

# The Insider Threat to Medical Records: Has the Network Age Changed Anything?

Craig Valli

School of Computer and Information Science  
Edith Cowan University  
Mount Lawley WA, Australia

**Abstract** – *There is increasing pressure on medical practices to use digital information systems for storage of patient data. Some consideration is given to protecting these systems from a external or “ hacker” focus. This paper looks at the issue that the increasing use of digital information systems has for insider malfeasance.*

**Keywords:** insider, malfeasance, medical, practice, broadband, security

## 1 Introduction

In various nations of the world medical practitioners are being encouraged or forced into using computer based information systems for the storage, processing and transmission of medical records. Many of these records are being transmitted across the Internet and are often sent encapsulated as plaintext formats such as e-mail making interception of the medical information a relatively trivial task.

It is well documented in the computer security literature and surveys that insiders are a significant risk to systems integrity. The other alarming trend is that inside attacks are often the most successful and damaging in terms of money and loss of reputation. This is typically as a result of the insider having intimate operational knowledge that an outsider must either socially engineer and extract from the organization or bypass in the case of security countermeasures.

One of the prime motivators for moving to the ubiquitous use of medical records in digital form is cost and the quality of care delivered for the cost. Traditionally medical records have been kept as paper based indexes often with the filing compactors holding the records being the dominate feature within a medical practice.

These paper records were offline in the true sense of the word, if any one wanted to obtain the medical record one had to have physical access to the file storage device in this case a filing cabinet or compactor to obtain the file. Furthermore to take a copy of the file one then had either copy notes about the file to a notepad by hand or have

access to a photocopier or simply purloin it. Some of the problems intrinsic to copying the medical information in this manner is that unless the filer is organized it could be difficult or time consuming to locate information initially. If the information is not organized alphabetically or by incident, or uses chronological placement of information within the file locating the exact piece of information could take considerable time. The increased time makes the threat of discovery in commission of the breach escalate considerably. This means that such a breach is a high risk activity for commission by an outsider but is a profile well suited insider malfeasance. The insider however still runs the risk of discovery either in commissioning of the breach or egress of the information across the physical practice boundary.

There is little argument that a modern database centric information system, typically based on SQL, will garner significant cost savings and strategic advantage for an organization principally in timely delivery of information for legitimate purposes. Further, cost savings can be found in significantly reduced storage space required to house records. a standard 2m tall rack with a foot print of 0.25m<sup>2</sup> or 0.5m<sup>3</sup> can hold a server and several terabytes of storage space. This could replace several rooms of paper based storage realizing savings in reduced rental costs for floor space and given that many medical practices are located in high rental value areas this could be substantive. Records of this type normally have considerable periods for retention of the record that is mandated often via legislation.

Further advantage can be gained through the timely retrieval or interrogation of medical records from a database system. Little labour expense is now expended in the physical retrieval and re-storage of the record itself a further significant cost saving.

A counter to this is that speed of compromise and specific targeted attack for illegitimate purposes by an attacker is also likely to gain significant advantage through the use of digital systems on networks. With digital records several risk factors for the intruder in the compromise of a file are significantly reduced or even moot. This is further compounded if the internal network is connected to the Internet. The risk of covert retrieval, destruction,

modification or discovery of medical records is now significantly increased and some of this risk is co-incident risk. This is where the medical record for example is transmitted co-incidentally as a product of malicious activities and not as a specific target of an activity. In this scenario a mass mailing malware program that simply finds documents or existing emails on a hard disk and emails them to people within the address book could have devastating and real effects.

This paper will explore the issues the move towards medical information systems and their increasingly on-line interactions have for medical practitioners and the threat from insider malfeasance.

Many medical organizations are being as mentioned before being coerced or cajoled into installing IT based systems by governments or suppliers to replace paper based record systems with cost being touted as one of the main drivers. Little if any thought is often given to the security of that data at rest on the hard disk of the database server. Furthermore, now as other suppliers of medical diagnostics in the form of pathology tests, x-ray or ultrasound are generating their data in electronic forms they too for reasons of efficiency and costs savings are moving to electronic delivery of results. The fax machine is supplanted now with an email of results to the requesting health professional further extending the problem domain.

## **2 Infrastructure**

### **2.1 Networking and Servers**

Most medical information systems contain customized SQL database applications that run on specialized and dedicated server architectures. These databases are normally accessed by client PCs which are distributed across a network typically using Ethernet within the physical confines of the medical business. Furthermore, these networks are increasingly now being linked to the Internet typically via broadband connection such as ADSL with access speeds as high as 24Mbits per second.

The infrastructure described is relatively complex in computing terms and some exploration of the attendant risks for medical practices in particular will be undertaken in the following sections. Firstly, there is typically a SQL database server which contains the actual client databases which contain the digital records of the customers. These records not only record textual data but may also contain scans, diagnostic results and graphical images of patients. These databases need to be maintained, patched and secured against a large range of threats requiring highly specialised skills nearly always beyond the scope and capabilities of IT support mechanisms within medical practices. The SQL database engines themselves are

vulnerable to exploit and there are many documented instances of this on computer security sites such as CERT, AusCERT and vendor specific sites such as Microsoft or Oracle.

What further complicates the issue for many medical practices is that these medical applications are highly specialized in application and therefore they are generated often by boutique or specialist developers whose primary focus is the generation of a competent medical records system and not security. Hence, the applications themselves may contain serious security flaws or errors of logic resulting in exploit that could allow escalation of privilege either within the database or the underlying operating system. Many of these potential exploits due to the low profile of many of these companies may go undetected for considerable lengths of time.

SQL Servers are increasingly open to malicious attack in the form of SQL injection attacks [1-3]. These types of attack allow malicious users to inject or modify the data contained in a database structure from a Web-based interface that uses a scripting language such as PHP or Microsoft ASP to accept and pre-process input. These sort of attacks can be perpetrated by any individual with access to the scripting language either via a Web interface or a command line, allowing external or internal compromise.

Client access to the database systems will normally be done through a customized client interface often using Web technologies to enable it. It is also reasonable to assume because these systems are used in a trusted environment often they will have lower enforced security settings. The job function of a medical secretary is often to update notes and other annotations as directed by the medical practitioner. The ability to do this means, that a secretary must have high levels of access to the database, that in other systems typically they would not have such a high level of access.

### **2.2 Internet connection**

Many medical practices are now also being forced to use the Internet for communications and conduct of normal practice business. Diagnostic tests such as pathology and x-rays are increasingly corresponded in electronic formats. In addition many medical supply companies now have online ordering systems which are accessed across the Internet to effect the rendering of goods and services. In some cases doctors particularly specialists are using Web sites to promote their businesses and acquire customers. This now sees many medical practices using broadband technologies on a 24/7 basis exposing not only the connecting PC but potentially the entire medical information system to compromise.

Broadband connection itself brings many advantages to the user including increased speed of download and the ability to search and work faster for instance however, these same capabilities also work to aid an attacker. In the same way that a legitimate user using the system can download information up to 100 times faster than conventional analog modems so too can attackers send and receive at increased speeds[4]. The greater use of bandwidth across the Internet connection allows an attacker when internal or external to hide their attack within bigger data streams than is possible with conventional analog modems. What makes some medical practices high-value targets is the type of data they store such as before and after photography of cosmetic surgery for instance. Some other groups may also want to access patient medical histories for example before employing them or insuring them. It is far easier for a malicious insider to readily re-transmit this data at broadband speeds on the Internet than the conventional methods of physically accessing and duplicating the physical asset.

With many of these medical practices being small in size they typically will use personal firewall products which in some cases were found to be defective[5]. Fortunately, many of the new operating systems such as Windows XP Service Pack 2 and hardware devices such as ADSL routers have firewalls and other countermeasures turned on by default. However, most Internet-based countermeasures are typically externally focused and are not well suited to detecting insider malfeasance. With the introduction of broadband into these practices it will allow insiders for instance use personal data stores on the Internet to hide stolen data with little risk of detection.

It has been shown in previous studies that systems that are not regularly patched are susceptible to a wide range of attacks and this includes networking hardware. Many of these attacks allow for remote execution of code on the victim system an example of this is MS03-26 [6] whose vector of exploit is a specifically crafted TCP packet sent to the victim machine. The receipt of this packet on a vulnerable machine then allows for remote procedure calls (RPC) to be made to the victim machine from the attacker. RPC allows the execution of programs or utilities on the system for instance `format C: /del *.*` with impunity. Similarly insiders will have intimate knowledge of the patch level of systems and will be able to use suitable malware to attack the system. This would allow for possible remote compromise in non-business hours from a remote location such as a home based ADSL connection as the insider already knows the IP and the level of vulnerability in the system. So traditional scanning activities an outside attacker would have to perform is moot and compromise of the system is almost assured with insider knowledge.

As well as traditional viruses and worms there is the increasing use of targeted spyware programs[7]. Unlike conventional viruses and worms these spyware programs are specifically built to extract confidential data from systems such as passwords to then enable full compromise of the system at will. This emergent trend is worrying as unlike previous malware vectors its purpose is not wanton destruction of systems for fun but specific targeted activities for potential profit through theft or fraud. An insider can literally load these types of programs at will onto internal systems and have them report results to an external server for later collection and use or even internally to their computer.

### **2.3 Memory gone in a flash**

There has been massive expansion in the growth of flash memory technologies such as USB memory sticks, SD memory sticks, portable storage and playback devices such as IPOD, MP3 players. Staff in medical practice regularly bring these devices into their work environment with little if any observation or auditing of activity. Examples of the real threat that these devices pose will now be illustrated.

USB memory sticks can now be purchased that are 16 GB in raw storage capacity and are small enough to be readily concealable. Using text files and compressive technologies on such large memory sticks it is feasible to store up to 200 GB of raw data posing significant threats for protection of data. For example it could be possible to store all of the medical records from a sizeable practice on one stick using a simple SQL database ASCII text file dump routine that contains SQL queries and table constructs for the whole database. Similarly, saving all word processing documents in text format and storing them on the stick is possible. Detection of such activity would be beyond most medical practices and in fact many IT enabled enterprises.

USB memory devices allow for targeted extraction of information about patients on to the media for later transport beyond the organizational barrier and disclosure and distribution to others. One of the other major problems is a recognition that these devices are capable of carrying computer related data for example someone walking out of an organization which is iPod around the neck does not send the same signal as the same individual carrying a handful of CDs.

### **2.4 Tangible to Intransigent Data**

Governments and supplier organizations are pushing medical practices to move from paper-based records to digital records. This in itself is not an illogical objective and it has been proven in various case studies such as McKesson's Medical Supplies to enable significant

strategic benefit through the use of information technology. This change however, has taken away many of the organizational cues and clues to potential insider malfeasance. Previously for a patient record to be compromised typically the insider needed physical access to the storage system or location so that they could access the physical paper folder that contained the medical notes. To extract this information the insider had to either memorize, photocopy or note particularly relevant pieces of information. This process often required several attempts at extraction of the relevant information meaning that there were several instances of physical potentially seen activity that had to occur. Also, the diversity of media often found in the physical file, everything from handwritten notes, type letters, type notes and photographic x-ray film made total atomic compromise virtually infeasible.

The increasingly digital nature of the data stored on medical systems expunges many of these visual and physical cues that insiders would have to risk to obtain the relevant charter. Furthermore, the increasingly monolithic nature of these medical databases i.e. they store everything in digitally accessible forms in one record or patient instance, makes theft, destruction or compromise of this data significantly easier.

Another attack vector that was not possible or hard to achieve with paper-based records, is that of alteration. For instance, it is a reasonably difficult process to modify an x-ray film, however, for its digital equivalent it is not. Likewise alteration of digital test results is a relatively trivial task as many of these are sent as e-mail which are often saved as text files which can be readily manipulated.

### 3 Remedies

It is inevitable that medical systems will become IT based and appropriate risk methodologies and responses must be developed to protect these systems. Many of the systems used in practices have parallels with out SOHO based businesses and much of the existing literature in this area can be leveraged to support development of best practices in this area. Recent work by Williams [8] is looking at developing risk assessment methods for medical practices and this will aid in addressing these issues. There are however, some basic security steps that can be undertaken to protect data both in transit and at rest from insider malfeasance for minimal or low cost.

Encryption technologies can assist greatly in protecting data in transit and at rest. Firstly, in transit the use of SSL tunnels or enabled services such as email (POP3S, IMAPS) or web (https) prevents compromise in transit. Secondly the use of operating system enabled encryption such as Encrypting File System (EFS) in Microsoft operating

systems makes compromise of data more difficult for any attacker. EFS uses per user encryption meaning that several users can use the same PC or server and not be able to access each others files except through a direct login using the other users credentials. Finally the use of an at rest data encryption tool such as a Silicon Data Vault or Seagate (Drive) will further protect data from insider malfeasance.

Standard Operating Environment (SOE) development, securing and restriction of same can alleviate many problems by denying avenues for malfeasance. As an example Windows XP SP2 now allows for policy based restrictions to be placed on the USB ports of the machine disallowing connection of USB based devices. The enforcement of EFS via policy is also possible adding further barriers to insider malfeasance.

Auditing technologies likewise will at least alert to insider access of materials. Nearly all network operating systems all for extensive auditing of file access on server platforms. SQL servers have extensive logging and auditing capabilities that can be used to track down to field level within a record who has accessed or altered content. This nearly always requires specialist setup but have various easy to use tools to alert an administrator or business owner of unusual activity.

The use of file integrity checkers such as Tripwire which computes MD5 checksum hashes of files and notifies when there are changes to files could also be very useful. These integrity checkers can also be employed at PC level to detect the installation of malware and spyware.

Monitoring of Internet usage is a simple and effective tool that is often neglected. Tracking a users browsing or email habits can show if a users activity has become abnormal i.e. they have recently been sending multi-megabyte files to a external email address or their outbound web activity has increased significantly all of these are indicators of possible malicious activity by insiders.

The use of firewalls, anti-virus and spyware checkers should be mandatory as should their updates. A review or audit of these periodically will also potentially indicate where insiders have changed configurations or allowed activities that are not allowed such as opening the firewall to allow file transfer, file sharing or chat clients access to the Internet. This are again indicators of potential insider threat either by accident or intent. Some of these changes can also be as a result of social engineering attacks perpetrated by chain emails.

## 4 Conclusion

The move to digital records for medical data has significantly changed the threat landscape for compromise by insiders. Many vendors are well aware of external threats but often are lax or discounting of the threat that insiders pose when developing or selling product. Digitized medical artifacts are far easier to intercept, manipulate, destroy or transmit than their physical paper or film counterparts. However, some simple steps can be taken to mitigate against internal threats which also have the bonus of hardening the systems to external attack. Many of the suggested changes to systems come at little for no extra expense to the system owner.

Most crimes are as a result of knowledge motive and opportunity. Knowledge for insiders to glean useful information as a result of digitization is lowered no longer does the insider have to make a determination of what notes are relevant they simply copy and transmit the entire monolithic record. Opportunity is greatly increased as a high speed conduit is now available to transmit the data on or an easy concealable storage device has the capacity to hold all data needed. Furthermore, the opportunity to be caught doing this is greatly decreased unless appropriate steps have been taken to internally secure the data store. Motivation or lack thereof is all too readily overcome with disparate proportioned cash incentives.

Urgent research needs to be conducted in this area to identify suitable methods and frameworks to enable SOHO or small medical practices to better protect patient records.

Finally, next time you are at your doctors and they are happily typing in your details on their system ask them politely how they secure your information from compromise by staff or external attackers.

## 5 References

- [1] C. Anley, "Advanced SQL injection in SQL Server applications.," 2002.
- [2] J. deJong, "Top Ten, Other Lists Catalog Security Threats," in *Software Development Times*, 2005, pp. 5.
- [3] R. Kwon, "Is Your Web Site at Risk of Injection?," *Baseline*, vol. 2, pp. 108, 2002.
- [4] C. Valli, "With Speed the Hacker Cometh," presented at 2002 Australian Information Warfare and Security Conference, Perth, 2002.
- [5] J. Yee, "Firewall or FireFolly - An initial investigation into the effectiveness of Personal Firewalls in securing personal computers from attack," presented at 2002 Australian Information Warfare and Security Conference, Perth, Western Australia, 2002.
- [6] Microsoft, "Microsoft Security Bulletin MS03-026 - Buffer Overrun In RPC Interface Could Allow Code Execution (823980)," vol. 2006: Microsoft, 2003.
- [7] F. C. Freiling, T. Holz, and G. Wicherski, "Botnet Tracking: Exploring a Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks," vol. 2006, 2005.
- [8] P. A. H. Williams, "The Underestimation of Threats to Patient Data in Clinical Practice," presented at 3rd Australian Information Security Management Conference, Perth, Western Australia, 2005.