Special Report

Cybersecurity Challenges for PACS and Medical Imaging

Marco Eichelberg, PhD, Klaus Kleber, Marc Kämmerer, MD

Cybersecurity issues have been on the rise for years, increasingly affecting the healthcare sector. In 2019, several attacks have been published that specifically aim at medical network protocols and file formats, in particular digital imaging and communications in medicine. This article describes five attack scenarios on picture archiving and communications systems (PACS) and medical imaging networks: the import of patient data from storage media containing malware, a compromise of the hospital network, malware embedded in digital imaging and communications in medicine images or reports, a malicious manipulation of medical images and a network infiltration of malicious health level seven messages. Prevention and mitigation measures for each of these attacks exist, some of which can be implemented by the system user (e.g., hospital), while others require implementation in the PACS and medical imaging devices by the vendors. In practice, however, many of these are not in common use. What is missing today are PACS network security guidelines for practitioners that support users in keeping their network secure. Furthermore, integrating the healthcare enterprise integration profiles and test tools might be needed to address the deployment of public key infrastructure and digital signatures in the PACS environment.

Key Words: Cybersecurity; PACS; DICOM; IHE.

© 2020 The Association of University Radiologists. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license. (http://creativecommons.org/licenses/by-nc-nd/4.0/)

INTRODUCTION

Over the past 20 years, the Internet has become an indispensable resource for accessing and exchanging information. Hospitals worldwide are connected to the Internet, which often serves both as a medium for services such as e-mail and Web, and as a transport infrastructure for secure services, such as the exchange of patient health information or access to a regional or national electronic health record.

A negative side effect of the widespread adoption of the Internet is the dramatic increase in cybersecurity incidents, such as computer virus infections, ransomware, or the theft and publication of patient data. While in the past, cybersecurity issues were often caused by hobbyists driven by curiosity, today they are primarily attributed to organized crime and advanced persistent threat groups associated with nation states (1). Correspondingly, the cybersecurity threats faced by hospitals are reaching a new quality. While in the past attacks were often widespread and random, they now become increasingly targeted at the healthcare sector, which is apparently seen as an attractive target by the attackers. Nippon Telegraph and Telephone Security's 2017 Global Threat Intelligence Report (2) reports that healthcare is among the sectors most affected by ransomware attacks, with 15% of all ransomware attacks globally occurring in healthcare institutions in 2017. Furthermore, several attacks have been published in 2019 that specifically aim at medical network protocols and file formats. Examples include weaknesses found in the wireless protocols of implantable devices (3) and insulin pumps (4), the embedding of malware in a digital imaging and communications in medicine (DICOM) image (5), and the use of artificial intelligence techniques to falsify medical images by rendering a convincingly looking tumor into the images of CT studies (6).

In this article, we discuss cybersecurity challenges from the perspective of medical imaging and picture archiving and communications systems (PACS). In each case, we start by presenting a scenario and then discuss possible consequences and measures that could prevent the attack from succeeding. It should be noted, however, that PACS specific security measures need to be implemented as part of a comprehensive security concept for the IT infrastructure as a whole. A perfect protection against a hacker breaking into the hospital network will be of limited value if the PACS server is completely open and answers to queries from all over the Internet. This is, unfortunately, not a theoretical issue. Gillum et al. (7) performed a study in 2019 that found hundreds of PACS systems around the globe exposed to access from the Internet due to a complete lack of basic IT security measures.

ATTACK 1: IMPORT OF PATIENT DATA FROM STORAGE MEDIA CONTAINING MALWARE

The first scenario is a malware infection caused by the import of patient data from a storage medium brought by the patient. In

Acad Radiol 2020; ■:1–14

From the OFFIS-Institute for Information Technology, R&D Department Health, Escherweg 2, Oldenburg 26121, Germany (M.E.); VISUS Health IT GmbH, Bochum, Germany. **Address correspondence to:** M.E. e-mail: eichelberg@offis.de

© 2020 The Association of University Radiologists. Published by Elsevier Inc. This is an open access article under the CC BY-NC-ND license. (http://creativecommons.org/licenses/by-nc-nd/4.0/)

https://doi.org/10.1016/j.acra.2020.03.026

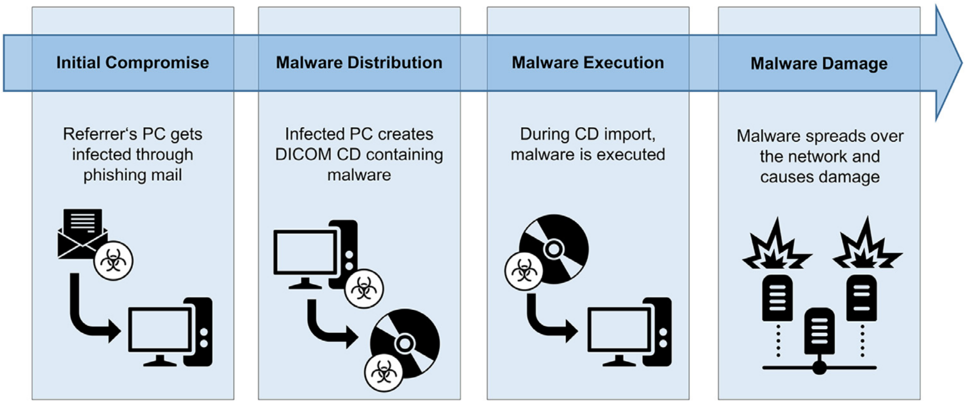
Initial Compromise
Malware Distribution
Malware Execution
Malware Damage
Referrer's PC gets infected through phishing mail
Infected PC creates DICOM CD containing malware
During CD import, malware is executed
Malware spreads over the network and causes damage

Figure 1. Import of patient data from storage media containing malware – phases of attack.

many cases today, medical images are given to the patient on a storage medium such as a recordable compact disc (CD). The patient can carry the CD to a hospital where follow-up treatment is planned and performed, making the images available as priors. In many cases, these images will be imported into the local PACS infrastructure of the hospital, either as a permanent copy in the image archive, or as temporary images on a dedicated import server or on the diagnostic workstation.

The cybersecurity scenario, depicted in Figure 1, begins with a computer virus infection of the personal computer (PC) used to create the patient's CD in the first place. This may happen for example by a careless click on a link in a SPAM e-mail, or by opening an infected document also received by e-mail. The virus would cause any executable file on the infected PC that is opened for reading or writing to be infected as well – this is the classic spreading model that gave rise to the name "computer virus."

Most systems that create DICOM CDs write an executable DICOM viewer to the CD that can be started from the CD and will be used when no dedicated DICOM workstation is available. Usually, these DICOM viewers are started automatically when the CD is inserted into a drive by means of the Windows "AutoRun" function, unless AutoRun is explicitly disabled. A system infected with the type of malware described previously would most probably involuntarily write an infected version of the DICOM viewer executable to the CD.

The third phase of the attack takes place when the CD is imported at the receiving hospital or private practice. Unless a dedicated DICOM workstation is used to read and import the images from the CD, the executable viewer on the CD will most likely be launched and cause an infection of the PC used for CD import. The virus could now execute arbitrary software or try to download and run further software modules from an Internet server controlled by the attackers. Different types of attacks are possible now: The malware could passively intercept the network traffic (see next section) and try to identify logins and passwords and send these to an Internet server controlled by the attackers. It could try to spread to other PCs over the internal network. The currently most probable and most harmful type of attack, however, would be ransomware: this type of malware would try to encrypt as many files as possible – on the infected PC and on all network shares accessible – and then display a message demanding the payment of a ransom (typically using a cryptocurrency such as Bitcoin). This is, unfortunately, a rather likely scenario: a document published by the United States. Department of Justice (8) states that 4000 ransomware attacks *per day* were reported to the authorities in 2016, an increase by a factor of four compared

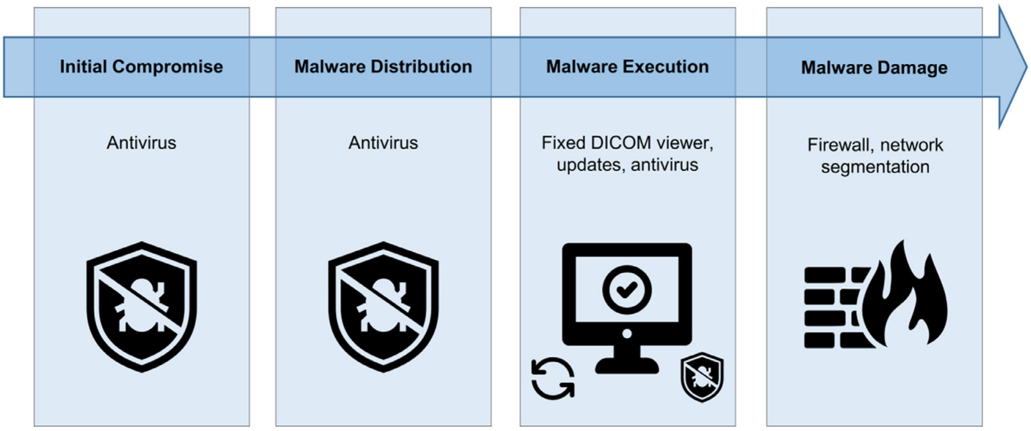

Figure 2. Technical measures against malware infections during storage media import.

to 2015. In the year 2017, 50% of all cybersecurity incidents in hospitals were related to ransomware (2).

Technical measures to prevent this type of attack are rather straightforward, as shown in Figure 2: First of all, the use of antivirus software on the side of the media creator should in many cases prevent the creation and distribution of infected storage media in the first place. At the recipient's site, a fixed installation of a DICOM viewer or importer application should be used instead of the viewer provided on the CD, and "AutoRun" should be disabled on the import CD. This solution also avoids the problem that the user is confronted with many different viewer applications that require different user interactions for the same task. Furthermore, the import system should be provided with regular updates and have antivirus software installed. It is also recommendable to configure a firewall between this system and the internal network so that only explicitly desired interactions (such as the transmission of imported images using the DICOM network protocol) are possible and all other network ports are closed (in particular those for accessing network shares), thus limiting the possible damage that could by caused by malware infection. In addition, these import workstations should be placed into dedicated network segment, separated from the remaining network by a firewall, in order to offer possible threats as little contact surface to the remaining network as possible.

ATTACK 2: ATTACKER HACKS INTO THE HOSPITAL NETWORK

The second scenario is centered on an attacker who at the hospital premises manages to get access to the hospital's internal local area network (LAN). Figure 3 shows the phases of this type of attack.

The first phase of the attack is the compromise of the hospital's LAN. This may either happen through access to an unprotected network port of the cabled network, or by compromising the encryption of the wireless network (WLAN). Over time, weaknesses have been discovered in all WLAN protection mechanisms from WEP ("Wired Equivalent Privacy") to the WPA2 (Wi-Fi Protected Access 2) protocol still commonly used today. For example, a successful attack against WPA2 called "KRACK" (Key Reinstallation Attacks) was published by Vanhoef et al. in 2017, with a follow-up report by the same authors in 2018 (9) showing that the mitigation measures implemented by the IT industry since publication of the weakness did not fully solve the issue.

The second phase of the attack is the passive interception of the network traffic by the attacker, in order to learn about the network structure, systems on the network, user credentials, and the type of network protocols used. Both DICOM and the health level seven (HL7) version 2 standard by default transmit messages in unprotected, clear-text format. This enables an attacker with access to the network to use a so-called "packet analyzer" to passively intercept and analyze the network traffic. For example, Wireshark (10), a widely used packet analyzer, explicitly supports the HL7 and DICOM network protocols and is even able to store the content of a passively captured DICOM image transmission as a valid DICOM file. This means that the attacker is able to learn about the network addresses and port numbers of DICOM and HL7 systems in the network as well as capture patient names, demographic data and identifiers of patients currently admitted to the hospital.

The third phase of the attack is unauthorized access to systems in the network in order to download images or reports. While passive network interception might provide an attacker with information about many general purpose network services used within the network (e.g., e-mail or Website credentials), this discussion focuses on the specific issues related to medical imaging and PACS. When the DICOM network protocol was originally designed in the early 1990s, no mechanisms for access rights were foreseen. Any client that can successfully connect to the PACS server over the network can issue queries related to the patients, studies and images stored on that server. Downloading images (or reports in DICOM format) is more difficult, because the DICOM C-MOVE protocol that is most commonly used for this purpose requires the PACS server to open a separate network connection to the client, based on a symbolic name called "move application entity title". PACS servers, therefore, maintain in their system configuration a list of known clients with fixed network addressed. Only systems in that list are able to download from the PACS server. However, even without the ability to download images, a hacker could still issue queries and thus access confidential patient information about all patients for whom images were ever stored in the archive. Furthermore, the

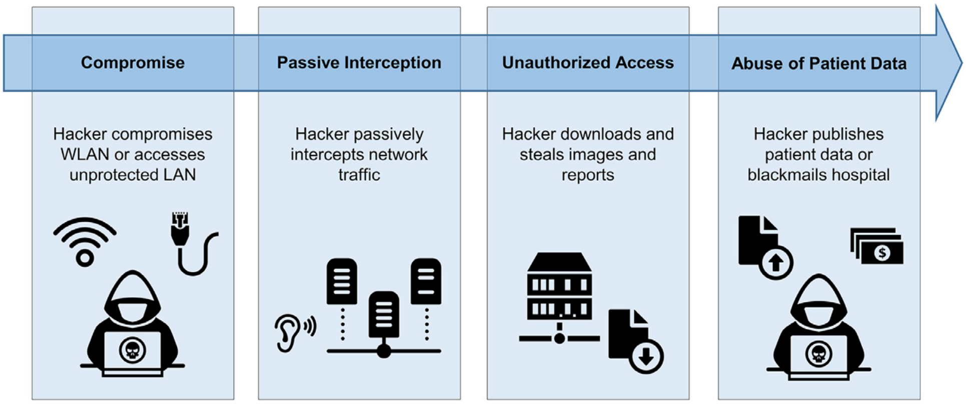
Compromise
Hacker compromises WLAN or accesses unprotected LAN
Passive Interception
Hacker passively intercepts network traffic
Unauthorized Access
Hacker downloads and steals images and reports
Abuse of Patient Data
Hacker publishes patient data or blackmails hospital
$

Figure 3. Attacker hacks into the hospital network – phases of attack.

DICOM C-GET protocol, which is supported by most modern PACS servers, eliminates the need for a preconfigured list of known clients and enables each client that can connect to the server to also download images.

The last phase of the attack would be the abuse of the illegally acquired information "for fun and profit," as a common phrase in the IT community puts it. The attackers could simply anonymously publish the data on the Internet, thus causing legal problems, penalties and bad press for the hospital (and annoyance for the patients affected), or they could try to blackmail the hospital with the threat of publication of the data.

The technical measures that need to be implemented to prevent this type of attack should consist of several layers to achieve a "defense in depth," as shown in Figure 4. The first layer of protection consists of physical safeguards and a secure network architecture. Cabled network ports should not be located in rooms to which unauthorized persons may have unsupervised access, network plugs should be physically secured, so that they cannot be pulled out and plugged into a different device. Many network switches can be configured so that only computers with well-known media access control addresses (i.e., serial numbers of the network interface controller) are permitted to connect. Furthermore, unused ports should be switched off until they are needed. Wireless networks should be operated in a secure configuration, which needs to be reviewed and updated, if necessary, at regular intervals. While none of these measures alone will provide perfect security, they will increase the effort required from an attacker. Furthermore, firewalls and network segmentation should be used to isolate the medical devices and PACS from the office PCs that may be more susceptible to attacks.

The European Union Agency for Network and Information Security (11) points out that "it is important to separate critical parts of the network from noncritical parts. For instance, it is recommended to separate medical devices to the largest possible extent from office components that are typically – due to the use of standard components – susceptible to a wide range of attacks. Nippon Telegraph and Telephone Security explains that network segmentation is important because "if attackers can breach back-end servers, they may be able to move laterally to access other portions of your network, doing further damage, and possibly gaining a foothold across multiple systems" (12). They recommend the use of "firewalls, routers, and other network security devices to implement and enforce network segregation", i.e., "restricting the flow of network traffic between network segments with different security profiles" (2).

The second layer of protection is the use of encryption for network transmission not only over the Internet, but also in-house. While both DICOM and HL7 by default communicate in clear-text, as described previously, both protocols can be protected by using Transport Layer Security (TLS) (13), a network protocol that enables "applications to communicate over the Internet in a way that is designed to prevent eavesdropping, tampering, and message forgery" (13). The DICOM standard offers a set of "secure transport connection profiles" that describe how to use TLS with DICOM network connections. The first of these was added to the DICOM standard in 2000, almost 20 years ago, and the first open source implementation of this DICOM extension was published in the same year (28). For systems that do not support TLS, a gateway can be implemented that accepts "normal" DICOM network connections and forwards these using TLS. An early implementation of such a gateway was already described by Thiel et al. in 1999 (14). When DICOM and HL7 are protected with TLS, a passive interception of the network traffic will not provide attackers with any confidential information (at least related to these protocols) even if they manage to compromise the network and gain network access. Furthermore, if TLS is used with bidirectional certificate exchange (an option in the TLS protocol), then an attacker that gains network access will not be able to connect to any of the protected systems, in particular preventing any attempt to download images or reports from the PACS server.

The third layer of protection is the implementation of access rights on the PACS server. For this purpose, the DICOM standard was modified in 2004 (15) to enable the transmission of user identity information during the initial phase of a DICOM network connection. This information can be used by the PACS server to restrict access to images and reports based on information such as the assignment of users to departments, user roles, and the current status of the patient. The DICOM standard does not specify how such access rights should be defined and linked to the user identity, as this will depend on local policies and laws. In any case, the implementation of such access

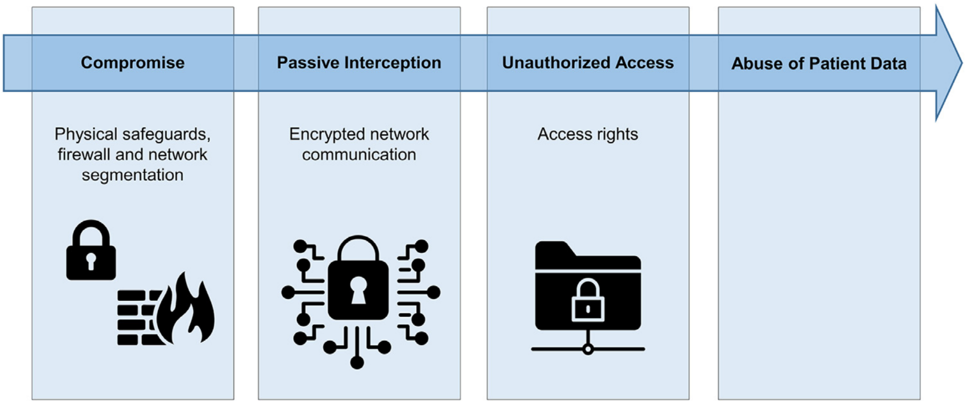
Compromise
Passive Interception
Unauthorized Access
Abuse of Patient Data
Physical safeguards, firewall and network segmentation
Encrypted network communication
Access rights

Figure 4. Technical measures against data theft due to network compromise.

rights will limit the number of images and reports any attacker might be able to access and download, if the attacker manages to compromise the network and successfully establish a TLS connection (e.g., using a certificate and private key stolen from another system on the network), thus not preventing but mitigating the effect of an attack.

ATTACK 3: MALWARE EMBEDDED IN DICOM IMAGES OR REPORTS

The attack scenarios described in this and the following sections have in common that they are significantly more complex than the attacks described so far. They require detailed knowledge about vulnerabilities in software libraries used in medical devices, physical access to devices, or an analysis of the hospital network after compromise of the network. On the other hand, the damage caused by these attacks is possibly much higher because the malicious software acts behind all firewalls on the inside of the PACS network. Such attacks are more likely to be prepared and performed by organized crime or advanced persistent threat groups, which are often associated with state actors. Objectives of such attacks could be the disruption of health services, blackmail or they could target individual "VIP" patients.

Malware is usually associated with executable files and with certain document types such as Microsoft Word or Portable Document Format (PDF) that allow executable scripts to be embedded in a document. Under certain conditions it is possible, however, to embed malware into a DICOM image or into a report in DICOM format such that the execution of the malware does not take place on the system importing the DICOM data into the local PACS network, but on a PACS workstation or the PACS server itself. The phases of this attack are shown in Figure 5.

The scenario starts with the import of DICOM images or report from a storage medium brought by a patient or from a regional or national electronic health record. The DICOM object contains malware, but since the images and/or reports are not viewed during the import process, the malware remains inactive and the malicious documents are stored in the PACS server. Later, a Radiologist retrieves and displays the documents as prior images or prior report. At this point in time, the malware is executed, either on the diagnostic workstation or in the PACS server itself. The malware now executes in the PACS network, behind all firewalls. When the malware is executed on the PACS server, it probably gains read access to the whole PACS archive and can also overwrite (e.g., encrypt) significant parts of the archive as part of a ransomware attack. The question is how an attacker can embed malware in a DICOM document so that execution occurs when the document is opened for reading. There are three possible "routes" for this kind of attack:

- *Abuse of the DICOM File Preamble.* The DICOM file format specifies that the first 128 bytes of the file, the so-called "preamble," are not used by the DICOM standard and may contain arbitrary information. The file format was deliberately designed this way in order to permit "dual-personality" files that are at the same time a valid DICOM image and a valid tagged image file format (TIFF) image. An application of such dual-personality files in digital pathology is described by Clunie (16). In April 2019, security researcher Ortiz published a report and a proof of concept (17) that shows that dual-personality files can be constructed that are at the same time a valid DICOM image and a valid Windows "Portable Executable" program. Ortiz calls such files "PE/DICOM." This issue was registered in the National Vulnerability Database of the National Institute of Standards and Technology (NIST) as common vulnerabilities and exposures (CVE)-2019-11687 and rated with a severity base score of "HIGH." The CVE description (18) explains that "to exploit this vulnerability, someone must execute a maliciously crafted file that is encoded in the DICOM Part 10 File Format. PE/DICOM files are executable even with the .dcm file extension. Antimalware configurations at healthcare facilities often ignore medical imagery."
  It should be noted that the DICOM file preamble is *not* transmitted when an image is sent over a network using the DICOM network protocol, e.g., between PACS and

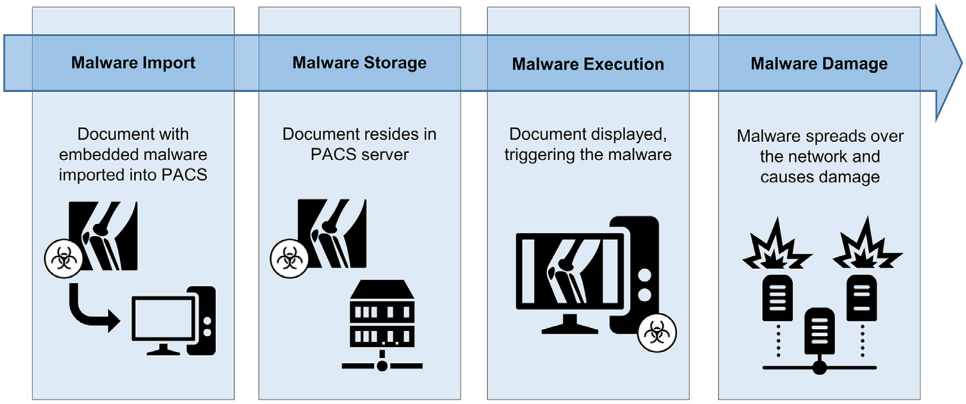
Malware Import
Malware Storage
Malware Execution
Malware Damage
Document with embedded malware imported into PACS
Document resides in PACS server
Document displayed, triggering the malware
Malware spreads over the network and causes damage

Figure 5. Malware embedded in DICOM images or reports – phases of attack. DICOM, digital imaging and communications in medicine.

viewing workstation. That means that a network transmission of a DICOM image automatically "cleans" the image by removing the header that marks the image as being executable. The threat is, therefore, reduced to scenarios in which DICOM files are imported or displayed from possibly unsafe sources. This includes on one hand storage media provided by the patient *before import over the network* and on the other hand DICOM documents submitted using the new DICOM web service extensions ("DICOMweb"), which transfer complete DICOM files *including* the preamble. When such a malicious PE and/or DICOM file is received, it is not automatically executed − this still requires a manual interaction by a user. As a press release of the DICOM committee (19) explains, "a user might be convinced to execute the file via social engineering. Alternatively, a separate malicious actor that knew about the embedded executable and had access to the modified file could install and execute the malware. This type of intrusion is referred to as a multi-phase attack."

- *Malware in Encapsulated DICOM objects.* The DICOM standard not only supports the storage and transmission of images, but there are also document formats for various other types of information including signals (e.g., ECG recordings), measurements, or reports. In particular, the DICOM standard in its current edition (20) supports the encapsulation of certain other file formats into a DICOM file. Currently DICOM defines "encapsulated" formats for documents in PDF and HL7 clinical document architecture (CDA) format as well as for the STL ("stereolithography") and OBJ ("object") file formats commonly used in 3D manufacturing and Virtual Reality applications. These file formats may have cybersecurity issues of their own. In particular the PDF format is very complex and permits the inclusion of executable scripts. PDF has been a source of malware in the past, either through the use of scripts embedded in PDF documents, or through maliciously manipulated documents triggering buffer overflows (or other software bugs) in an application that in turn could lead to arbitrary code execution. For example, the NIST National Vulnerability Database lists more than 1500 known vulnerabilities related to older versions of the Adobe Reader application, and more than 500 vulnerabilities related to older versions of the Foxit PDF reader. Since most DICOM applications will not implement a PDF reader on their own, but use an available software library or tool for processing PDF documents, they "inherit" vulnerabilities present in the libraries or tools used. While no vulnerabilities have been reported for the CDA document format as such, CDA can in turn be used to encapsulate other formats like PDF. The main risk related to the cybersecurity of the STL file format is described by Sturm et al. (21) as related to cyber-physical attacks in which STL files are maliciously manipulated so that the 3D printer will create an object that looks correct to a human observer but has built-in defects or weaknesses that only become apparent after implantation: "Additive manufacturing is unique in that the interior of a part can be altered without affecting the exterior of the part, resulting in a part that looks and feels strong, but is weak on the inside."
- *Malware based on manipulated compressed DICOM images.* The DICOM standard supports the storage and transmission of compressed images. A large number of compression schemes − both reversible and irreversible − is supported by the DICOM standard, including the JPEG format (ISO/IEC 10918), named after the ISO/IEC Joint Photographic Expert Group, and the more recent compression algorithms JPEG-LS (ISO/IEC 14495) and JPEG 2000 (ISO/IEC 15444), as well as various video compression standards specified by the ISO/IEC Moving Picture Experts Group (MPEG). DICOM also supports the compression of complete DICOM documents using the common "deflate" algorithm (22) that is also used in ZIP files. An attacker could create maliciously manipulated compressed DICOM objects that upon decompression would trigger buffer overflows or other software bugs in the decoding application that in turn could lead to the execution of malicious code embedded in the object. The feasibility of this kind of attack was demonstrated in 2004, when a vulnerability (CVE-2004-0200) was detected in the Windows operating system that could be exploited with a malicious JPEG image. Any DICOM viewer using the Windows Graphics Device Interface (GDI) to decode and display JPEG-compressed DICOM images at the time of publication of the attack would have been vulnerable. The attack is described in detail by Hornat (23). Another example is the so-called "Stagefright" vulnerability reported in 2015, named after the affected software library in the Android operating system, which permitted remote code execution by means of a maliciously manipulated MPEG-4 video sent to an Android device as a multimedia message. The user did not even have to open the message, as message receipt was sufficient to trigger the vulnerability. The attack is described in detail by Be'er (24). The NIST CVE database lists more than 450 entries related to MPEG, more than 100 entries related to JPEG 2000, and there are also entries related to implementations of JPEG-LS and Deflate compression. Since there is only a limited number of software libraries available that implement these algorithms, it is likely that DICOM applications are − or were − affected by some of these vulnerabilities.

Malware based on manipulated compressed DICOM images can possibly be used by an attacker to compromise the PACS server: When a DICOM workstation tries to retrieve images, it can negotiate with the server whether image transmission should take place in compressed or uncompressed form. If the workstation does not support compression, it is the task of the server to decompress the images and then deliver an uncompressed version over the network. In this situation, the potential buffer overflow and malware execution would take place directly in the PACS server.

The implementation of technical safeguards against the attacks described in this section, outlined in Figure 6, is simple in the case of "PE/DICOM" files and difficult in the case of malware embedded in encapsulated documents or compressed images.

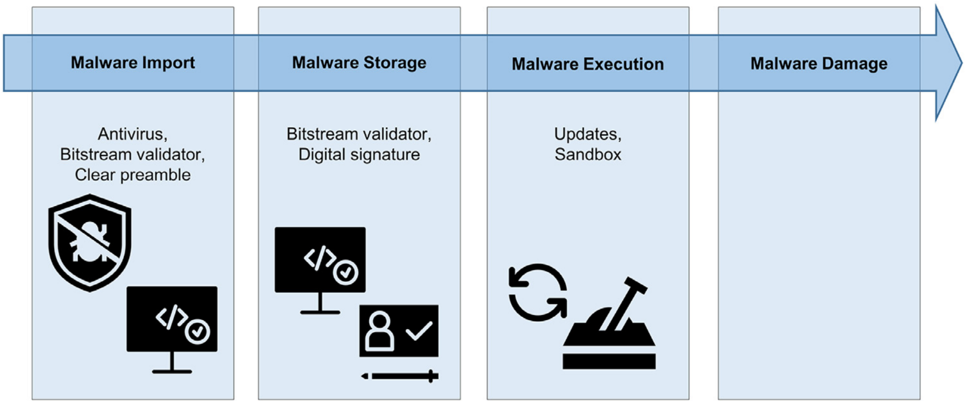

Figure 6. Technical measures against malware embedded in DICOM images or reports. DICOM, digital imaging and communications in medicine.

Since the DICOM file preamble is not required by the DICOM protocol, in most cases the preamble can be safely overwritten when importing a DICOM file. It is actually sufficient to replace the first two bytes of the file with zeroes to render it safe. In settings where dual-personality DICOM/TIFF files are used, files starting with "II" or "MM" (which identifies the TIFF format) can remain unmodified.

Preventing the installation and spreading of malware through encapsulated or compressed DICOM objects requires that vendors rigorously test their applications that read and display such documents or images, that they update products based on third-party libraries when vulnerabilities in these libraries become known, and that they employ, where possible, bit-stream validators that identify malformed documents and prevent their processing and display. Furthermore, the decoding of embedded documents can be moved into a so-called "sandbox", a separate process with minimal rights. This is an implementation technique that minimizes the damage that can be caused by vulnerabilities in the software. Some vulnerabilities can possibly be identified by malware scanners (antivirus software). Furthermore, in situations where encapsulated or compressed DICOM documents are only accepted from a limited number of known sources, digital signatures embedded in the DICOM documents by the creator could prove that no malicious manipulation has taken place after the creation. See the discussion on DICOM digital signatures in the following section.

ATTACK 4: MALICIOUS MANIPULATION OF MEDICAL IMAGES

Machine learning techniques, often referred to as "artificial intelligence" (AI), have significantly progressed in the last few years, due both to increased hardware performance and improved algorithms, and AI driven solutions are also increasingly used in medical imaging (25). One less desirable result of the progress in machine learning are so-called "deep fakes": convincing forgeries of images or videos where for example the face of an actor has been replaced. Mirsky et al. (6) have shown in 2019 that this technology can also be applied to the creation of convincing forgeries of medical images. They trained so-called generative adversarial networks (GAN) to either insert ("paint") a lung cancer into a volumetric CT scan, or to remove it, based on a training dataset derived from 888 annotated CT scans of the public research image database published by the Lung Image Database Consortium and the Image Database Resource Initiative.

Mirsky et al. state that "to verify the threat of this attack, we trained CT-GAN to inject/remove lung cancer and hired three radiologists to diagnose a mix of 70 tampered and 30 authentic CT scans. [. . .] The experiment was performed in two trials: blind and open. In the blind trial, the radiologists were asked to diagnose 80 complete CT scans of lungs, but they were not told the purpose of the experiment or that some of the scans were manipulated. In the open trial, the radiologists were told about the attack, and were asked to identify fake, real, and removed nodules in 20 CT scans. In addition, the radiologists were asked to rate the confidence of their decisions." The results were quite impressive: in the blind trial, "the radiologists diagnosed 99% of the injected patients with malignant cancer, and 94% of cancer removed patients as being healthy. After informing the radiologists of the attack, they still misdiagnosed 60% of those with injections, and 87% of those with removals."

The phases of a cyberattack based on the malicious manipulation of medical images is shown in Figure 7. In order to "inject" modified images into the clinical workflow, it will be necessary for the attackers to place a small gateway computer between the modality and the network, or to compromise and modify the software running on the modality. We do not discuss the latter case further in this article because it would require an intimate knowledge of the software architecture of the modality. While a small form-factor computer may look sufficiently innocuous to staff, this requires unattended physical access to the modality, and as such, "insider" knowledge or careful preparation by the attackers. The gateway computer will then transparently intercept, analyze and forward all DICOM messages (including all images) sent by the modality. If the gateway opens a wireless network (as described in the article by Mirsky et al.), it can also be used to

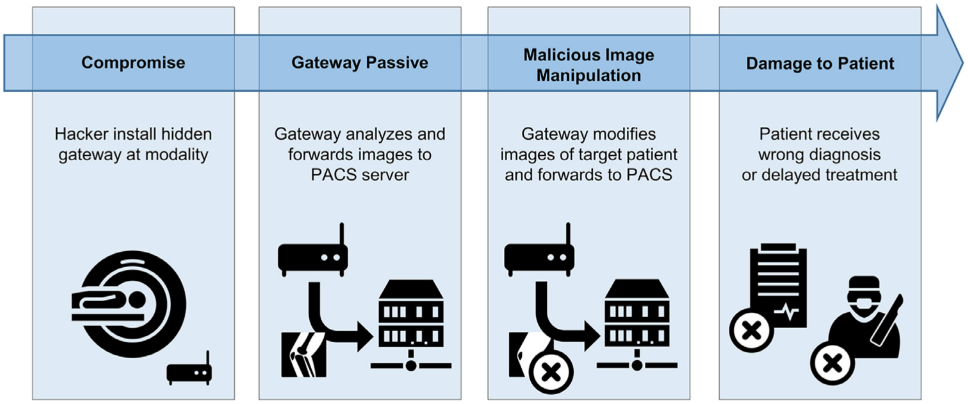
Compromise
Hacker install hidden gateway at modality
Gateway Passive
Gateway analyzes and forwards images to PACS server
Malicious Image Manipulation
Gateway modifies images of target patient and forwards to PACS
Damage to Patient
Patient receives wrong diagnosis or delayed treatment

Figure 7. Malicious manipulation of medical images – phases of attack.

passively intercept other network communication (e.g., capture logins and passwords transmitted in clear text) and permit remote control by the attackers. The attack as such would happen when the gateway detects certain identifiers such as the name of a VIP patient it has been waiting for. The system would now render false information into the image, either by adding or removing lesions, and only then forward the images to the PACS archive or diagnostic workstation. Except for a short delay in the network transmission, there would be no other noticeable conspicuity. As described by Mirsky et al., the probability would be very high that the unsuspecting Radiologists would base their diagnostic report on the manipulated image, unless the discrepancy between the images displayed on the modality console (before manipulation) and the images displayed on the diagnostic workstation (after manipulation) gets noted.

However, the risk of maltreatment due to manipulated images into which a tumor has been inserted may not be as dramatic as it sounds because treatment decisions, in particular in the case of tumors, are preceded by further examinations such as lab tests, a biopsy, additional CT or magnetic resonance imaging sequences, or ultrasound examinations that would turn out inconsistent with the manipulated images. The risk may be higher if the manipulation removes tumors and shows a normal result, as in this case the patient might be sent home without any further examination, thus delaying a correct diagnosis and treatment. However, such an attack would be difficult to aim at a specific patient, as this would require that the attacker knows about or suspects the presence of a tumor while the responsible health professionals do not – a rather unlikely situation. In summary, the attack could perhaps be performed successfully against random patients, thus damaging a hospital's reputation and perhaps causing legal and financial consequences for the hospital, but it is difficult to conceive a successful directed attack against individual VIP patients. Nevertheless, the work by Mirsky et al. shows that the technical means for manipulating image content have clearly reached a new level, and that an integrity protection of medical images might be advisable in the future.

Figure 8 shows measures that can be implemented to prevent this attack from succeeding. First of all, since the attack requires physical access to the modality, locked doors (which includes the use of nontrivial PIN codes where electronic locks are used) that prevent unauthorized access in particular during off-work times are an important first step. Furthermore, network plugs should be physically secured (so that they cannot be pulled out and plugged into a different device) and the network switch should be configured to only accept the modality's MAC address, as this will make it more difficult for an attacker to successfully install a gateway for the "man in the middle" attack.

Secondly, TLS should be used to encrypt network communication between the modality and the PACS. This will

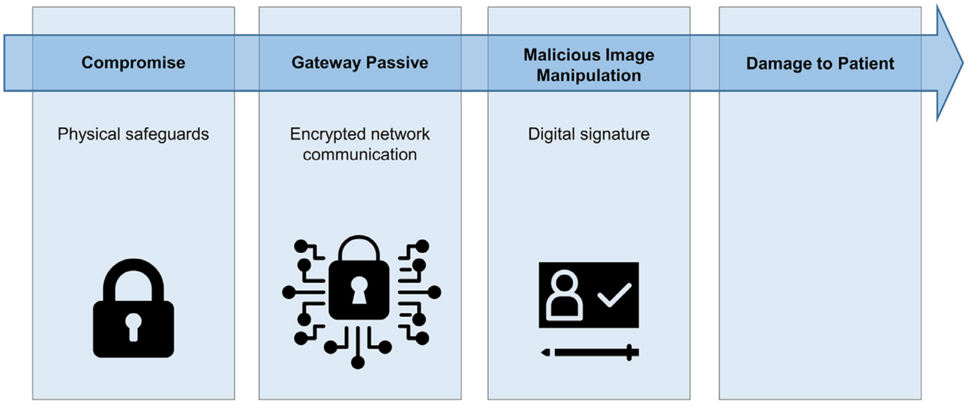

Figure 8. Technical measures against a malicious manipulation of medical images.

not only prevent an attacker from analyzing the network traffic, but, if implemented with bidirectional certificate exchange, will prevent any man-in-the-middle attack from succeeding (see discussion on attack scenario 2.)

The third layer of protection is the use of digital signatures to guarantee that modifications of an image cannot remain undetected at any point after image creation. This is also recommended by Mirsky et al., who state that "the best way to detect this attack is to have the scanner sign each scan with a digital signature." The idea of using digital signatures to protect the integrity and authenticity of medical images is not new: Wong et al. (26) proposed the use of digital signatures and timestamps to prevent an unauthorized modification of images already in 1995. The DICOM standard introduced the concept of digital signatures and trusted timestamps in 2001. DICOM allows users to apply one or more digital signatures to a complete DICOM image or parts thereof, and then to embed the signatures in the DICOM header, which ensures that the digital signature is always stored and transmitted as part of the signed image or document, together with the certificate of the signer. This enables a validation of the signature by any system that receives the image. An early implementation of DICOM digital signatures is described by Riesmeier et al. (27). Unfortunately most imaging modalities do not support the creation of DICOM digital signatures. Kroll et al. (28) proposed the use of a small gateway computer that receives the images from one modality, adds a digital signature to each image and then forwards the images to the image archive. This is essentially a set-up that is very similar to that of the cyberattack, with the difference that the gateway is used to add integrity protection to the images instead of compromising it.

Another necessary condition for the use of digital signatures is that the workstations that retrieve and display medical images support the verification of signatures in the images and display a warning to the user if any digital signature is invalid (which might indicate a malicious modification of the image) or missing (since the attacker could try to simply remove the signature and then modify the image). Unfortunately, digital signature support in PACS workstation is also very rare, and, since it requires user interaction if signature validation fails, it cannot be retrofitted to legacy systems by means of a separate gateway computer.

ATTACK 5: NETWORK INFILTRATION OF MALICIOUS HL7 MESSAGES

The last cybersecurity threat to PACS to be discussed in this article are malicious HL7 messages. While DICOM covers the majority of communication needs in a PACS environment, HL7 version 2 messages are commonly used to keep information consistent across information systems such as Hospital Information Systems, Radiology Information Systems, and the PACS. HL7 messages are used to update patient information consistently and automatically across multiple IT systems. Such updates can either change certain fields like the patient's name, address or telephone number, or they can request the merging of two patient records into one – an operation that becomes necessary when it is discovered that two patient records have been created for the same patient, either through user error, or because a patient was admitted as an unidentified emergency case with a temporary identifier. Unfortunately, the HL7 message standard does not provide any means to prevent the malicious abuse of such messages. An attacker could passively monitor HL7 network traffic and learn about the patients, admissions, orders, diagnoses, and lab results of patients currently admitted to the hospital. Perhaps more importantly, an attacker could try to actively send malicious HL7 messages or modify legitimate messages during transmission.

The phases of the attack are shown in Figure 9. The attackers would first compromise the network by either connecting to an unprotected cabled network port or by compromising the WLAN. They would then passively intercept network traffic and identify systems sending or receiving HL7 messages including the message types sent, network addresses and the identifiers of patients currently admitted. The attackers would then prepare a set of malicious HL7 "update" or "merge" messages to change patient data and infiltrate these into the

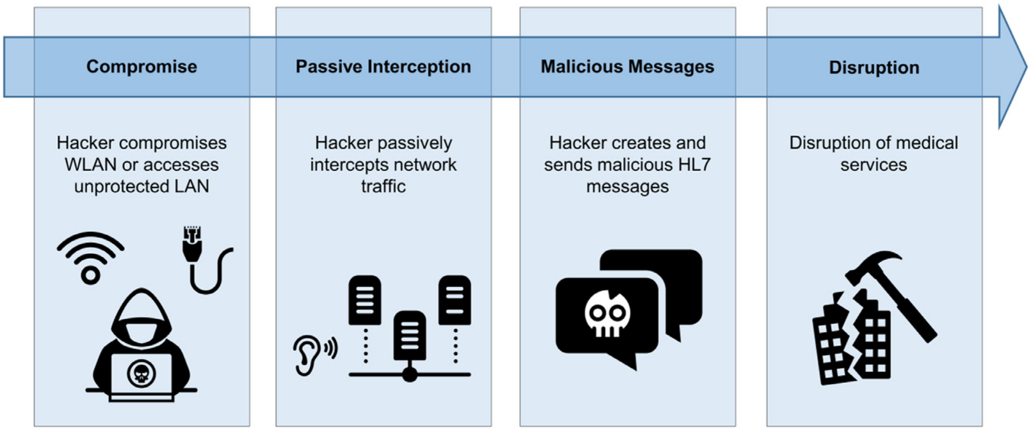
Compromise
Passive Interception
Malicious Messages
Disruption
Hacker compromises WLAN or accesses unprotected LAN
Hacker passively intercepts network traffic
Hacker creates and sends malicious HL7 messages
Disruption of medical services

Figure 9. Network infiltration of malicious HL7 messages – phases of attack. HL7, health level seven.

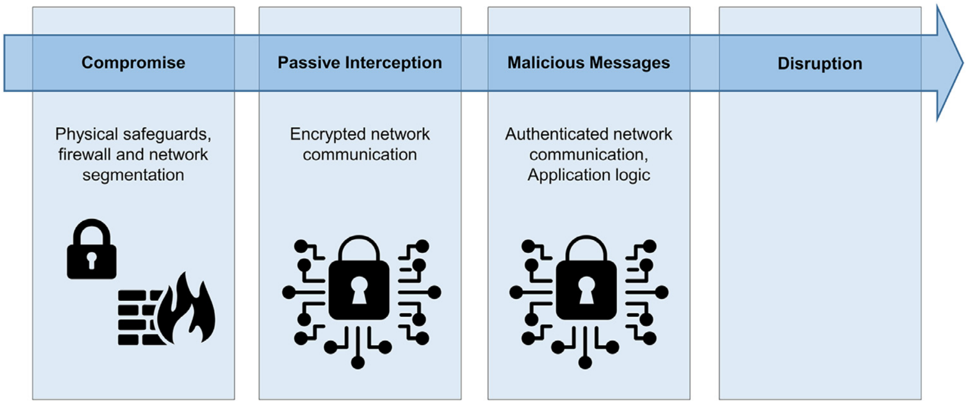
Compromise
Passive Interception
Malicious Messages
Disruption
Physical safeguards, firewall and network segmentation
Encrypted network communication
Authenticated network communication, Application logic

Figure 10. Technical measures against a network infiltration of malicious HL7 messages. HL7, health level seven.

network. They could, for example, rename all patients to "John Doe" or merge all patient records into one. While it might be possible to reverse the damage done, this would require a significant amount of manual work. In the meantime, medical services would be at least partially disrupted because access to patient records, orders, results and images would be near impossible.

The technical measures against this attack are shown in Figure 10. The first two layers of protection are identical to those discussed in the section on attack scenario 2. Protecting the HL7 message exchange with TLS using bidirectional certificate exchange not only prevents the passive interception of the HL7 message traffic by the attacker but also prevents the infiltration of malicious messages because the sending system needs to have access to a trusted certificate and the corresponding private key. The final layer of protection is the implementation of application logic that tries to identify unusual patterns of message communication and raise an alarm if these occur. Systems could, for example, measure the percentage of update messages in comparison to other messages and raise an alarm if it suddenly increases significantly or if there are unusual types of updates (e.g., change of first name and family name in a patient record that was not assigned to an unidentified emergency case). The merging of patient records should be a relatively rare event and may justify human confirmation before execution.

TABLE 1. General Security Measures

Security Measure	Responsible	Attack
Configure network switches to accept only known MAC addresses.	User	2,5
Define a secure WLAN configuration, review and update regularly	User	2,5
Install antivirus software where permitted, update regularly	User	1,3
Keep operating systems and application software updated regularly	User + vendor	1,3
Keep room locks when unused	User	2,4,5
No cabled network ports in unsupervised areas	User	2,5
Physically secure network plugs	User	2,5
Split LAN and WLAN into different segments, with firewalls in-between.	User	1,2,5

LAN, local area network; MAC, media access control; WLAN, wireless local area network.

DISCUSSION

In this article we have presented a number of cybersecurity attack scenarios and discussed countermeasures for each scenario. In general, we can distinguish security measures that are not specific to PACS/medical imaging but also apply there, summarized in Table 1, and more specific measures, summarized in Table 2. It should be pointed out that this summary is not a complete list of cybersecurity measures that apply. Further measures not discussed in this article include a regular backup, the use of network monitoring and intrusion detection systems, the whitelisting of permitted applications, and the whole domain of organizational measures such as user training, penetration testing and incident management. An overview of these topics is provided by the European Union Agency for Network and Information Security (11).

Most of the general security measures shown in Table 1 can be implemented by the user organization (i.e., the hospital) without support from device vendors, with the exception of regular updates to operating systems and application software on all systems, which requires the provision of updates by the device vendors, in particular in the case of certified medical devices where any modification must undergo rigorous testing by the vendor before being released to users.

On the other hand, most PACS/medical imaging specific security measures, as shown in Table 2, require support from device vendors. While a hospital should be able to deploy a fixed installation of a DICOM viewer for media import, the move from unencrypted communication in the network to encrypted communication requires device support, or alternatively the deployment of gateway computers (which might be a business opportunity for startup companies to address

TABLE 2. PACS/Medical Imaging Specific Security Measures

Security Measure	Responsible	Attack
Use fixed installation of DICOM viewer for media import	User	1
Protect DICOM and HL7 network connections with TLS	User + vendor	2,4,5
Use DICOM user identity information to restrict access to the PACS	User + vendor	2
When importing DICOM files, clear the file preamble	Vendor	1,3
Use bitstream validators to check encapsulated documents and compressed images	Vendor	3
DICOM Viewers should render encapsulated documents or compressed images in a "sandbox" process with limited rights	Vendor	3
Protect DICOM images and documents with digital signatures	Vendor	3,4
Use application logic to block suspicious HL7 update/merge operations	Vendor	5
Verify digital signatures when reading DICOM images or documents	Vendor	3,4

DICOM, digital imaging and communications in medicine; HL7, health level seven; PACS, picture archiving and communications system; TLS, transport layer security.

these issues faster than the PACS and modality vendors.) The implementation of access rights in the PACS requires on one hand support both in the PACS server, which must enforce the access rights, and in the workstations, which must authenticate the user and transmit the user identity to the server. On the other hand, it also requires work by the hospital, which must define appropriate rules for access rights and provide interfaces to the systems that maintain the required information, e.g., which patient has been assigned to which department, ward or doctor. This information is typically available in the Hospital Information System but not in the PACS.

Systems that sanitize DICOM file preambles, employ bitstream validators and sandbox processes when processing encapsulated documents and compressed images, and employ application logic to "catch" possibly malicious HL7 messages can only be provided by the system vendors. Finally, digital signatures also require vendor support: While it is possible to add signature creation functionality to legacy systems by means of gateway computers, as described in the discussion of attack scenario 4, the integrity protection offered by digital signatures is useless unless the viewers verify the signatures when reading a DICOM document or image and warn the user if a signature is invalid or missing.

Another point highlighted by Table 1 and Table 2 is that protection even against complex cybersecurity attacks is possible and that most of the required measures have been common knowledge or even standardized for a long time, as in the case of encrypted communication and digital signatures, which have been standardized in DICOM for some 20 years. The obvious question is: why have these measures not (or rarely) been deployed in the past. In the view of the authors, there are two main reasons: one reason is that the necessity to implement such measures within the hospital network and not just on the firewall protecting the "trusted" LAN from the untrusted internet, has only become obvious recently. Since there was very little user demand in the past, vendors have not implemented security features, and it will require significant effort from the user community to change this now. The second reason is that the implementation of security measures may be more expensive (in terms of effort required) than the discussion in this paper seems to indicate. For example, both the use of encrypted communication and digital signatures require hospitals to deploy a public key infrastructure as each system needs to be provided with an individual private key and signed certificate, all of which need to be renewed regularly since certificates have a finite lifetime (typically between three months and three years).

TABLE 3. Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
APT	Advanced Persistent Threat
CDA	Clinical Document Architecture
CT	Computed Tomography
CVE	Common Vulnerabilities and Exposures
DICOM	Digital Imaging and Communications in Medicine
DICOMweb	DICOM web service extensions
EHR	Electronic Health Record
GAN	Generative Adversarial Network
GDI	Graphics Device Interface
HIS	Hospital Information Systems
HL7	Health Level Seven
IHE	Integrating the Healthcare Enterprise
JPEG	Joint Photographic Experts Group
KRACK	Key Reinstallation Attacks
LAN	Local Area Network
MAC	Media Access Control
MPEG	Moving Picture Experts Group
MRI	Magnetic Resonance Imaging
NIST	National Institute of Standards and Technology
NTT	Nippon Telegraph and Telephone
OBJ	Object
PACS	Picture Archiving and Communications System
PDF	Portable Document Format
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RIS	Radiology Information Systems
STL	Stereolithography
TIFF	Tagged Image File Format
TLS	Transport Layer Security
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

TABLE 4. Glossary of Cybersecurity Related Terms Used in this Article

Term	Explanation
Access Rights	The Permissions Granted to an Individual User to Read, Write, Modify, or Delete Information Stored in a Database
Advanced Persistent Threat (APT)	A computer network threat actor that uses clandestine, and sophisticated hacking techniques to gain unauthorized access to a system and remain inside for a prolonged period of time.
Antivirus Software	Software that is used to prevent, detect, and remove malware.
Authentication	The act of proving the identity of a computer system or computer user.
Backup	A copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.
Bit-stream Validator	A computer program that checks the validity of a document.
Certificate	An electronic document that includes a public key, information about the identity of its owner, an expiration date, and a digital signature of an entity called “Certificate Authority” that has verified the certificate’s contents.
Common Vulnerabilities and Exposures (CVE)	A catalog of publicly known information security vulnerabilities.
Computer Virus	A malicious program that, when executed, replicates itself by modifying other computer programs and inserting its own code.
Cybersecurity	The practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
Digital Signature	A mathematical technique used to validate the authenticity and integrity of a message, software or digital document.
Encryption	The process of encoding a message or document in such a way that only authorized parties can access it and those who are not authorized cannot.
File Preamble	In the DICOM file format, the first 128 bytes of the file are called the “file preamble”.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Gateway Computer	A system that serves as an access point to another network that may be using a different networking technology.
Generative Adversarial Network (GAN)	A machine-learning technology that trains an artificial neural network to generate data with the same statistics as the training set. A GAN can be used to synthesize fake or manipulated images or photos.
Integrity	The accuracy and validity of data over its lifecycle. Data integrity requires assuring that data cannot be modified in an unauthorized or undetected manner.
Interface	A connection between two systems or programs.
Intrusion Detection System	A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
Key Reinstallation Attack (KRACK)	An exploitable flaw of the WPA2 protocol that allows an attacker to intercept data from a wireless network unless the software running on the access point and the client computers contains protection measures against this attack.
Local Area Network (LAN)	A network that interconnects computers within a limited area such as a building or campus.
Malware	Malicious software, i.e. software intentionally designed to cause damage to a computer or computer network.
Media Access Control (MAC) Address	A unique identifier assigned to a network interface controller for use as a network address within a network segment.
Network Address	A numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.
Network Port [logical, physical]	This term either refers to a physical network socket into which a network cable can be plugged to connect a computer to a network, or to a logical communication endpoint for a certain program running on a computer.
Network Segment	A part of a computer network that is separated from other parts of the network by a Firewall.
PE/DICOM Portable Executable	A computer file that is at the same time a valid DICOM file, and a valid executable program for the Windows operating system.
PIN Code	A numeric or alpha-numeric password.
Packet Analyzer	A program or device that can intercept and log traffic that passes over a digital network or part of a network.
Penetration Testing	An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.
Private Key	

(*continued*)

TABLE 4. (Continued*)*

Term	Explanation
	In public-key cryptography, a private key is an encryption key that must be kept strictly secret. The private key can be used to authenticate as the owner of related certificate, to create digital signatures on behalf of the owner, and to decode encrypted information sent to the owner.
Public Key Infrastructure (PKI)	Public-key cryptography is a cryptographic system that uses pairs of keys: public keys which may be disseminated widely, and private keys which are known only to the owner. A public key infrastructure (PKI) is a system for the creation, storage, and distribution of digital certificates which are used to verify that a particular public key belongs to a certain entity.
Ransomware	A type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.
SPAM Mail	Unsolicited messages sent in bulk by email.
Sandbox	A security mechanism for executing software in a restricted operating system environment, in order to mitigate software vulnerabilities from spreading.
Switch	A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
Transport Layer Security (TLS)	A cryptographic protocol designed to provide communications security over a computer network.
Vulnerability	A weakness that can be exploited by a threat actor to perform unauthorized actions within a computer system.
Whitelisting	A technology that prevents the execution of all software on a computer that is not explicitly included in a list of permitted programs.
Wi-Fi Protected Access (WPA)	A family of encryption protocols for wireless networks. WPA2 is the version in most common use today; WPA3, published in 2018, is an improved version that addresses weaknesses of WPA2 such as KRACK and in general provides a higher level of security.
Wired Equivalent Privacy (WEP)	An outdated encryption protocol for wireless networks, superseded in 2003 by Wi-Fi Protected Access (WPA).
Wireless Local Area Network (WLAN)	a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a building or campus.

DICOM, digital imaging and communications in medicine.

For hospitals with hundreds or thousands of systems this requires automation, as manual installation of certificates and keys on each system is not sustainable. Failure of certificate renewal will automatically cause an interface to completely fail once the certificate expires. Furthermore, the cryptographic algorithms used for encrypted communication and digital signatures will have to evolve over time since algorithms and key lengths considered secure today may become insecure in the future. This needs to be coordinated across all systems that use these algorithms, because an update of one system that removes support for an outdated algorithm may render an interface inoperable if the newer algorithms are not yet supported by all other devices this system is supposed to communicate with (Tables 3 and 4).

Finally, the question remains which security measures should be taken by the Radiologists. In general, there should be a team of IT professionals with the responsibility of planning and maintaining the IT infrastructure under consideration of medical, operational, economic, safety and security factors. Part of this work should be the development of a set of local security guidelines, together with user awareness and training measures for medical users. These guidelines should instruct users how to react when a virus scanner raises alarm, how to handle storage media brought by the patients, how to report abnormalities that may or may not be cybersecurity related, and how to manage cybersecurity incidents, should these happen. If no such guidelines are available yet, Radiologists should insist on the development, and collaborate with the IT professionals to make sure that the rules specified do not negatively affect medical practice. Once guidelines are available, Radiologists should ensure that they are adhered to. Furthermore, it is of key importance that health professionals, who will often be the first ones to notice, do not ignore IT related abnormalities but report them immediately, since time to the start of incident management may be critical for limiting the damage done.

CONCLUSIONS

The recent increase in cybersecurity publications focusing on PACS and medical imaging has made it clear that this is a topic that in the future the PACS vendor and user community will have to address more intensively than in the past. While there are many guidelines and implementation guides for generic IT cybersecurity, little practical help is available so far for the practitioner who wants to bring the security of a PACS network up to the state of the art. A recent draft publication by the U.S. NIST entitled “Securing Picture Archiving and Communication System – Cybersecurity for the Healthcare Sector” (29) and a publication by Desjardins et al. (30) that provides recommendations to the DICOM committee, vendors and users, are first steps in this direction, but there will certainly be a need for more, for example in the form of IHE integration profiles and test tools that address the public key infrastructure issues discussed in the previous section, and the requirements of a deployment of DICOM digital signatures.

FUNDING

Dr. Eichelberg reports a grant from VISUS Health IT, during the conduct of the study. Mr. Kleber and Dr. Kämmerer report a grant from the European Regional Development Fund (Grant Number EFRE-0801341), and the German State of North Rhine-Westphalia, during the conduct of the study.

ACKNOWLEDGMENTS

This paper is based on work of the project MITSicherheit. NRW, which received funding from the European Union through the European Regional Development Fund and the German State of North Rhine-Westphalia.

REFERENCES

1. EUROPOL European Cybercrime Center, "Internet Organised Crime Threat Assessment 2018," https://doi.org/10.2813/858843.
2. NTT Security, "2017 Global Threat Intelligence Report (GTIR)," Available at: https://www.nttsecurity.com/de-de/gtir-2017. (Accessed November 21, 2019).
3. U.S. Cybersecurity and Infrastructure Security Agency, "Medtronic Conexus Radio Frequency Telemetry Protocol", ICS Medical Advisory (ICSMA-19-080-01), 2019. Available at: https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01. (Accessed November 21, 2019).
4. U.S. Food and Drug Administration, "Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks," FDA safety communication, 2019. Available at: https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication. (Accessed November 21, 2019).
5. U.S. Cybersecurity and Infrastructure Security Agency, "DICOM Standard in Medical Devices", ICS Alert (ICS-ALERT-19-162-01), 2019. Available at: https://www.us-cert.gov/ics/alerts/ICS-ALERT-19-162-01. (Accessed Nov 21, 2019).
6. Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: malicious tampering of 3D medical imagery using deep learning. 28th USENIX Secur Symp 2019: 461–478. Available at: https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky. (Accessed November 21, 2019).
7. J. Gillum, J. Kao and J. Larson, "Millions of Americans' medical images and data are available on the internet. Anyone can take a peek," ProRepublica report, 2019, Online: https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet. (Accessed November 21, 2019)
8. "How to Protect Your Networks from Ransomware," US Government interagency technical guidance document, 2016. Available at: https://www.justice.gov/criminal-ccips/file/872771/download. (Accessed November 21, 2019).
9. M. Vanhoef and F. Piessens, "Release the Kraken: new KRACKs in the 802.11 Standard," *Proc. 2018 ACM SIGSAC Conference on Computer and Communications Security*, 299-314. https://doi.org/10.1145/3243734.3243807.
10. Wireshark® Network Protocol Analyzer. Available at: https://www.wireshark.org/. (Accessed November 21, 2019).
11. European Union Agency for Network and Information Security (ENISA), Smart hospitals – security and resilience for smart health service and infrastructures," 2016. https://doi.org/10.2824/28801.
12. NTT Security, "2019 Global Threat Intelligence Report (GTIR)," Available at: https://www.nttsecurity.com/landing-pages/2019-gtir/. (Accessed November 21, 2019).
13. E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, Internet Engineering Task Force (IETF) Request for Comments 8446, 2018. Available at: https://tools.ietf.org/html/rfc8446 (Accessed November 21, 2019).
14. Thiel A, Bernarding J, Jensch P. Security concepts in image management. Proc. EMBEC 1999; 37(2):1552–1553.
15. DICOM Standards Committee, Working Group 14. Digital imaging and communications in medicine (DICOM) supplement 99: extended negotiation of user identity. Final Text 2004. Available at: ftp://medical.nema.org/medical/dicom/final/sup99_ft.pdf (Accessed Nov 21, 2019).
16. Clunie DA. Dual-personality DICOM-TIFF for whole slide images: a migration technique for legacy software. J Pathol Inform 2019; 10:12.. https://doi.org/10.4103/jpi.jpi_93_18.
17. Ortiz MO. HIPAA-protected malware? Exploiting DICOM flaw to embed malware in CT/MRI imagery. Cylera Labs 2019. Available at https://labs.cylera.com/2019/04/16/pe-dicom-medical-malware/ (Accessed November 21, 2019).
18. NIST National Vulnerability Database, CVE-2019-11687 detail. Available at: https://nvd.nist.gov/vuln/detail/CVE-2019-11687 (Accessed November 21, 2019).
19. DICOM Committee, "DICOM 128-byte preamble – press release," 2019, Available at: https://www.dicomstandard.org/wp-content/uploads/2019/05/Press-Release-DICOM-128-Byte-Preamble-Posted1-2.pdf (Accessed November 21, 2019).
20. DICOM Standards Committee, "Digital imaging and communications in medicine (DICOM)," NEMA Standard PS3.1-21 2020a. Available at: https://www.dicomstandard.org/current/ (Accessed March 3, 2020).
21. Sturm LD, Williams CB, Camelio JA, et al. Cyber-physical vulnerabilities in additive manufacturing systems: a case study attack on the .STL file with human subjects. J Manuf Syst 2017; 44(1):154–164. https://doi.org/10.1016/j.jmsy.2017.05.007.
22. L.P. Deutsch, "DEFLATE Compressed Data Format Specification version 1.3", Internet Engineering Task Force (IETF) Request for Comments 1951, May 1996. Available at: https://tools.ietf.org/html/rfc1951 (Accessed September 19, 2019).
23. C. Hornat, "JPEG Vulnerability: A day in the life of the JPEG Vulnerability," Technical Report, Info Security Writers, 2004. Available at: http://www.infosecwriters.com/text_resources/pdf/JPEG.pdf (Accessed November 21, 2019).
24. H. Be'er, "Metaphor: a (real) reallife Stagefright exploit," NorthBit technical report, 2016. Available at: https://www.exploit-db.com/download/39527 (Accessed November 21, 2019)
25. Artificial intelligence in medical imaging: opportunities, applications and risks. In: Ranschaert ES, Morozov S, Algra PR, eds. Springer nature; 2019. . https://doi.org/10.1007/978-3-319-94878-2.
26. S.T.C. Wong, M. Abundo, and H.K. Huang, "Authenticity techniques for PACS images and records," *Proc. SPIE 2435, Medical Imaging 1995: PACS Design and Evaluation: Engineering and Clinical Issues*. https://doi.org/10.1117/12.208827.
27. Riesmeier J, Eichelberg M, Kleber K, et al. Authentication, Integrity and Confidentiality in DICOM Structured Reporting: Concept and Implementation. In: Medical Imaging 2002: PACS and Integrated Medical Information Systems: Design and Evaluation, Proc. SPIE, 4685; 2002. p. 270–278.
28. Kroll M, Schütze B, Geisbe T, et al. Embedded systems for signing medical images using the DICOM standard. Int Congr Ser 2003; 1256:849–854. https://doi.org/10.1016/S0531-5131(03)00463-1.
29. NIST Special Publication 1800-24, "Securing picture archiving and communication system (PACS) - cybersecurity for the healthcare sector," DRAFT, 2019. Available at: https://www.nccoe.nist.gov/projects/use-cases/health-it/pacs (Accessed November 21, 2019)
30. Desjardins B, Mirsky Y, Picado Ortiz M, et al. DICOM images have been hacked! Now what? Am J Roentgenol 2020; 214:1–9. https://doi.org/10.2214/AJR.19.21958.