Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 7 (2012) pp. 355-365

Cyber Security and Portability of Electronic Medical Records

Daniel E. Burgner, Luay A. Wahsheh, Jonathan M. Graham, and George Hsieh

Department of Computer Science, Norfolk State University,
700 Park Avenue, Norfolk, Virginia 23504, USA
d.e.burgner@spartans.nsu.edu, {law, jmgraham, ghsieh}@nsu.edu

Abstract: **The recent healthcare debate has thrust the healthcare system in the spotlight. One aspect of the healthcare system is the medical records themselves. The biggest difficulty in accessing patients' electronic medical records (EMRs) is a lack of uniformity related to healthcare data, specifically the format in which this data is stored. In this paper, we propose PortableEMR (PEMR), a secure, portable EMR system that works with established EMR standards. This system uses a secure personal token (SPT) that carries a patient's EMR that is encrypted in a Pretty Good Privacy (PGP) file. The patient's EMR includes: a digitally-signed EMR written in Extensible Markup Language (XML), digital signatures of the patient and the practitioners modifying the EMR file, and related legal and medical files to the patient's EMR. The PEMR system results in a user-friendly system that is easy to use by healthcare providers and patients alike.**

Keywords: Electronic medical records, Security, Portability, HIPAA, XML.

I. Introduction

This paper provides necessary information regarding the use of electronic medical record (EMR) systems and the need for security and privacy. We offer security issues and solutions involving EMRs. EMR systems are governed by rules used to manage resources (in this case, patient medical records) or to define a direction that leads to current and future decisions (in this case, the information gathered on a patient can be used to determine a treatment plan). Based on the very nature of the records involved in this process, mandatory compliance with regulations involving EMRs is required. These regulations have to define what information and resources have to be protected. In this instance, the information and resources would be a patient's personal information and medical history. Security regulations have to define how to protect this information and why it needs to be protected. In some cases, a combination of what/how/why would need to be used for some of the data involved. Security in the context of EMR systems refers to keeping healthcare information secure by using any means necessary to prevent these systems from being compromised. Privacy in the context of EMR systems refers to keeping healthcare information of patients private and that only those who have a need to know be allowed access to this information.

EMR systems were thrust into the spotlight a few years ago when President George W. Bush mandated that all American citizens have access to their EMRs by 2014. President Barack Obama reinforced that commitment to this target by allocating $20 billion over the next five years to help healthcare providers implement digital record systems [1]. Complicating matters is complying with federal and state privacy regulations aimed at making these systems secure. This problem is not confined to the United States alone as Canada, Australia, New Zealand, and European countries all have EMR systems. In every case, these countries have nationalized healthcare systems. Security and privacy risks have been multiplied through the use of Internet applications that medical applications access, which is an obstacle the deployment of EMR systems. A gap exists between data privacy requirements and functionalities of existing EMR systems [2].

The biggest difficulty with EMR systems is a lack of standards formally adopted by The Joint Commission (JCAHO) and the National Integrated Accreditation for Healthcare Organizations (NIAHO). Multiple vendors offer EMR products, but the standards of each vary from product to product [1]. EMRs written in one format may not be compatible with other EMR systems. This paper investigates authentication methods such as passwords, biometrics, and radio frequency identification (RFID) readers and recommends the implementation of the PortableEMR (PEMR) system on a secure personal token (SPT) that would work with established EMR standards and can be integrated with an EMR system operated by a medical facility, with the SPT carrying a patient's EMR encrypted in a Pretty Good Privacy (PGP) file. The patient's EMR would be written as an Extensible Markup Language (XML) file that would be read by a Java graphical user interface and would link to files that are a part of the patient's EMR, such as: prescriptions, treatment records, and appointments. Healthcare providers and patients benefit from PEMR by having an easy to use EMR system that would work with existing EMR standards. The patient's EMR archive file (see Figure 1) would include: a digitally-signed EMR written in XML, digital signatures of the patient and the practitioners, and related legal and medical files to the patient's EMR. The next five sections will cover federal and state legislation specific to EMRs, security issues, related work, Universal Serial Bus (USB) medical products along with an introduction to the PortableEMR system and how the PortableEMR system works.

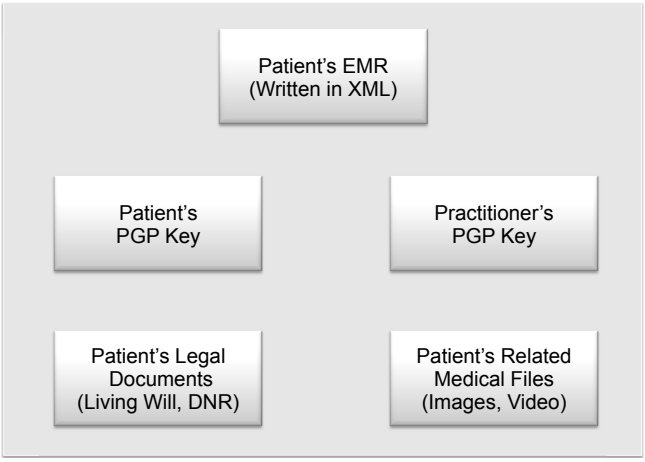

Figure. 1: Patient's EMR archive file.

II. Federal and State Legislation

This paper provides information on United States and state legislation passed into law or currently being offered for consideration. It also discusses the Health Insurance Portability and Accountability Act (HIPAA) as well as concerns and legislation from Congressmen regarding EMR systems.

A. State Legislation in California

Legislation on a state and federal level is being introduced and, in some cases, passed that affects EMR systems. California recently passed legislation extending its data breach notification laws to include incidents centering on electronic health insurance and medical information. Its legislation includes medical and health insurance information as personal information. Application of the Confidentiality of Medical Information Act is expanded to include businesses that maintain medical information. Unencrypted medical and health insurance information is also included in the legislation. These new provisions apply not only to healthcare providers, but also employers and entities that possess computerized health data as well as computerized employee data [3].

B. HIPAA

In the United States, we have HIPAA, which is a stringent set of laws and regulations for healthcare providers. In addition, Congress has written legislation that addresses the creation of an electronic medical records system. The downside to a majority of this legislation is the absence of a "right to consent", the right for patients to control who can access and use their medical records. These bills depend on the privacy standards set forth in the HIPAA Amended Privacy Rule, but the right to consent was stripped by the Department of Health and Human Services in 2003 through amendments to the HIPAA Privacy Rule. Patient privacy no longer exists as over 600,000 businesses can currently see and use Americans' medical records without their knowledge, consent, or compliance [4].

C. Congressional Concerns

More recently, members of Congress wrote a letter to Health and Human Services Secretary Kathleen Sebelius regarding interpretations by the Department of Health and Human Services (HHS) that require notification of individuals in the event of unauthorized disclosure of personal health information. The letter states that the American Recovery and Reinvestment Act of 2009 allows for provisions promoting health information technology as a means for improvements in the United States healthcare system. The benefits can only be realized with safeguards in place protecting the security and privacy of individuals' health information. The HHS' interim final rule interprets "compromise" to include a substantial harm standard. The members of Congress request that HHS revise or remove the harm standard set in its interim final rule [5].

Congressman Ron Paul introduced a bill entitled "The Protect Patients and Physicians Privacy Act" on May 21, 2009. The bill would give Americans the ability to opt out of any healthcare information system mandated, created or funded by the United States Government. In addition, it would repeal unique health identifiers as well as not allow any electronic medical record in a federally-funded database to be shared with another healthcare provider without the informed consent from the patient unless it is in the case of a medical emergency. It also prohibits any health information from an individual's medical records to be placed in a federally-funded database without the informed consent of the patient. It allows for provider freedom from required participation in a federal healthcare program by not requiring a healthcare provider to participate in such a program. It also states that no healthcare provider shall be denied participation in a federal healthcare program resulting from refusal to participate in a federally-funded database [6].

III. Security Issues

This paper provides information on security issues related to EMR systems. It also provides information on access control and the effects of security issues on these systems if security procedures are not followed.

A. Security Issues Related to EMR Systems

Security issues involving EMRs would address security issues such as confidentiality, integrity, and availability [7]. Confidentiality refers to the preservation of authorized restrictions on disclosure and information access with unauthorized disclosure of information constituting a loss of confidentiality [8]. Confidentiality includes: data confidentiality, which is assuring that private or confidential information is not disclosed or made available to unauthorized personnel, and privacy, which assures that individuals control or influence what information related may be collected or stored as well as by whom and to whom this information is disclosed. Integrity refers to checking against improper modification or destruction by ensuring information non-repudiation and authenticity [8]. Specifically, we refer to data integrity, which assures that information and programs are changed only in a specified and authorized manner, and system integrity, referring to a system performing its intended functions unim-

paired, free from unauthorized manipulation of the system. Availability refers to a system working promptly with no denial of service to authorized users [8]. This involves having an EMR system available for timely and reliable access with its disruption to and use of information or an EMR system constituting a loss of availability. For an EMR system, these policy rules, when implemented, correctly guarantee the transmission of patient medical records securely between entities. These entities include all sources, destinations, and intermediaries through which all patient information can flow (patient, physician, nurse, hospital, clinic, pharmacy, government agency, insurance company, researcher, computer system, just to name a few).

B. Access Control

A critical aspect of medical systems' security is access control. Access control rights specify who is allowed to access an entity and what he or she can do with the information located inside the entity (read or write) once he or she has access to this information. Access control is usually divided between multiple control entities: mandatory access control (MAC), discretionary access control (DAC), and role-based access control (RBAC). MAC is widely used in multi-level systems having sensitive data (similar to what is used in the military). They involve different security levels used to classify the information in the system. In an EMR system, the highest level of classification is reserved for records of patients that have deadly diseases (e.g., AIDS, cancer). The next highest level of classification belongs to general medical information (e.g., medications, non-life threatening illnesses), while the lower levels of classification are usually reserved for accounting information (e.g., financial, insurance company) and basic information (name, gender, address). DAC provides the owner entity the authority to allow or deny access to an entity and what type of access these entities could have if he or she has access. RBAC allows the use of roles to define access to the system and the rules regarding what access is allowed to entities that are assigned roles in this system.

C. Effects of Security on EMR Systems

When dealing with security, it is a matter of risk management when one has to balance the security costs of the system (electronic medical records) against the loss of breaches (electronic medical information being compromised). Losses involve the instances of breaches combined with the expenses associated with addressing these issues. Security costs involve budgeting for firewalls, software, and technical support for the time users spend resetting their accounts and addressing warnings. Both of these costs are hard to measure. In the final analysis, security is an economic issue since all parties involved are drawn to perceived incentives [9].

IV. Related Work

This paper provides the evolution of EMR systems. It discusses suggested changes, privacy concerns, and authentication methods, including those specially designed for EMR systems.

A. Evolution of EMR Systems

For many years, elements of an EMR have been computerized. These elements include the administrative and the financial portions. They have evolved to include laboratory results coming from automated testing equipment for laboratory specimens as well as word processing transcriptions from clinicians' dictations. Most EMRs have data dictionaries that define the content as well as date and time stamps of all data. This makes the patient's healthcare record become a chronological record. The advent of EMRs presents their own challenges. These include: increased provider time, computer down time, lack of standards, and threats to confidentiality. Electronic order entry in earlier studies indicates that entering orders into the system increased. Computer down time is another concern in that not having the right piece of information at the right time is real but this is mitigated by advancing computer technology. A lack of standards to interchange information is real since a consensus is lacking regarding patient signs and symptoms, radiology, test interpretation, and other procedure codes. Finally, threats to confidentiality are an issue simply because of the very nature of the information contained in an EMR. Procedures such as using a key card, confidentiality agreements as well as implementing an audit trail can help in the process while legislation would have to be passed that makes an EMR usable but keeps the patient's privacy protected [10].

In 1997, the Boston Electronic Medical Record Collaborative began work on developing a system that uses the World Wide Web as a means to transmit patient data to clinicians working in emergency departments. It involves a protocol that makes transmission of data possible through electronically identifying patients and providers, securing permission to release records as well as the tracking of data being transmitted. This system will use information with identifiers removed until confidentiality methods are sufficient and appropriate. Regarding confidentiality, a patient's consent is needed before access to a record is granted. Should the patient explicitly state that his or her record should not be released over the web, it will not be accessible on the web even in an emergency. The system allows for methods of authentication such that the request for information originates from a known source, the recipient provider provides a username as well as a secure password to the reporting institution [11].

B. Suggested Changes

It has been suggested that EMRs be designed to support the exchange of all data according to public standards. One must also consider the privacy implications that are involved in this matter. For this reason, it has also been suggested that patients should be granted control over who can access their record. This would be a key factor to ensure a patient's record is accessible yet remains private. Complicating matters is a situation where this medical data being used for unregulated uses. A serious concern is that the companies involved want to own the medical data their systems maintain [12]. One solution would be to enact legislation addressing this issue.

C. Privacy Concerns

Privacy concerns have additional issues with EMRs since existing legislation was written before these systems came into being. State privacy laws vary from state to state, making it difficult to design an EMR system that would be compliant with all privacy laws related to health data. In the European Union, where electronic medical records are more widespread, its citizens are granted ownership to their medical data. This is not addressed by HIPAA but it does allow patients to access their own data. Healthcare delivery is another privacy issue since one needs to determine who has the ability to access the data. Should a patient be sent into the emergency room, this timing is critical since the providers are dealing with life or death issues [1]. One potential solution is to amend HIPAA to include data ownership for patients.
In summary, the tools needed for the protection and safeguarding of healthcare information systems are available for use. It does a company no good if these tools are not implemented. It is imperative that the highest levels of a healthcare organization be familiar with security measures needed to ensure the security of EMR systems. As an organization's reliance on information systems grows, this results in the potential of financial loss and compromise of patient confidentiality. When an organization prepares plans for the design and construction of a healthcare information system, it must take into consideration the importance of including security measures as well as being compliant with existing laws [13].

D. EMR Standards

Standards have been developed to address multiple issues regarding EMRs. One such standard is from the Health Level Seven (HL7) organization. Its structure is built upon the foundation provided by XML and is structured specifically for medical-specific information [14]. This integration approach is dependent on a defined data model that is pragmatic and allows for the achievement of data integration. Interoperability is not possible through HL7 but through acceptable integration costs it accomplishes much. It is being rapidly adopted in the United States, primarily through the benefits that are achieved through this approach [15]. Another standard specific to EMRs is the Digital Imaging and Communications in Medicine (DICOM), best suited for the domain of clinical medical imaging. It accomplishes its tasks by storing their pixels as two-dimensional (2D) slices but it also incorporates MPEG2 for video-based imagery, which is important since MPEG2 is suitable for many applications [16]. The only and possibly the first nationwide EMR system in the United States is the Veterans Health Information Systems and Technology Architecture (VistA), currently used by the Veterans Health Administration (VHA). It is based upon Bidirectional Health Information Exchange (BHIO), a set of protocols utilizing peer-to-peer transmission of large amounts of related healthcare information. It is developed in accordance with HL7.

E. Authentication Methods

A variety of authentication methods are used for access control to a number of resources. The simplest method is the password-based authentication method. This method would involve a user typing in a username and a password. Passwords can easily be forgotten or worse, someone who needs access to the system during a critical time would not be allowed in since his or her account may not have been set up. Another method of authentication is biometrics, in which non-behavioral features such as fingerprints and face geometry are used to verify a user's identity. These features are easily available, requiring no action from the user [17]. Fingerprint biometrics is a common authentication method since users do not need to bring anything else with them for them to use the system. The drawbacks involved include: having the finger placed in a proper position; perspiration, heat and cold; and fingerprints being damaged by injuries. Each of these factors can affect how this system can work [18].
The use of smart cards is another means of authentication in that they hold a wealth of information such as a virtual medical record file, security services to include authentication and access control and event notification to provide interfaces to EMR systems. XML can be used as a mark-up language since it can be used with application-specific tags to facilitate processing by an EMR system. XML would be best suited since it can work with HL7, which has structures built on XML [14].
An RFID reader is another method for authentication in that a user can swipe his or her badge through a reader and provide a password. Users could forget their employee badge, which would result in a temporary badge being issued for the day. These badges can be associated with their accounts and could include a common backup method asking a user a series of pre-answered questions. Should the user answer correctly with his or her login information, the user can have access for that day. Equally important is the proper tracking of these events for documentation of malicious behavior [18].

F. Applications of Authentication Methods in EMR systems

A number of authentication methods are currently being used in EMR systems. Some methods may also include authorization in their approach to authentication. One such method allows for policy-driven authorization that incorporates role-based and privilege-based policies for the electronic health service system. In addition, the authentication method is a two-pronged approach involving fingerprint biometrics and a digital personal identification number (PIN). Once successful, the users will gain access to their system [19].
Another two-pronged approach to authentication involves using a user/password with no restrictions on the passwords along with an RFID reader since it was a better choice as opposed to using fingerprint biometrics since employees in the healthcare field use gloves, which would prevent them from using a fingerprint reader. Physicians also suggested that they were not in favor of using fingerprints and wanted something easier to use [18].
Another authentication method, MASPortal, is used for home healthcare applications by using a multi-layered infrastructure using access control and authentication services. MASPortal uses Medical Advice Service, which performs a medical condition assessment for a given patient context and a knowledge base containing a diagnosis based on listed symptoms. MASPortal uses a Lightweight Directory Ac-

cess Protocol (LDAP) directory service and a Grid Security Infrastructure (GSI) authentication mechanism that handles the authentication process. LDAP provides user/password access for authentication of users to MASPortal while GSI uses Grid authentication, which defines single sign-in algorithms and protocols that include cross-domain authentication and temporary or proxy credentials [20].
One authentication method involves gaining access to EMRs on wireless phones. Multiple methods are used to gain access, which includes: a password supplied by the EMR's owner, a share used solely by paramedics, biometrics involving the owner's face geometry and fingerprint, and a special authorization process when all other methods have failed. In the case of the special authorization process, the user stores a special key and an encryption of this share on his or her wireless phone. This key and share would be unique only to the user and may not be used to access another user's EMR. Personnel who use this approach would have to contact the authority involved in creating this share to let them know that this method was used so that a new key pair can be generated with its encryption being updated to reflect the change. The share for an emergency medical technician (EMT) would allow for an EMT to have his or her key pair along with its encryption issued by a regional health information organization with the EMT's key pair being unique only to the EMT [17].
Another authentication method involves using a Communication Virtual Machine (CVM) to enforce security and privacy by enabling logging and authentication, to name a few. This CVM would negotiate the involved parties' capabilities and underlying networks to guarantee presentation compatibility as well as quality of service. The CVM would be a part of an exchange that would generate EMRs independent of existing healthcare applications. Each institution would have a medical mediator that would generate a virtual medical record with a unique patient identifier. This virtual medical record will describe the items in an EMR and are built at the discretion of the institution. Each institution also has a copy of a CVM, which does the efficient, online and secure transfer and presentation of virtual medical records [21].

G. XML Encryption

Released in 2002 as a proposed World Wide Web Consortium (W3C) recommendation, the XML encryption specification provides for processing rules and syntax for digital signatures [22]. Specifically, it specifies the steps needed to encrypt and decrypt data as well as the XML syntax to represent encrypted data and information to decrypt this data. XML elements, XML element content and arbitrary data can have encryption applied to this data. Encrypted data is represented as an EncryptedData element with prefixes "e" and "ds" being associated with Uniform Resource Identifier (URI) references of namespaces belonging to XML Encryption and XML Signatures, respectively. The steps involved to encrypt data are as follows: select the algorithm and parameters; obtain the key; encrypt the data; construct an EncryptedData element and return the EncryptedData element. Should the key be encrypted, an EncryptedKey element should be built with these steps applied recursively. This sequence of steps is applicable for all encryptable data items. The steps for decrypting the data are: identify the algorithm, parameters and KeyInfo element; locate the key according to the KeyInfo element; decrypt data in CipherData element and return the decrypted data. If the EncryptedData element needs to be replaced, the decrypted data will be its replacement [23].
The XML encryption specification also specifies a confidentiality mechanism for XML. User data such as complete XML documents, single elements inside an XML document, the elements' contents inside an XML document (this also includes descendants as well as some or all child nodes) and arbitrary binary contents are outside an XML document. Granularity levels allowed are the encryption of full subtrees (single element and all descendants) and sequences of subtrees (subtrees can be single nodes like text nodes or mixed sequence of comments, elements, text, and processing instructions). Should elements be included, its descendants are also included in the encryption process [24].

H. XML Authentication

The use of XML is increasing and has become a choice format for publication of information over the Internet in various venues such as government, healthcare, and finance, where integrity of the information is a priority. Servers processing queries certify answers by digitally signing them with an online private key. Such an approach could be vulnerable to hacking as well as insider attacks. Devanbu et al. [25] suggest using untrusted servers to answer certain path queries and selection queries over XML documents, eliminating the need for a trusted online signing key, which provides for security and scalability of publishing information in XML on the Internet [25].
Another authentication method for XML involves the use of refreshable tokens. Refreshable tokens are an expansion of an offline electronic cash scheme. A coin would include the privacy information of the user, the key to the user's identification. When the system is refreshed, a new coin containing the same information is created. This means that anyone can compute the user's identity from a double usage of the same coin. The scheme has the characteristics of unlinkability (no one would be able to determine if two tokens are related to the same user), unforgeability (for N tokens, no adversary would be able to compute $N + 1$ tokens in computer polynomial time) and double use traceability (an organization would be able to compute a user's identification if same token is used twice). Two aspects of security definitions are parallel-aspect and refresh-aspect. Parallel-aspect is a means in which a user is allowed to use and hold multiple tokens at one time for a single service since the user can be given services parallel. Refresh-aspect involves passing the information to another token when the token is refreshed [26].

I. Relevance

The PEMR system being proposed writes an EMR in XML using a username and password authentication method. This system will facilitate encryption using PGP.

V. USB Medical Products

This paper provides information on current USB medical products. This includes information on their drawbacks as

well as the introduction of the PEMR system we are proposing.

A. USB Medical Bracelets

A medical bracelet has been around for many years. It ranged from a tag giving no more than a name, address and a phone number of an emergency contact to a small USB drive carrying personal medical information of the owner with a separate card authorizing care to a practitioner in case of an emergency. The problem with these products is that a tag does not carry information about medications, allergies, and medical conditions and that a card could get separated from its owner. Other issues involving USB medical bracelets include integration of the device into an EMR system and workability with established EMR standards.

One product available commercially is the CARE Medical History Bracelet. It is billed as the world's first EMR bracelet that can be plugged into a PC or a Macintosh compatible computer. It claims that no special software is needed to view one's emergency information. Personal profile data on the bracelet is the patient's medical-history and is stored in a read-only HyperText Markup Language (HTML) format [27]. This is different from the system we are proposing since it does not allow for the data to be encrypted and that the EMR files for the system we are proposing is written in XML.

Another product available commercially is MedicTag. It is billed as the original USB medical alert tag designed for emergency medical information. It comes with a template form for a patient to fill out his or her information which is then saved to the bracelet. It also requires Microsoft Word since the documents would be saved in Word format. MedicTag also has a switch that enables the bracelet to be "read-only", meaning that files would not be saved if the device was in "read-only" [28]. This is different from the system we are proposing since we would be saving our EMR files in XML format and that MedicTag does not have a means for encryption while our system does.

Another product available commercially is the EMR Medi-Chip USB Flash Drive. It also comes with a comprehensive template form for a patient to fill out. It does allow for password-protection of certain information with 256-bit Advanced Encryption Standard (AES) encryption. Patients would be able to read and review relevant medical information as well as the patient's medical providers, first responders and emergency room staff [29]. Encryption is similar to what is used in the system we are proposing but since the format of the data is proprietary, it is different from what we are proposing.

B. Research Regarding EMRs on USB Drives

Little research has been completed regarding EMRs on USB drives. Yee and Trockman [30] proposed a portable EMR that can be stored on a USB drive. The system would be portable in that a system would be used anywhere, whether it is on a laptop computer operated by a paramedic or a desktop computer owned by the patient. In addition, this system would consist of an executable and data files. This system would be protected by a username/password system with the patient having the role as an administrator. The patient would create the EMR and then populate it. The patient generates the keys that would allow access to medical personnel (e.g., paramedics, doctors, and pharmacists). Only one patient type exists but multiple instances of medical personnel types. One issue that exists is how a personal EMR would be integrated with an EMR system operated by a medical facility to better facilitate health delivery [30].

Anciaux et al. expanded in this area by presenting an implementation of an EMR on an SPT [31]. The SPT would have its own web server along with Servlets, a protocol Java uses to respond to HTTP requests, generating database requests that would build the next page of the interface. A graphical user interface is used to view the contents of the patient folder by generating HTTP requests to the server. Regardless of the server, the graphical user interface will allow for access to patients' folders and management of authorization, to name a few. Anciaux et al.'s research did not discuss if the content of the patients' folder would be able to work with EMR standards such as HL7 and DICOM, the former is based on XML.

C. The PortableEMR (PEMR) System

Next, we offer an introduction to a portable EMR system that will address the workability with established EMR standards and integration of the device with an EMR system operated by a medical facility. We present a system that accepts EMRs carried on a SPT. The interface handling SPTs will use an experimental Java USB application programming interface (API) created in 2003 by Michael Stahl [32]. An SPT would be a dedicated USB drive whose sole purpose is to carry a patient's EMR. This SPT would only work in a PEMR system with any attempt to access it outside of PEMR would be denied since the SPT would be encrypted. The ultimate goal is that once the SPT is inserted into the computer, the PEMR application would run automatically and that it would prompt the user to login to the application to access his or her EMR. This SPT would have a software platform consisting of a graphical user interface application asking the user to open his or her EMR file written in XML and the hardware platform consisting of a secure microcontroller and large flash memory, hosting onboard code complete with tamper-resistant properties. This is similar to what is being proposed for an SPT in [31] except that it would not have its own operating system, Web server, and database management system. The mechanism will create an EMR by writing all information needed in an EMR to an XML file that will be used later not only by the interface itself but also the EMR system since XML is a base language for EMR standards such as HL7 and DICOM. The file will contain documents such as treatment records, insurance, personal contact information, emergency contact information, and a consent form delegating to a family representative or a practitioner chosen by the patient in the event the patient is unable to give consent.

The patient will be able to create the medical record by filling out necessary forms, such as: contact information, emergency contact information, insurance, lifestyle and habits information, and family medical history; that are saved to the SPT which will be encrypted along with the XML file as a PGP key file. A practitioner will be able to access the SPT

by plugging it into his or her computer and enter his or her passphrase to decrypt and modify information in the EMR located on the SPT. Practitioners can download the EMR file along with related files (such as images and laboratory test results) to the SPT that will be encrypted along with the XML file and the forms previously filled out by the patient. The contents of the personal EMR folder saved to the SPT would consist of: the digital signatures of the patient and practitioners who have modified the record, the EMR file that is digitally signed, legal documents and related files to an EMR. Examples of legal documents would include: a living will, consent for emergency treatment of a minor, a do not resuscitate form, and a limited power of attorney. A digitally-signed EMR is important since the digital signature provides for authentication, non-repudiation and data integrity. Data integrity would be facilitated when the healthcare provider uploads the information into the patient's EMR, signing this information with the provider's digital signature. One aspect of data integrity when EMRs are saved and/or modified is that data must not be destroyed without permission. Once an EMR is destroyed or subsections of it were modified or deleted, it has been compromised. Manual recovery could be the only option in cases of no software backup. Another aspect is using digital signatures to mark an EMR when saving it to the hard disk or SPT with the user needing to compute the link between the hash function and the decryption function with the link being intact if they are equal [30]. This means that the digitally-signed EMR file was originated or modified only by the person who digitally signed the EMR file. Patients will be able to view their EMR but can only modify certain areas, such as: personal info, insurance, family history, lifestyle and habits, doctors, documents, and emergency contacts. The system is portable in that a patient would be able to carry his or her EMR and present it to a doctor. The data would be transported securely on an SPT, which is a dedicated USB drive for the sole purpose of carrying a patient's EMR. Multi-level security when dealing with multiple healthcare providers can be facilitated by allowing one healthcare provider to add new information to an EMR but not modify information added in the system by another healthcare provider.

One detail that has to be noted is that the EMR file can be set to read-only, but the process would be irreversible in Java. One work-around would be to use an XML Digital Signature as generated by the Java XML Digital Signature API. When the EMR file is opened, PEMR will check to see if the file is digitally signed and check if the file was changed outside of PEMR, effectively validating the digital signature. PEMR uses an enveloped digital signature to sign the file. The following objects are created: XMLSignatureFactory (getInstance method is used), Reference (URI is specified to include the entire document), DigestMethod, Transform, KeyInfo (creates the key pairs using the KeyPairGenerator, KeyInfoFactory and KeyValue objects). The document will then be prepared for signing and then is signed. The signed document is written to a file. Validation of the XML signature involves: finding the Signature element, creating a DOMValidateContext object, unmarshaling the signature and validating the signature. Such a digital signature would have the ability to cover the entire XML file since the API has the means to sign the EMR once it is saved and then validate the EMR once it is opened by the system. The API does work with PGP key pairs [33]. The user's digital signature would indicate who last modified the file. Should the user encounter an EMR whose digital signature is not valid, the file will still open and the user will determine if any area of his or her EMR has been tampered. A software backup can be used to do a comparison of the two files. Once all errors have been corrected, the file will be saved with a new digital signature computed for his or her EMR.

PEMR uses PGP keys to facilitate encryption and decryption, which means PGP would have to be installed for key generation. PEMR is also reliant upon PGP Desktop, an external application, to facilitate encryption and decryption of EMRs into archive files that would keep these EMRs secure. PEMR would have to be adapted to meet other means of data entry, such as voice recognition. Should changes be made to PEMR, contractors can be hired who have the authority to modify PEMR to meet the healthcare facility's needs. PEMR is useful to patients in that they would be able to view their medical records at home on a computer while making changes to their personal information (e.g., changing insurance and provider information and adding related legal documents) and is useful to providers in that they would be able to update a patient's medical history so that other providers can see what has been done for the patient to provide the best possible service for that patient.

VI. How the Portable EMR System Works

This paper provides information on how the portable EMR system works. Specifically, we describe how EMRs operate with HL7 and DICOM, which are two of the most common EMR standards currently in use. Lastly, we present the role of PGP and a real-world example of how the portable EMR system works.

A. DICOM

DICOM is a specification that is accepted worldwide for the transmission, storage, and manipulation of diagnostic and therapeutic images along with related information to it. It also defines a file format as well as a network protocol for exchanging medical images [34]. As stated earlier, DICOM has the ability to store its pixels as two-dimensional slices with support available for video-based imagery from file types such as MPEG2 [16].

Development of DICOM started in 1983 and continued until a final specification was published in 1993, which was before the advent of XML. Two standards that are based on DICOM are Web Access to DICOM Persistent Objects (WADO) and DICOM Standard Reporting (DICOM SR). WADO is a web-based service capable of retrieving DICOM objects via either HTTP or HTTPS from a web server. Query mechanisms are not supported. Web clients must specify a DICOM object for retrieval by unique identifiers for study, series and instance level of a hierarchical DICOM information model. Clients can request the server to convert DICOM objects to JPEGs for images and HTML for reports. WADO servers are required to return any DICOM SR document in HTML format. Commercial implementations supporting WADO are

available, meaning the standard can be implemented with little effort. WADO provides a way to harmonize HTTP query syntax of web servers that have DICOM enabled.
DICOM SR is a model that encodes medical reports in a manner similar to DICOM's tag-based format. The structured report's format is represented by a document tree. All content items in the tree have information related to a medical record, such as a report or an image. Well-defined relationships describing parent and child content items in the hierarchical document structure are related. The DICOM standard does not specify how SR documents are to be rendered by an application. Applications must ensure that the report's full meaning is conveyed unambiguously. DICOM SR also has an explicit specification regarding digital signatures through rules addressing binary encoding peculiarities used by DICOM, which are extensive in nature [35]. A digitally-signed image would be integrated in a patient's portable EMR as a related medical file. The digital signature of the practitioner who originated the image file would prove that the image only came from the practitioner and no one else.

B. HL7

HL7 is a standard set that defines a message model used for transmission of data in healthcare organizations. It is the basis of a variety of medical data exchange architectures such as VistA [34]. It is an ANSI-accredited Standards Developing Organization operating solely in the healthcare arena. The domains under its jurisdiction are administrative and clinical. Ninety percent of all United States healthcare facilities use HL7. HL7 messaging has a legal status in a number of countries that use it.
HL7 has a standard known as the Clinical Document Architecture (CDA), which defines the XML architecture for exchange of Clinical Documents (CDs). CDA can contain any type of clinical content and it does use XML. However, CDA does allow for non-XML entities for simple implementations. This is important since DICOM uses video-based imagery for its representation. CDA documents can be displayed on web browsers that are XML aware, such as Internet Explorer. CDA's features as well as its use in the healthcare industry make it a pragmatic choice regarding a reference standard [36]. The EMR file generated by the portable EMR system is written in XML, meaning that it can be modified to be compatible with HL7. In addition, the EMR file generated by the portable EMR system is digitally signed, meaning the file was originated by one of the users whose digital signature is in the patient's portable EMR file.

C. PGP

PGP is used to encrypt the files of a patient's EMR. PGP is an application that provides authentication and privacy. In addition, PGP also uses integrity checking to determine if a message has been altered since it was sent. Message authentication is used to determine if a message was actually sent by the sender claiming to be such. Public keys in PGP are bound to an email address and a username, either of which would work as a username, while the passphrase for the public key would be sufficient for a password in the portable EMR system we are proposing. PGP users submit their public keys to a PGP database at MIT [37] so that other users can verify the identities of those users who have sent messages to them using a PGP public key.
PGP was chosen for this system since it is an established means for encrypting and decrypting data. An earlier version of PGP has been characterized as the next best thing to military-grade encryption [38]. PGP-encrypted devices were unable to be decrypted by law enforcement agencies when they were seized several years ago; making it the only known form of encryption that cannot be broken by cryptographic or computational means [39]. XML encryption has the ability to apply encryption and/or digital signature to portions of an XML document, making signature verification difficult, which means that the signature may be computed over either the encrypted or unencrypted form of elements [22].

D. Real-World Example

Next, we present a real-world example on how this system works. Heather Peterson is a process engineer who has two daughters named Veronica and Abby. Veronica and Abby go to a pediatrician on a regular basis in Jonesborough, Tennessee. Their medical information is stored on an EMR system at an area hospital as well as the medical information of Heather and her husband John. That changed when Heather lost her job when the company for which she worked several years shut down. Heather, on the advice of her brother, ends up finding a job at Norfolk Naval Shipyard as a process engineer. John finds a job at Norfolk Naval Shipyard as a draftsman. The medical records for Abby, Veronica, Heather, and John have to be transferred to a secure medium in a format that can be easily integrated into another EMR system. They meet with their family practitioner, Dr. Gordon Hoppe, about transferring their medical records to a USB drive. Dr. Hoppe asks for a USB drive, which he calls an SPT, and downloads their EMRs to their SPT. He also installs on the SPT the PEMR system that allows them to read their EMRs.
Upon arriving in Norfolk, John and Heather meet their new family practitioner, Dr. Nelson Monroy, and present their SPT to be integrated into the new medical facility's database. Dr. Monroy begins the process by logging into the application (see Figures 2 and 3) using his digital signature. He inserts the SPT into his computer. The application detects the SPT and prompts Dr. Monroy to choose the PGP file. Once the file is selected, Dr. Monroy will enter his passphrase, at which point the file will be decrypted. Dr. Monroy transfers the EMR folders to his computer. He opens the EMR file (see Figure 4) for each patient, reviews the information (see Figure 5), and saves the file. Once the files are saved, the EMRs will be digitally signed with Dr. Monroy's digital signature and will have the keys of the respective family members for each EMR (which in this case, would be Heather, John, Abby, and Veronica) as well as the keys of the practitioners who accessed the EMR in the patient's EMR folder.

VII. Conclusions and Future Work

We demonstrate that the proposed PEMR system is a secure means to store EMRs on SPTs. We also demonstrate that a digitally-signed EMR file allows for the EMR file to be authentic. A digitally-signed EMR file improves security

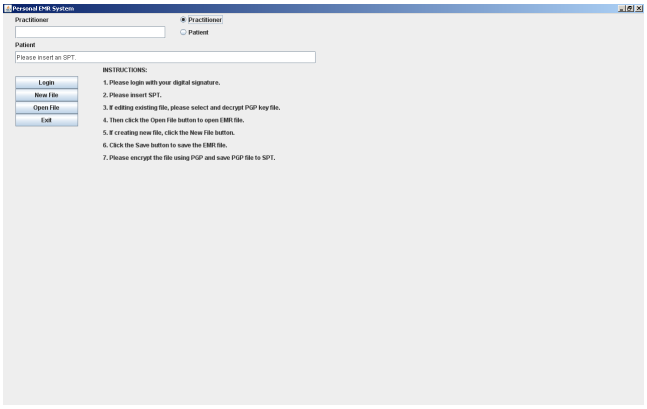

Figure. 2: Initial login screen.

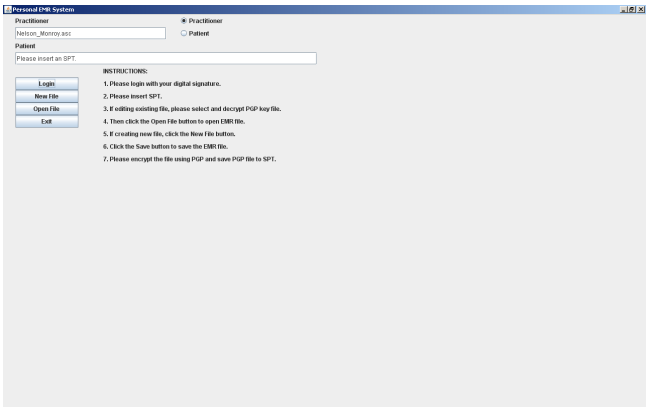

Figure. 3: Practitioner's login screen.

of EMRs since the digital signature provides for authentication, non-repudiation, and data integrity. This means that the digitally-signed EMR file was originated or modified only by the person who digitally signed the EMR file. Coupled with encrypting the contents of a patient's EMR folder in a PGP file, the portable EMR system is a secure means to store an EMR on an SPT. The system is portable in that a user would be able to carry his or her EMR on an SPT and present it to a doctor. The data would be transported securely on an SPT, which is a dedicated USB drive for the sole purpose of carrying a patient's EMR. Healthcare providers and patients would both benefit in that they have a secure means to store and transport electronic medical information since the patient's EMR file is digitally signed and that the files in a patient's EMR folder are encrypted with PGP.

The PEMR system, when plugged into a practitioner's computer, works within the medical facility network that employs the practitioner. It is recommended that a public key database similar to what is being used for PGP keys at MIT [37] be constructed to allow for practitioners to confirm identities of other practitioners who may have modified the patient's EMR file. It is also recommended that a web-based application and/or cloud computing application that is accessible to patients and physicians be constructed that would allow for EMRs to be stored in a database that can transfer the EMR files to patients and physicians. This would enable healthcare providers within the healthcare network to retrieve an EMR in the event the patient has no SPT when requesting care. The portable EMR system is reliant on an external PGP

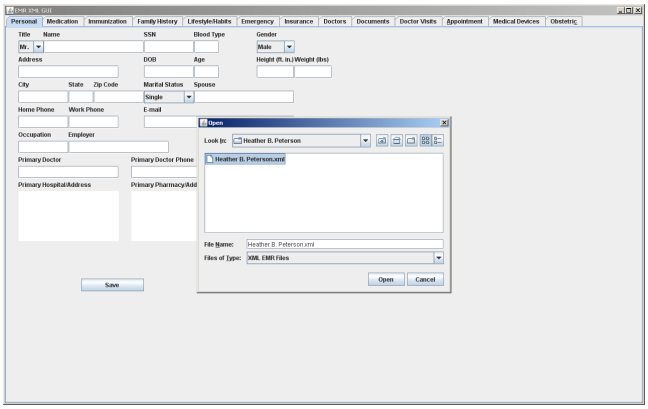

Figure. 4: EMR interface with patient's EMR open file dialog box.

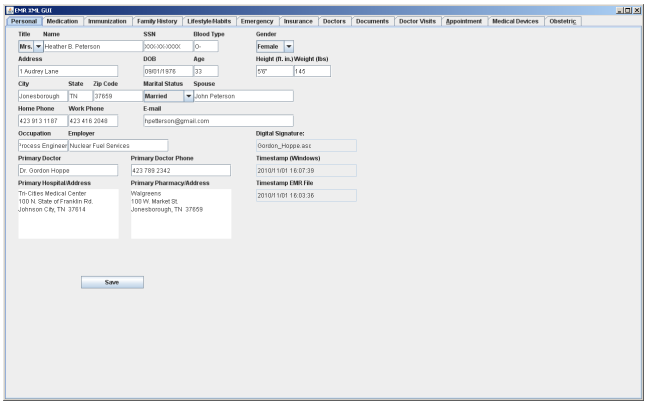

Figure. 5: Patient's EMR when personal information is filled in.

application for EMR files to be encrypted and decrypted, so it is recommended that it be modified to allow for such encryption and decryption to be done in-house. PEMR would have to be adapted to meet other means of data entry, such as voice recognition. An SPT would have to be constructed to facilitate the hardware and software platform required for PEMR. Usability testing would be conducted to obtain input from users, such as patients and healthcare providers alike. The benefit of this testing would make PEMR a more secure system capable of carrying a patient's digitally-signed EMR on an SPT.

Acknowledgement

We wish to acknowledge the United States Department of Energy (DOE) and National Nuclear Security Administration (NNSA) for their support. This material is based on research sponsored by DOE and NNSA under agreement number DE-FG52-09NA29516/A000. The U.S. Government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DOE, NNSA, or the U.S. Government. We also wish to acknowledge the anonymous reviewers and journal editors for reviewing this paper.

References

[1] L. Hoffmann. Implementing Electronic Medical Records. *Communications of the ACM*, 52(11):18–20, 2009.

[2] S. Braghin, A. Coen-Porisini, P. Colombo, S. Sicari, and A. Trombetta. Introducing Privacy in a Hospital Information System. In *Proceedings of the 4th International Workshop on Software Engineering for Secure Systems*, pp. 9–16, 2008.

[3] C. Brownlee. California Breach Disclosure Law Now Covers Medical Records. Available at http://www.privsecblog.com/2008/01/articles/medical-records/california-breach-disclosure-law-now-covers-medical-records, Sept. 2011.

[4] Patient Privacy Rights. Available at http://www.patientprivacyrights.org, Sept. 2011.

[5] Letter to the Honorable Kathleen Sebelius. Available at http://www.patientprivacyrights.org/media/E_Csebelius_letter.pdf, Sept. 2011.

[6] Protect Patients and Physicians Privacy Act, H.R. 2630, 111th Congress. Available at http://www.govtrack.us/congress/billtext.xpd?bill=h111-2630, Sept. 2011.

[7] J. Israelson and E. C. Cankaya. A Hybrid Web Based Personal Health Record System Shielded with Comprehensive Security. In *Proceedings of the 45th Hawaii International Conference on System Science*, pp. 2958–2968, 2012.

[8] W. Stallings and L. Brown. *Computer Security: Principles and Practice*, second ed., Prentice Hall, 2012.

[9] B. Lampson. Usable Security: How to Get it. *Communications of the ACM*, 52(11):25–27, 2009.

[10] W. R. Hersh. The Electronic Medical Record: Promises and Problems. *Journal of the American Society for Information Science*, 46(10):772–776, 1995.

[11] D. M. Rind, I. S. Kohane, P. Szolovits, C. Safran, H. C. Chueh, and G. O. Barnett. Maintaining the Confidentiality of Medical Records Shared over the Internet and the World Wide Web. *Annals of Internal Medicine*, 127(2):138–141, 1997.

[12] K. D. Mandl, P. Szolovits, and I. S. Kohane. Public Standards and Patients' Control: How to Keep Electronic Medical Records Accessible but Private. *British Medical Journal*, 322:283–287, 2001.

[13] T. Huston. Security Issues for Implementation of E-Medical Records. *Communications of the ACM*, 44(9):89–94, 2001.

[14] A. T. S. Chan, J. Cao, H. Chan, and G. Young. A Web-Enabled Framework for Smart card Application in Health Services. *Communications of the ACM*, 44(9):76–82, 2001.

[15] J. Grimson, W. Grimson, and W. Hasselbring. The SI Challenge in Health Care. *Communications of the ACM*, 43(6):48–55, 2000.

[16] M. T. Dougherty, M. J. Folk, E. Zadok, H. J. Bernstein, F. C. Bernstein, K. W. Eliceiri, W. Benger, and C. Best. Unifying Biological Image Formats with HDF5. *Communications of the ACM*, 52(10):42–47, 2009.

[17] R. W. Gardner, S. Garera, M. W. Pagano, M. Green, and A. D. Rubin. Securing Medical Records on Smart Phones. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Medical and Home-Care Systems*, pp. 31–39, 2009.

[18] K. Garson and C. Adams. Security and Privacy System Architecture for an E-Hospital Environment. In *Proceedings of the 7th Symposium on Identity and Trust on the Internet*, pp. 122–130, 2008.

[19] S. Han, G. Skinner, V. Potdar, E. Chang, and C. Wu. New Framework for Authentication and Authorization for E-Health Service Systems. In *Proceedings of the IEEE International Conference on Industrial Technology*, pp. 2833–2838, 2006.

[20] V. Koufi, F. Malamateniou, and G. Vassilacopoulos. A Medical Diagnostic and Treatment Advice System for the Provision of Home Care. In *Proceedings of the 1st International Conference on Pervasive Technologies Related to Assistive Environments*, pp. 1–7, 2008.

[21] V. Hristidis, P. J. Clarke, N. Prabakar, Y. Deng, J. A. White, and R. P. Burke. A Flexible Approach for Electronic Medical Records Exchange. In *Proceedings of the International Workshop on Healthcare Information and Knowledge Management*, pp. 33–40, 2006.

[22] D. Eastlake, J. Reagle, and D. Solo. XML-Signature Syntax and Processing. W3C Recommendation, available at http://www.w3.org/TR/2002/REC-xmldsig-core-20020212, Jan. 2011.

[23] T. Imamura, A. Clark, and H. Maruyama. A Stream-Based Implementation of XML Encryption. In *Proceedings of the ACM Workshop on XML Security*, pp. 11–17, 2002.

[24] C. Geuer-Pollmann. XML Pool Encryption. In *Proceedings of the ACM Workshop on XML Security*, pp. 1–10, 2002.

[25] P. Devanbu, M. Gertz, A. Kwong, C. Martel, G. Nuckolls, and S. G. Stubblebine. Flexible Authentication of XML Documents. In *Proceedings of the 8th ACM Conference on Computer and Communications Security*, pp. 136–145, 2001.

[26] R. Shigetomi, A. Otsuka, and H. Imai. Anonymous Authentication Scheme for XML Security Standard with Refreshable Tokens. In *Proceedings of the ACM Workshop on XML Security*, pp. 86–93, 2003.

[27] CARE Medical History Bracelet. Available at http://www.carememoryband.com, Jan. 2011.

[28] MedicTag Could Truly Save Your Life. Available at http://www.medictag.com, Jan. 2011.

[29] Medical Alert Jewelry 4U. Available at http://www.medicalalertjewelry4u.com, Jan. 2011.

[30] W. G. Yee and B. Trockman. Bridging a Gap in the Proposed Personal Health Record. In *Proceedings of the International Workshop on Healthcare Information and Knowledge Management*, pp. 49–56, 2006.

[31] N. Anciaux, M. Berthelot, L. Braconnier, L. Bouganim, M. De la Blache, G. Gardarin, P. Kesmarszky, S. Lartigue, J.-F. Navarre, P. Pucheral, J.-J. Vandewalle, and K. Zeitouni. A Tamper-Resistant and Portable Healthcare Folder. *International Journal of Telemedicine and Applications*, 2008(3):1–9, 2008.

[32] M. Stahl. *Java USB API for Windows*, Thesis, Institute for Information Systems, ETH Zurich, 2003.

[33] XML Digital Signature API. Available at http://download.oracle.com/javase/6/docs/technotes/guides/security/xmldsig/XMLDigitalSignature.html, Jan. 2011.

[34] N. Kaviani, D. Gasevic, M. Karimifar, M. Hatala, and S. Sheidaei. Rule Modeling to Unify Policies and Processes in Service-Oriented Health Information Systems. In *Proceedings of the Workshop on Model-Based Trustworthy Health Information Systems*, Nashville, TN, 2007.

[35] M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, and G. B. Laleci. A Survey and Analysis of Electronic Healthcare Record Standards. *ACM Computing Surveys*, 37(4):277–315, 2005.

[36] R. Bhatti, A. Samuel, M. Y. Eltabakh, H. Amjad, and A. Ghafoor. Engineering a Policy-Based System for Federated Healthcare Databases. *IEEE Transactions on Knowledge and Data Engineering*, 19(9):1288–1304, 2007.

[37] MIT PGP Public Key Server. Available at http://pgpkeys.mit.edu, Jan. 2011.

[38] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, second ed., John Wiley & Sons, 1996.

[39] P. Willan. PGP Encryption Proves Powerful. PCWorld, 2003.