How Secure Is Your Radiology Department? Mapping Digital Radiology Adoption and Security Worldwide

Mark Stites[1]
Oleg S. Pianykh[2,3]

OBJECTIVE. Despite the long history of digital radiology, one of its most critical aspects—information security—still remains extremely underdeveloped and poorly standardized. To study the current state of radiology security, we explored the worldwide security of medical image archives.

MATERIALS AND METHODS. Using the DICOM data-transmitting standard, we implemented a highly parallel application to scan the entire World Wide Web of networked computers and devices, locating open and unprotected radiology servers. We used only legal and radiology-compliant tools. Our security-probing application initiated a standard DICOM handshake to remote computer or device addresses, and then assessed their security posture on the basis of handshake replies.

RESULTS. The scan discovered a total of 2774 unprotected radiology or DICOM servers worldwide. Of those, 719 were fully open to patient data communications. Geolocation was used to analyze and rank our findings according to country utilization. As a result, we built maps and world ranking of clinical security, suggesting that even the most radiology-advanced countries have hospitals with serious security gaps.

CONCLUSION. Despite more than two decades of active development and implementation, our radiology data still remains insecure. The results provided should be applied to raise awareness and begin an earnest dialogue toward elimination of the problem. The application we designed and the novel scanning approach we developed can be used to identify security breaches and to eliminate them before they are compromised.

Keywords: DICOM, firewall, networking, PACS, security

DOI:10.2214/AJR.15.15283

Received July 14, 2015; accepted after revision November 2, 2015.

Based on a presentation at the European Congress of Radiology 2015 annual meeting, Vienna, Austria.

[1]Graduate Division, Harvard Medical School, Harvard Extension School, Boston, MA.

[2]Department of Radiology, Harvard Medical School, Massachusetts General Hospital, 25 New Chardon St, Office 470, Boston, MA 02114. Address correspondence to O. S. Pianykh (opiany@gmail.com).

[3]School of Data Analysis and Artificial Intelligence, National Research University–Higher School of Economics, Moscow, Russia.

AJR 2016; 206:797–804

0361–803X/16/2064–797

Over the past few years, the question of inadequate clinical security has been gaining attention from both industry leaders and clinical practitioners [1–8]. However, the real scope of security breaches has been always hard to estimate: one had to rely on already confirmed breaches (e.g., a report that more than 80% of health care systems had already been compromised [1]), or one had to examine only the local devices (e.g., discovering that 83% of a radiology department's devices had high-risk vulnerabilities [2]). Moreover, it was often assumed that the intruders would use an extensive arsenal of hardware, networking, and malware to exploit health care data vulnerabilities [1, 2]. As a result, we were falling short of assessing the breadth of the problem, because we were overestimating the effort required to breach an average clinical department.

Therefore, we decided to undertake a much more ambitious study by estimating, in the most complete, uniform, and objective way, the real scope of radiology security vulnerabilities worldwide. Instead of reporting what was already compromised in the past, we wanted to know what can be compromised now. Furthermore, we considered only the breaches that one can exploit with legitimate clinical standard–compliant tools.

The fundamental standards running contemporary digital medicine, DICOM [9, 10] and Health Level Seven International [11], were conceived and developed in the late 1980s. Certainly, these standards have not stayed intact: they went and still go through countless enhancements, managed by equally countless workgroups, vendors, and committees. However, one essential part—security—which was practically unknown to the computer gurus of the 1980s, remained nearly untouched. Despite later standard additions (e.g., part PS3.15 in the DICOM standard [9]) and legal reinforcements (e.g., HIPAA and the Health Information Technol-

ogy for Economic and Clinical Health Act), medical data security has never been soundly built into the clinical data or devices, and is still largely theoretical and does not exist in practice. As a result, DICOM security was left to generic solutions and protocols, such as firewalls, virtual private networks, or identity access management.

The major advantage of this approach was its universality: we did not have to reinvent another security wheel. Yet, inside hospital walls, this very advantage turned into a major pitfall, when all clinical security was left on the shoulders of information technology (IT) administrators. Simply speaking, medical data has been left in the hands of people who assume that its security features are built in, which they have never been. As a result, a very complex issue—medical data confidentiality, integrity, authentication, and safekeeping—has been removed from its clinical context and stuck into a huge information void between the patients, physicians, and IT administrators. Suddenly, medical security has become a do-it-yourself project [5, 8, 12, 13].

This is why we decided to study how much of this do it yourself gets actually done. The only way to do it objectively, without hospital or technology bias, was to evaluate radiology security worldwide, using the most standard medical data exchange protocols. Therefore, we relied on the DICOM standard—the reference standard of digital radiology—which provides for all image archiving, querying, transmitting, and viewing functionality. Moreover, DICOM is dedicated solely to medical data exchange and cannot be used elsewhere.

Technically, DICOM networking runs on the same computer networks used for web browsing or sending e-mails (i.e., transmission control protocol and Internet protocol [IP] networking) [10, 14]. Furthermore, DICOM software is traditionally shipped with standard radiology devices (scanners, workstations, and digital archives) in nearly plug-and-play mode, whereby the hospital IT staff only needs to assign the network IP addresses and open DICOM network ports, and then the system is ready to be used. Even the network port configuration step is often ignored: the DICOM standard defines its own default port settings, and they are rarely changed for consistency.

On the other side, the DICOM standard has never been easy. Since its inception nearly 3 decades ago, the standard has expanded into a very complex set of rules and abstractions that only experts can understand. This made DICOM unattractive for average hackers, who are more preoccupied with credit cards than a patient's chest radiographs. Consequently, DICOM's complexity and a lack of serious reviews of its vulnerabilities created a false sense of security, which is fostered by most clinical institutions. As we can tell from years of our personal experience with radiology and security projects, breaking into DICOM radiology networks from the outside is still viewed by many as a rather extraordinary and pointless adventure, but is it really? We decided to challenge this illusive assumption by studying the real scope of DICOM security leaks.

Materials and Methods

Designing DICOM Security Probing Application

The main goal of our study was to test remote radiology servers for their readiness to share medical image data with an external out-of-network computer to simulate a hacker. This could not be accomplished by simply checking for open DICOM connection ports [2], because the same ports might be used by non-DICOM applications. Therefore, we had to develop an entirely new network scanning tool (called DICOM Ping or DPing). The tool would use DICOM networking protocols and transfer syntax to speak the DICOM language to remote servers to see whether they would reply and engage in a medical data exchange (see parts PS3.7 and PS3.8 of DICOM standard [9, 10] for the exact communication protocol specifications). Thus, in simple words, DPing was acting as a standard and entirely legitimate medical application, pretending that it wanted to extract clinical data from its remote peers.

This process of DICOM communication between any two DICOM programs or devices starts with the initial network connection establishment, known as a DICOM handshake [10]; it is analogous to trying to open a web page in a web browser. During this handshake, the association-requesting application X (e.g., DPing) sends a DICOM association request to its peer application Y (e.g., a remote radiology server) over a standard network connection (Fig. 1). If this request is ignored (times out), then Y simply does not speak DICOM or is not network-accessible (Table 1, type 1). However, if Y replies with a valid DICOM message, Y is recognized as a DICOM-compliant device.

The DICOM-compliant reply from Y does not necessarily mean that its IP address is wide open for

TABLE 1: Different Types of DICOM Security Threats

Type	Request From X	Reply From Y	Interpretation	Clinical Security Threat
1	DICOM handshake	No reply	Y does not speak DICOM, or not accessible	No threat
2	DICOM handshake	Invalid reply	Y does not speak DICOM	No threat
3	DICOM handshake	DICOM association rejected	Y speaks DICOM; no firewall protection	Basic threat: DICOM application Y is open to the outside
4	DICOM handshake	DICOM association accepted	Y speaks DICOM and is ready to communicate	Elevated threat: DICOM application Y is open to the outside and can communicate DICOM data
5	DICOM query	DICOM query accepted	Y speaks DICOM and responds to medical data queries from X	High threat: outsider X can search Y for patient meta-data (e.g., names, dates of examinations, or examination descriptions)
6	DICOM data retrieve	DICOM retrieve accepted	Y speaks DICOM and can send DICOM images to X	Highest threat: outsider X can retrieve patient imaging data from Y; in this way, X gains most complete access to the patient records

Note—DICOM handshake-based types 1, 2, 3, and 4 were considered in our work.

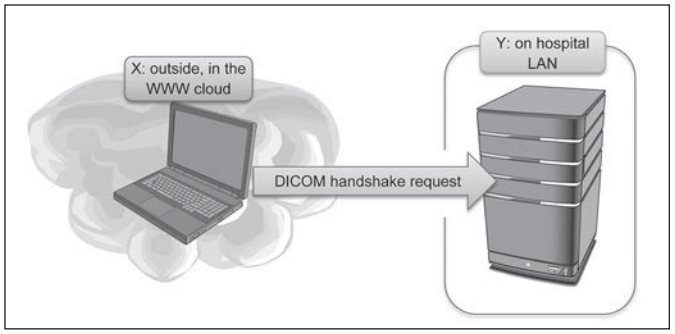

Fig. 1—DICOM application X, proposing handshake to DICOM application Y. This is layout we used for our work. WWW = World Wide Web, LAN = local area network. (Illustration by Pianykh OS)

DICOM communication. For instance, Y may receive a DICOM handshake request from X but may reject it if X is not considered a valid white-listed peer (Table 1, type 3). However, on this level, X will be already rejected in DICOM, thus revealing the clinical nature of Y, and if Y accepts the proposed handshake, it fulfills the major requirement for initiating DICOM data transfer between X and Y (Table 1, type 4 and below). From the clinical security point of view, DICOM communication acceptance opens the floodgates for partial (type 5) or complete (type 6) clinical data exchange. Thus, the security threat increases as we move to the bottom of Table 1, gaining more and more access to the clinical data of Y.

This security breach detection logic from Table 1 was incorporated into our DPing application. The application was running a sequence of steps, shown in Figure 2, probing remote devices (as their IP addresses) for their readiness to share medical data.

Initially, we did not expect to get a large list of DICOM devices: first, most of the probed IP addresses would not even exist. Second, the existing IP addresses can be firewalled to the outside requests. Then, only a very small fraction of existing and opened IP addresses would be running DICOM software. Compared with similarly designed web-browsing (i.e., http) or e-mail (i.e., simple mail transfer protocol) protocols, DICOM is still a rarity, with its strictly medical use. Finally, unsecured DICOM devices would be twice as rare. Yet, all our considerations only doubled our surprise, when we were able to discover hundreds of wide-open DICOM archives.

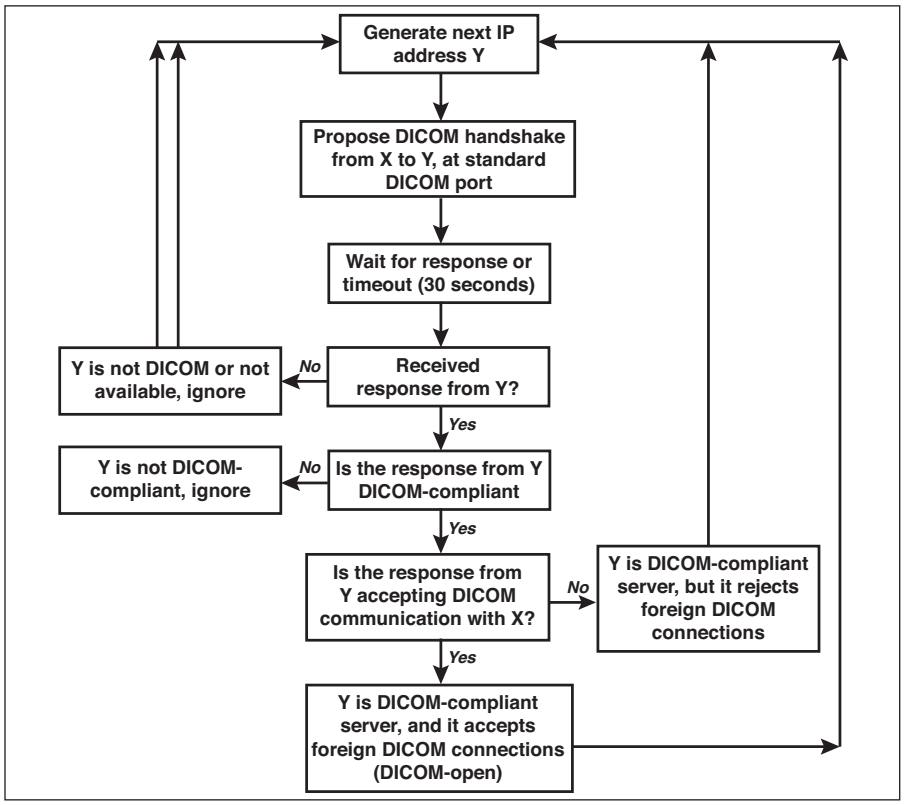

Fig. 2—Algorithm used to identify DICOM servers worldwide. See previously published description of DICOM standard [9]. IP = internet protocol.

Worldwide DICOM Search

Once we designed and implemented our DICOM-probing tool, our initial intention was to generate a small sample of random IP network addresses, check them with DPing, and find out what fraction supports DICOM and has its clinical data open to the outsiders. However, we soon realized that we could embark on a more challenging task: scanning all existing IP addresses worldwide (known as IPv4 address space).

With each IP address (e.g., 127.0.0.1) represented by its four bytes, the global IP address space amounts to 256^4, or 4,294,967,296 total addresses, but we took advantage of several elements to make the exhaustive search possible. First, a DICOM handshake is a very fast communication, exchanging only some 60–70 bytes of "Do you speak DICOM?" information. Second, we used only a single DICOM default port, as defined by the standard. Third, we gained some efficiency by not scanning RFC1918 and multicast addresses, leaving us with approximately 3,723,427,840 addresses to be scanned. Most importantly, DPing was designed as a superfast multithreaded application, running around 1300 concurrent handshake initiations.

We broke the entire IP address space into 223 octet groups, ordered by the first byte (skipping RFC1918), resulting in 16,777,216 addresses in each group. Multithreaded DPing was able to scan a single group in some 20 hours, which would result in some 200 days needed to DICOM-scan the entire IP universe. Therefore, to make DPing scans even faster and more concurrent, we enlisted Amazon EC2 to build the scanning cluster: twenty t1.micro instances running Windows Server 2012 (Microsoft), with one virtual core, up to two computing units, 0.6 gigabytes of random access memory, and low input/output per Amazon EC2 specifications. All nodes were kept to as close to 100% utilization as possible. After necessary application maintenance and configuration updates, the worldwide DICOM scanning time was reduced to a mere couple of weeks, finally making it entirely feasible for us (and for any moderately equipped hacker).

Logging and Mapping

For each IP address scanned, the DPing application logged a scanned result as one of three groups: no DICOM support (Table 1, types 1 and 2), DICOM rejected (Table 1, type 3), and DICOM open or accepted (Table 1, type 4).

A spreadsheet was built to document all type 3 and type 4 IP addresses. As mentioned, we did not expect to find a globally significant number of open

TABLE 2: Top 20 DICOM Countries, by Absolute Number, Per-Country Internet Protocol (IP) Address, and Per-Capita DICOM Server Counts

Absolute DICOM Server Count[a]			Relative DICOM Server Count Per Sampled Country IP Addresses[b]			Relative DICOM Server Count per 1,000,000 Country Population[c]		
Rating	Country	No. of Servers	Rating	Country	No. of Servers	Rating	Country	No. of Servers
1	United States	1335	1	Turkey	448	1	United States	4.21
2	India	192	2	Bolivia	435	2	Hong Kong	2.24
3	Turkey	143	3	India	346	3	Hungary	2.02
4	Brazil	118	4	Egypt	344	4	South Korea	1.96
5	South Korea	98	5	Iran	301	5	Turkey	1.87
6	Egypt	65	6	Philippines	279	6	Taiwan	1.75
7	Mexico	57	7	Hungary	225	7	Chile	1.55
8	Canada	52	8	Chile	219	8	Canada	1.47
9	South Africa	51	9	South Africa	164	9	Australia	1.41
10	China	43	10	Mexico	159	10	Portugal	1.24
11	Taiwan	41	11	Colombia	152	11	South Africa	0.96
12	Iran	40	12	Portugal	146	12	Bolivia	0.95
13	Italy	33	13	Thailand	132	13	Egypt	0.81
14	Australia	32	14	Venezuela	128	14	Colombia	0.65
15	Colombia	31	15	Brazil	125	15	Brazil	0.59
16	United Kingdom	29	16	Hong Kong	109	16	Italy	0.55
17	Chile	27	17	Taiwan	96	17	Iran	0.52
18	Philippines	24	18	South Korea	78	18	Spain	0.49
19	Spain	23	19	United States	71	19	Mexico	0.46
20	Germany	22	20	Spain	68	20	United Kingdom	0.45

[a]Absolute number of DICOM servers detected in our DICOM Ping scan, at standard DICOM port.
[b]Relative number of DICOM servers per all country IP addresses, based on our sample of 40,000 live IP addresses worldwide.
[c]Number of DICOM servers per capita.

DICOM nodes. Indeed, most scanned IP addresses fell into the first no-DICOM group (also including nonexisting and unavailable IP addresses), but the other two groups were undoubtedly the main target of our research. Although both DICOM-rejected and DICOM–open or accepted servers were reflecting the use of DICOM standard worldwide, DICOM open or accepted also provided us with the information on open unsecured DICOM entities.

Finally, geolocation was the final step in our worldwide DICOM scanning process. We wanted to study how DICOM security relates to various countries and geography. To determine this, the resulting list of DPing-scanned IP addresses was uploaded to the MaxMind geolocation service [15]. Per each DICOM IP address found, this gave us its exact location (latitude and longitude) and associated server metadata. Using Matlab (version R2014b, MathWorks) mapping functions, DICOM servers were graphically mapped to discover their density and frequency by location. Finally, we randomly selected a large 40,000 sample from the list of non-DICOM IP addresses known to exist to use as a representation of all the IP addresses worldwide.

As a result, the DICOM handshake association establishment mechanism was used to locate all worldwide radiology servers that responded to the handshake on the standard DICOM port. This highly empirical approach was chosen to provide us with the most realistic information on radiology security as it stands now. The results of our scan are summarized in the next section of the article.

Results and Discussion

The DPing scan resulted in a total of 2774 DICOM IP addresses discovered worldwide corresponding to type 3 and type 4 security threats, as defined in Table 1. Of all the IP addresses, 719 were open to DICOM communications (type 4 threat), with the remaining 2055 IP addresses rejecting a DICOM association (type 3 threat). In the following sections, we describe our specific DICOM-scanning findings, rated by different countries.

DICOM Servers Worldwide

The most immediate result of our scan was the worldwide distribution of DICOM servers by countries. It is summarized in three different ratings, gathered in Table 2. To eliminate outliers, we considered only the countries with at least 10 DICOM servers detected, which resulted in a total of 31 countries with 2610 DICOM servers (of which 679 servers were open and accepted the DICOM handshake).

Table 2 shows DICOM acceptance ratings by absolute server counts, which includes the total number of DICOM servers, rejecting or open, found during our scan. Undoubtedly, the true number of DICOM servers in any country would be significantly higher because the DPing caught only the nonfirewalled servers that were open at the standard DICOM port and responded to the DICOM handshake (via explicit rejection or acceptance). Nevertheless, Table 2 shows an excellent empirical representation of DICOM prevalence worldwide; the United States came in first place at a total of 1335 available servers, which accounted for half of all DICOM servers we detected worldwide. India is in second place with 192 DICOM serv-

ers. It is important to realize that none of these DICOM servers were protected with a firewall or the host server access control lists; nonlocal untrusted source addresses were allowed to access these clinical archives.

Although Table 2 represents the absolute DICOM server counts, given different countries' clinical infrastructures and populations, we were equally interested to take these factors into account with relative counts. Clearly, we could not relate the number of detected DICOM servers to the count of all undetected ones, because the latter was impossible to determine: by definition, one cannot count the hidden. Moreover, we did not find any reliable worldwide reports that would help us accurately estimate this value. Therefore, we developed an alternative and equally interesting approach, presented in Table 2, relating discovered DICOM servers to the IT infrastructure and the population of each country.

Table 2 shows the DICOM-to-all ratio, which expresses DICOM servers as a fraction of all IP addresses associated with the same country (according to our 40,000 live non-DICOM IP address sample mentioned earlier). Note how this relative DICOM rating changes the outcomes: the top country is Turkey with a relative score of 448, second place goes to Bolivia at 434, and the United States moves to the 19th place. This change in leading countries may be explained if we look at this rating from a security angle.

Table 2 also shows the ratio of unprotected DICOM servers (type 3 and 4 security threats) per each country's IP address pool. Therefore, the countries with less-developed clinical security climb to the top of Table 2: these countries must start paying more attention to protecting their clinical data.

Finally, Table 2 rates the top 20 countries by the accessibility of their digital medicine. The relative DICOM server per capita count shows the number of DICOM servers detected per 1,000,000 of the country's population. The United States wins this DICOM density battle by a large margin, showing that its DICOM infrastructure is the most accessible to its patients. Interestingly, Hungary is the only European country that makes the top 10 on this list, as well as in Table 2, with only 20 DICOM servers detected (so that it did not make the top 20 with regard to absolute number of DICOM servers). Hungary also achieves the highest per-IP and per-capita DICOM density in Europe.

To visualize DICOM server density worldwide, we used geolocation services with Matlab plotm function (version R2014b, MathWorks), resulting in the maps shown in Figure 3. The DICOM IP address map shows all 2774 DICOM servers found in our scan; the non-DICOM IP address map shows a sample of 40,000 live non-DICOM IP addresses, which we used to represent the overall live IP distribution worldwide. The maps illustrate our earlier observations, attributing the largest DICOM cluster to the United States. India and parts of South America follow, but Europe, although rich in IP addresses, shows a less dense presence of DICOM servers, as one would expect if network security was uniform.

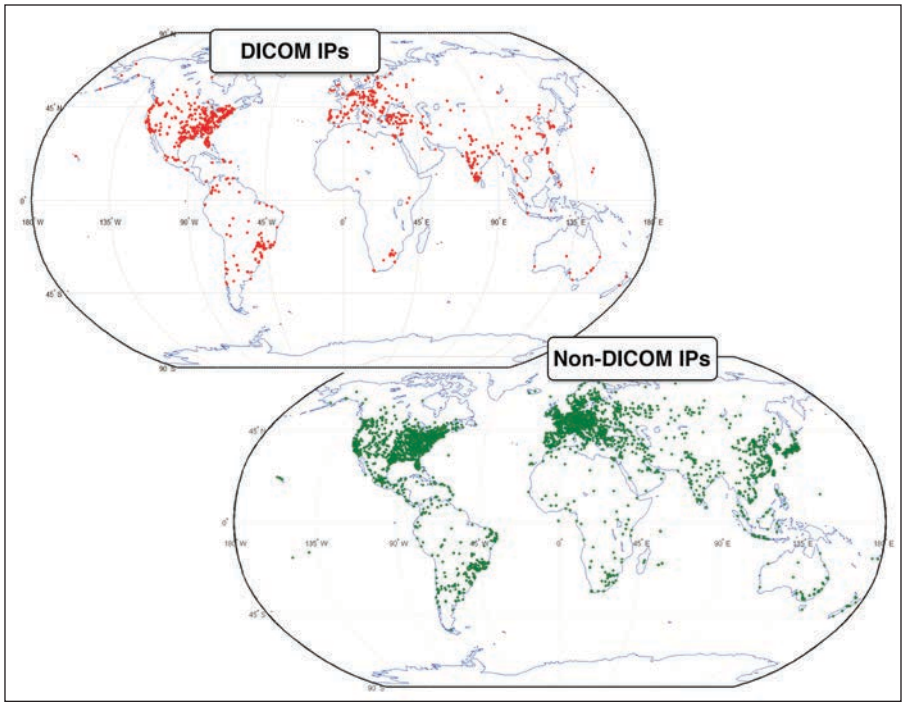

Fig. 3—Distribution of DICOM and non-DICOM internet protocol (IP) addresses worldwide. Note similarities and differences. For example, large number of IP addresses in Europe does not translate into large number of DICOM IP addresses. (Illustration by Pianykh OS)

DICOM Security Threats Worldwide

If one wants to study the lack of DICOM security, Table 2 would make a good starting point because the table is based on the DICOM servers that we were able to reach from the public Internet. Although most of the detected servers explicitly rejected our DICOM handshake, they still had their DICOM ports open to elementary denial-of-service attacks. In essence, these servers were most likely rejecting our DICOM communication requests simply because their vendors or support teams had configured the devices' white lists of acceptable DICOM peers, which would block our foreign connection; it was the only basic defense provided by some DICOM software. At the same time, their IT administrators apparently did not put a lot of effort into securing the network perimeter, which lacked simple firewall protection, because we were able to reach these servers from the outside.

Nonetheless, the most dangerous situation arises when DICOM servers are willing to communicate with the strangers, accepting their handshakes (Table 1, type 4). As we mentioned earlier, this resulted in 719 DICOM-open servers worldwide, which we detected with our DPing scan. Similarly to Table 2, these results are summarized in Table 3, with the same rating method.

Note that, unfortunately, the countries with the most prevalent DICOM infrastructure (e.g., United States) also tend to lead in the most unsecured DICOM ratings: Table 3 (left) shows U.S. leadership in the absolute count of open DICOM archives, and Table 3 (right) shows the same result per capita. The latter finding simply implies that, in the United States, patients run into the highest risk of having their medical records stolen or compromised, which is becoming more and more apparent with the recent reports on hospital data leaks [3, 4, 6]. This leads us to a rather

TABLE 3: Open DICOM Servers Worldwide, Top 20 Countries

Absolute No. of Open DICOM Servers			Relative DICOM Server Count per Sampled Country Internet Protocol Addresses			Relative DICOM Server Count per 1,000,000 Country Population		
Rating	Country	No. of Servers	Rating	Country	No. of Servers	Rating	Country	No. of Servers
1	United States	346	1	Iran	256	1	United States	1.09
2	Brazil	51	2	Bolivia	174	2	Turkey	0.64
3	Turkey	49	3	Turkey	154	3	Taiwan	0.60
4	Iran	34	4	Thailand	94	4	Australia	0.53
5	India	28	5	Philippines	70	5	Iran	0.44
6	South Korea	15	6	Chile	57	6	Hungary	0.40
7	Taiwan	14	7	Brazil	54	7	Chile	0.40
8	Mexico	14	8	India	50	8	Bolivia	0.38
9	Canada	13	9	Hungary	45	9	Canada	0.37
10	Australia	12	10	Mexico	39	10	South Korea	0.30
11	Spain	11	11	Taiwan	33	11	Hong Kong	0.28
12	China	11	12	Spain	33	12	Brazil	0.25
13	Thailand	10	13	Argentina	26	13	Spain	0.23
14	Germany	9	14	Egypt	21	14	Thailand	0.15
15	Russia	8	15	Australia	21	15	Argentina	0.15
16	Chile	7	16	United states	18	16	Mexico	0.11
17	Argentina	6	17	Poland	15	17	Germany	0.11
18	Philippines	6	18	Russia	15	18	Poland	0.10
19	Italy	5	19	Hong Kong	14	19	Italy	0.08
20	Hungary	4	20	Canada	13	20	Philippines	0.06

gloomy conclusion that, despite several decades of digital medicine, clinical security is still largely neglected, even in the countries where security should have been implemented years ago.

Finally, it is instructive to see what fraction of all DICOM servers was left handshake-open in each country. This ratio is shown in Table 4 as the number of open DICOM servers divided by the total number of DICOM servers per country. In many ways, Table 4 should be viewed as a DICOM security ignorance rating. Although the largest DICOM country, the United States, moves now to place 15, the result is still hardly flattering, with 26% of its DICOM servers open to communications with unknown external entities.

One may argue that some of these wide-open DICOM servers were not holding the actual patient data, but we do not find this argument to be sound. Unlike similar transmission control protocols and IP-based protocols (e.g., http for web-browsing or simple mail transfer protocol for e-mail), DICOM is entirely dedicated to the patient imaging data and serves no other purpose. That is, the high rates of unsecured DICOM servers cannot be explained by rather exotic scenarios of running DICOM for nonpatient nonradiology uses. This is why even 26% of the open U.S. DICOM servers manifest an enormous security hole. In addition, with seamless DICOM data exchange, patient data can be easily transmitted from more-secure to less-secure radiology archives (an extremely common scenario for patients traveling between different hospitals, for area-wide hospital networks, for hospital projects with DICOM vendors and medical companies, and so forth). Thus, even a small fraction of open DICOM servers can put virtually any patient's records at risk, regardless of how securely they were initially acquired or stored. We only hope that the clinical administrators from the countries topping our ratings would start paying attention to these results and proactively securing their patient data.

Correlation Analysis

If we view open DICOM servers (Table 3) as the main precursor for country's medical security breaches, what factors contribute to the open server numbers? Is it the overall DICOM server count, country population, IT infrastructure (in terms of IP address density), or anything else?

Without going into complex analysis, we used basic linear regression to express the number of open DICOM servers as a combination of those factors. The results are presented in Table 5. As Table 5 indicates, there is only one statistically significant factor ($p = 4.05311 \times 10^{-11}$), which almost exactly ($R^2 = 0.99417$) correlates with the open server count: the total number of DICOM servers per country. Its coefficient of 0.251517876 indicates that roughly a quarter of all DICOM servers found in our scan were open to DICOM communications. Note that this is consistent with our worldwide DICOM server counts (679 open out of 2610), and with the U.S. open server ratio (26%, Table 4), with the United States being the country accounting for half of the world's DICOM servers. Certainly, this ratio makes obvious sense IT-wise: the more servers we create, the more leaks we get. However, this is precisely the trend to be reversed if we ever want to take our clinical

TABLE 4: Rating the Lack of DICOM Server Security

Rating	Country	Total No. of DICOM Servers[a]	No. of Open DICOM Servers	Ratio of Open DICOM Servers to Total No. of Servers (%)
1	Iran	40	34	85
2	Thailand	14	10	71
3	Spain	23	11	48
4	Argentina	13	6	46
5	Russia	18	8	44
6	Brazil	118	51	43
7	Germany	22	9	41
8	Bolivia	10	4	40
9	Australia	32	12	38
10	Turkey	143	49	34
11	Taiwan	41	14	34
12	Poland	12	4	33
13	Japan	11	3	27
14	Chile	27	7	26
15	United States	1335	346	26
16	China	43	11	26
17	Canada	52	13	25
18	Philippines	24	6	25
19	Mexico	57	14	25
20	Hungary	20	4	20

[a]Absolute number of servers detected in our DICOM Ping scan, at standard DICOM port.

security seriously. Providing more digital medicine services to our patients should not mean putting them at proportionally higher security risks.

Limitations

Undoubtedly, our work has several natural limitations. First, during our worldwide DPing scan, each IP address was probed only once for scanning efficiency. If the IP address was not available at that moment because of off-work hours, maintenance, or other factors, it was not retried and was discarded as unavailable. Thus, we might have missed some DICOM hits, but we are sure that this miss was not biased because of the random nature of our scanning. Moreover, one would expect clinical archives to be on all the time. Second, only the default DICOM port was used. It was done intentionally because of its frequent use (and abuse) and to reduce the scanning load. As a result, we did not study the other ports. Third, as mentioned earlier, we assumed that DICOM servers are used for clinical purposes. To us, this is a very reasonable assumption: DICOM is a medical imaging standard and is not used for anything but medical imaging. Even if one presumes that some of the servers were not entirely clinical (e.g., a rather small fraction of research servers), the research images would originate from the patient scans as well. Therefore, exposing DICOM servers to the outside would be a serious security gap regardless of whose images they might store. Fourth, clearly, geolocation pinpoints the coordinates of the server provider, but it cannot tell who is really using the server. We do understand that a server registered in the United States could be used for a project in Turkey or Bolivia. Nonetheless, from our own experience, the vast majority of DICOM servers are used at the places of their registration: it is becoming mandatory in many countries to store all patient data locally [7].

TABLE 5: Factors Influencing the Number of Open DICOM Servers

Factor	Coefficients	Standard Error	*t* Statistic	*p*	Lower 95%	Upper 95%
Regression intercept	−3.554281483	3.79204926	−0.937298342	0.357942258	−11.3806865	4.27212353
No. of open DICOM servers	0.251517876[a]	0.022195649	11.33185487	4.05311E-11[a]	0.205708308	0.297327445
All country IP addresses	0.000654569	0.001623726	0.403127865	0.690422991	−0.002696636	0.004005775
Ratio of DICOM servers to all IP addresses	−0.028708031	0.021514578	−1.334352495	0.194611485	−0.073111937	0.015695876
Ratio of open DICOM servers to all IP addresses	0.095475176	0.051007593	1.871783603	0.073473824	−0.009799322	0.200749673
Ratio of open DICOM servers to all DICOM servers	16.31343213	10.52799505	1.549528857	0.134341929	−5.415281709	38.04214597
Population	-5.66053×10^{-9}	3.32026×10^{-9}	−1.704846421	0.101136295	-1.25132×10^{-8}	1.19215×10^{-9}

Note—R^2 = 0.99417 for all comparisons. IP = internet protocol.
[a]Statsitically significant.

All in all, these limitations would be expected for an empirical project like ours. Exceptions happen, but we believe that they do not affect the overall trends and the validity of our results.

Disclaimer

This project was based entirely on a standard DICOM communication handshake (association establishment process, as described in the DICOM standard, part PS 3.7 [9]). As a result, no sensitive clinical data have been exchanged or compromised, and no interference was created or intended to the functionality of the servers. Similarly, no malicious, destructive, or DICOM-incompliant instructions were ever attempted or transmitted.

For the same reason, we do not intend to publish any detailed information pointing to the actual unsecured DICOM IP addresses. Our initial intent was to contact their hospitals privately, but we found many more leaks than we expected. Instead, we will be glad to help clinical centers in identifying their security breaches by request. Please do contact us if you have doubts about your DICOM security.

Conclusion

The introduction of digital record keeping into medicine has made many projects possible, but not only for those with good intentions. In a complex universe of clinical information technology, where patients, physicians, and IT professionals speak completely different languages and have entirely different expectations, too many things can fall between the cracks or simply be ignored. Medical devices and archives, left wide open at their default DICOM ports and settings, are by far the most common security problem. During our study, we stopped only one step away from actually downloading patient data from the remote facilities we have identified. We stopped because it was illegal, yet it was completely possible. This is what needs to be finally understood and implemented within every radiology training and management project. Otherwise, we simply fail to provide our patients with hacker-proof digital medicine.

The distribution of DICOM servers worldwide presents another very interesting outcome of this work. To our knowledge, this is the first practical result showing the extent of the digital radiology worldwide presence. In many ways, these results challenge what one would expect as unusual leaders appear in our charts. In this regard, we believe that our empirical approach provides us with the most realistic data, and we are planning to continue our work in this direction.

Acknowledgment

We thank AlgoM Corp. for their collaboration in developing the DPing utility.

References

1. Mearian L. More than 80% of healthcare IT leaders say their systems have been compromised. ComputerWorld website. www.computerworld.com/article/2975988/healthcare-it/more-than-80-of-healthcare-it-leaders-say-their-systems-have-been-compromised.html. Published August 27, 2015. Accessed October 1, 2015
2. Moses V, Korah I. Lack of security of networked medical equipment in radiology. *AJR* 2015; 204:343–353
3. Ouellette P. Cogent Healthcare contractor M2ComSys breaches patient data. Health IT Security website. healthitsecurity.com/2013/08/12/cogent-healthcare-contractor-m2comsys-breaches-patient-data/. Published August 12, 2013. Accessed September 1, 2014
4. Pagliery J. Hospital network hacked, 4.5 million records stolen. CNN Money website. money.cnn.com/2014/08/18/technology/security/hospital-chs-hack/. Published August 18, 2014. Accessed September 1, 2014
5. Simplicio MA, Iwaya LH, Barros BM, Carvalho TC, Naslund M. SecourHealth: a delay-tolerant security framework for mobile health data collection. *IEEE J Biomed Health Inform* 2015; 19:761–772
6. Associated Press. Study: Utah health breach could approach $406M. Insurance Journal website. www.insurancejournal.com/news/west/2013/05/01/290357.htm. Published May 1, 2013. Accessed September 1, 2014
7. Hiller J, McMullen MS, Chumney WM, Baumer DL. Privacy and security in the implementation of health information technology (electronic health records): U.S. and EU compared. Published 2011. www.bu.edu/law/central/jd/organizations/journals/scitech/volume171/documents/Hiller_Web.pdf. Accessed September 1, 2014
8. Kommeri J, Niinimäki M, Müller H. Safe storage and multi-modal search for medical images. *Stud Health Technol Inform* 2011; 169:450–454
9. DICOM Committee. DICOM PS3.15 2014a: security and system management profiles. National Electrical Manufacturers Association website. dicom.nema.org/medical/dicom/2014a/output/pdf/part15.pdf. Published 2014. Accessed September 1, 2014
10. Pianykh OS. *Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide*. Berlin, Germany: Springer-Verlag, 2012
11. Health Level Seven International Standard. www.hl7.org/. Accessed October 1, 2015
12. Viswanathan P, Krishna PV. A joint FED watermarking system using spatial fusion for verifying the security issues of teleradiology. *IEEE J Biomed Health Inform* 2014; 18:753–764
13. Tan CK, Ng JC, Xu X, Poh CL, Guan YL, Sheah K. Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability. *J Digit Imaging* 2011; 24:528–540
14. DICOM Committee. DICOM PS3.1 2014a: introduction and overview. National Electrical Manufacturers Association website. dicom.nema.org/medical/dicom/2014a/output/pdf/part01.pdf. Published 2014. Accessed September 1, 2014
15. MaxMind. GeoIP databases & service: industry leading IP intelligence. MaxMind website. www.maxmind.com/en/geolocation_landing. Accessed January 8, 2016