Bibliography

Adelman, S., Moss, LT., & Abal, M., "Data Strategy", 2005, Addison Wesley Professional, IN

APACgrid Certification Authority [Internet]

URL:<http://www.vpac.org/twiki/bin/view/APACgrid/CAInterface>, accessed 20/08/06.

BT (Australasia) Pty Ltd v State of New South Wales & Anor [1998] FCA 363

Caelli, W., "E-Security Information and Management and Archiving in the Private Sector" Paper to the Courts for the 21st Century: Public Access, Privacy and Security, Conference, QUT, 6 Nov 2003

Digital Storage Solutions [Internet]

URL:<http://computerworld.com/hardwaretopics/storage/story/0,10801,107607,00.html>, accessed 21/08/06.

Federal Court of Australia Practice Notes [Internet]

URL:http://www.fedcourt.gov.au/how/practice_notes_cj17.htm, accessed 22/08/06.

Federal Court of Australia Rules FCR O41 R7 [Internet]

URL:<http://www.comlaw.gov.au/comlaw/Legislation/LegislativeInstrumentCompilation1.nsf>, accessed 21/08/06.

Ferreira, L., et al, "Introduction to Grid Computing with Globus", 2nd Ed, 2003, IBM

Find Law Magazine "Find Law spoke with John Mathieson, District Registrar, and Philip Kellow, Deputy Registrar, about the Federal Court's encouragement of electronic discovery" (2003) [Internet] URL: <http://www.findlaw.com.au/magazine>

Find Law Magazine "How to Deal with 6,000 Discoverable Documents" (2003) [Internet]

URL: <http://www.findlaw.com.au/magazine>

International Telecommunications Union Task Group [Internet]

URL:<http://www.itu.int/ITU-T/studygroups/index.html>, accessed 20/08/06.

Internet Engineering Task Force [Internet] URL:<http://www.ietf.org/overview.html>, accessed 22/08/06.

Internet Engineering Taskforce RFC 1321 [Internet] URL:<http://tools.ietf.org/html/rfc1321>

Internet Law and Policy Forum [Internet]

URL:http://www.ilpf.org/groups/analysis_IEDSII.htm, accessed 21/0/06.

Judicial Conference 2001 [Internet]

URL:<http://www.usdoj.gov/criminal/cybercrime/commento.htm>.

Magistrates Court of WA eLodgement [Internet]
URL:<http://www.magistratescourt.wa.gov.au/content/eLodgement>, accessed 19/08/06.

McGrath, D., "Backup tapes: friend or foe?" in Insight, Clayton Utz, Undated

Network Security, Analysis and Implementation [Internet] URL:<http://www.cse-cst.gc.ca/publications/gov-pubs/itsg/mg1-e.html>.

Nixon v. Warner Communications Inc., 435 U.S. 589 (1978)

NT Power Generation Pty Ltd v Power and Water Authority [1999] FCA 1623.

Peterson, K., "Technology was a tactical weapon in litigation" (2006) in Find Law Magazine [Internet] URL: <http://www.findlaw.com.au/magazine>

Schneier, B., "Secrets and Lies: Digital Security in a Networked World", 2000, Wiley and Sons, NY.

Shea, B., "Have You Locked the Castle Gate? Home and Small-Business Computer Security", 2002, Addison Wesley Professional, IN.

Snyder, J A., and Morelock, A., "Electronic Data Discovery: Litigation Gold Mine or Nightmare?" JOURNAL OF THE MISSOURI BAR, Volume 58 - No. 1 - January-February 2002

Sony Music Entertainment (Australia) Ltd v University of Tasmania (2003) 198 ALR 367

Stallings, W., "Data and Computer Communications", 3rd Ed, 1991, Macmillan Publishing, NY

Stevens, S., "Using Computer Forensics to Manage Electronic Evidence" (2003) Technologies, Inc. [Internet] URL: <http://www.dataforensics.com>

Techno Lawyer Community "E-Discovery Increases Demand for Advanced Litigation Support Tools" (2003) [Internet] URL: <http://www.coredge.com>

Thorsteinson, P., & Ganesh, A., ".NET Security and Cryptography", 2003, Prentice Hall, NJ

Utah Uniform Electronic Transactions Act 46-4-205 at www.ie.state.ut.us/-code/TITLE46/htm/46_02012.htm, accessed 21/08/06

Withers, Kenneth J., "Is Digital Different? Electronic Disclosure and Discovery in Civil Litigation", undated