aplite

Tailor-made IT Security

Millions of Patient Records at Risk

The Perils of Legacy Protocols

Sina Yazdanmehr <sina@aplite.de>

For more than 30 years, DICOM, standard protocol in medical imaging, has been a lifesaver

DICOM has become a known source of sensitive data leakage

2019 [1] Millions of Australians' sensitive medical images, data left openly accessible

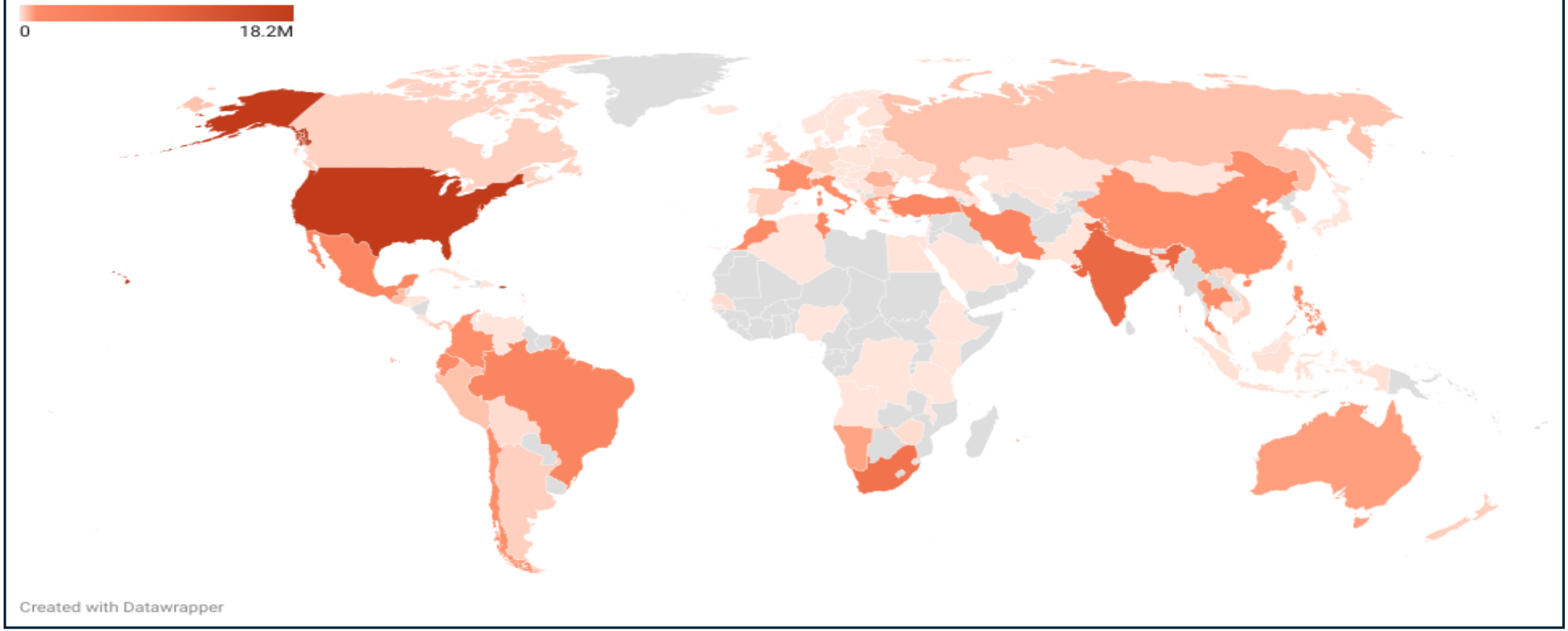
2021 [2] 45 million unique DICOM files stored on over 2,140 servers in 67 countries

2023 **How about now?**

1. https://itnews.com.au/news/millions-of-australians-sensitive-medical-images-data-left-openly-accessible-531248
2. https://cybelangel.com/stop-medical-device-leaks/

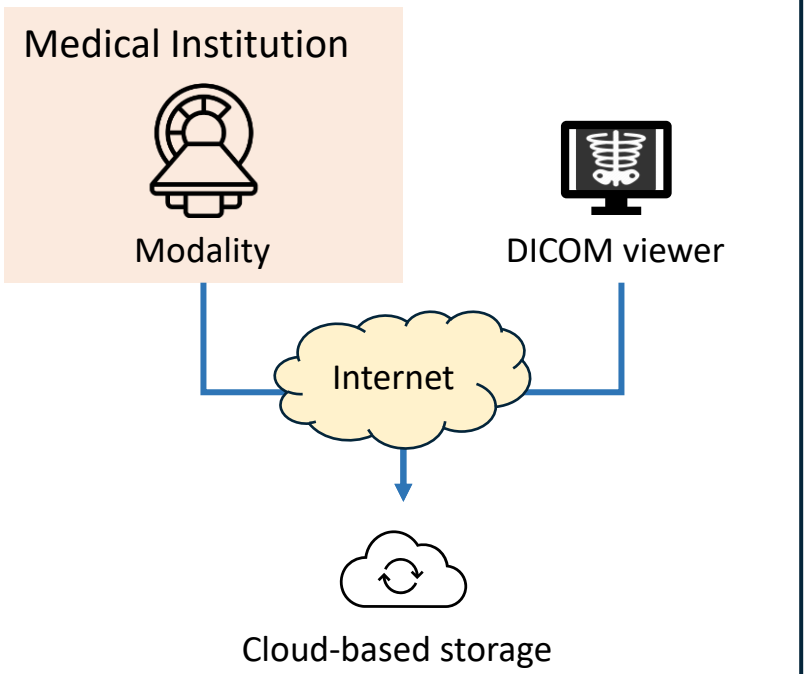
2023 Update: the leakage is increasing globally

Over 59M patients' personal and medical records are accessible on the internet



Health sector is embracing new technologies like Cloud while still using legacy protocols

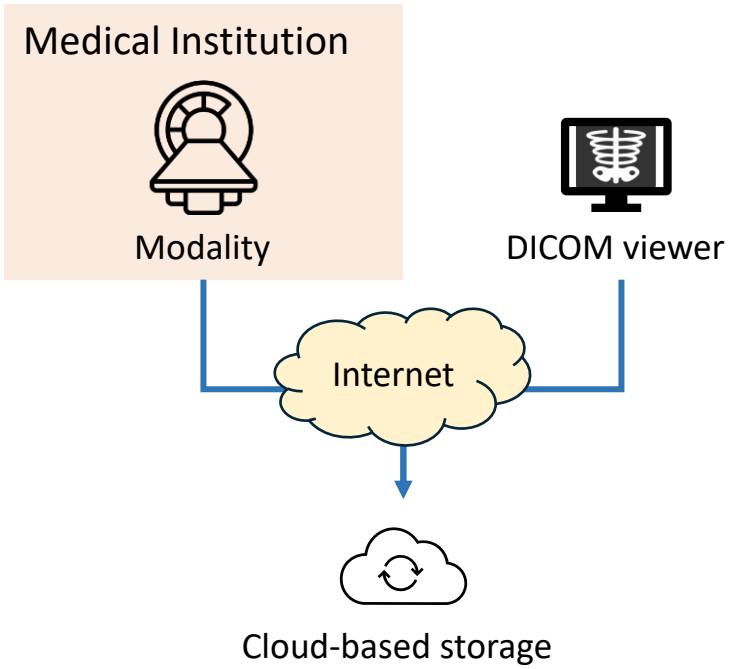
The industry is moving towards cloudification



- Many medical institutions now use the Cloud
- The Cloud-based servers are often publicly accessible due to lack of knowledge or misconfiguration

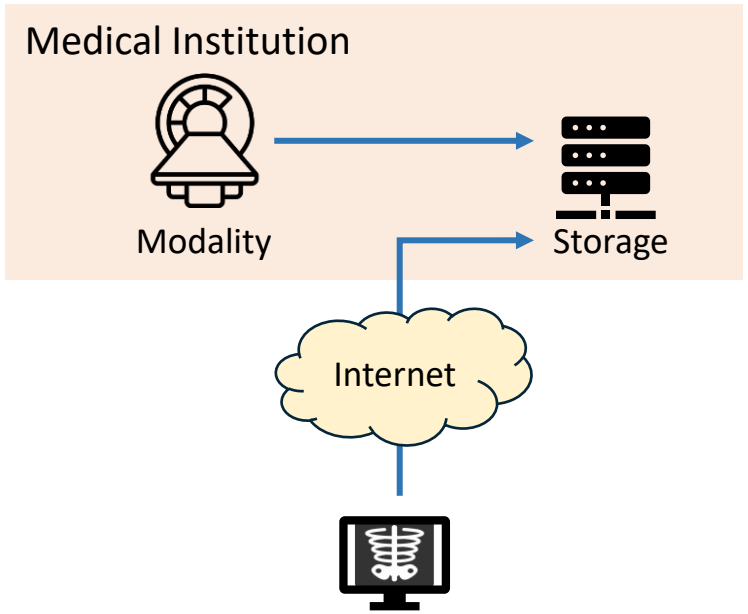
This shift forces small business to align their workflows with the new trends

The industry is moving towards cloudification



- Many medical institutions now use the Cloud
- The Cloud-based servers are often publicly accessible due to lack of knowledge or misconfiguration

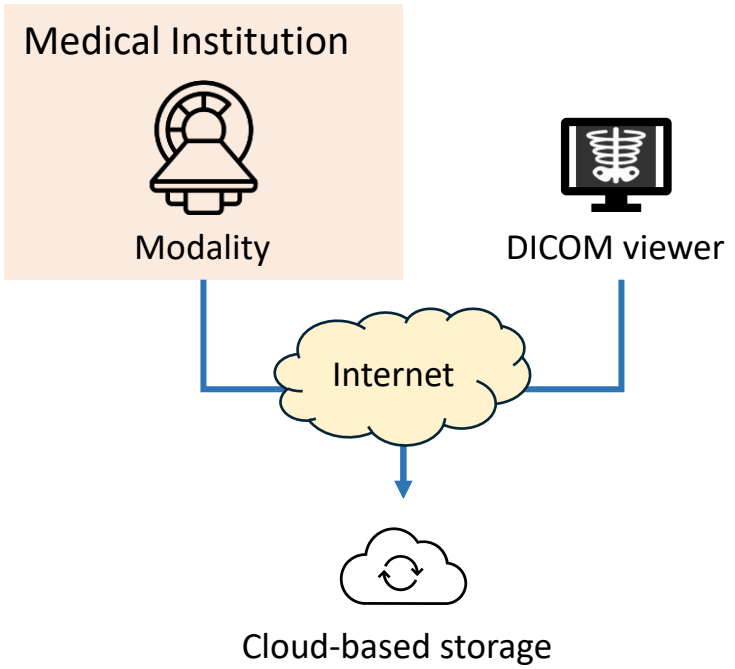
Small businesses try to adopt the new trend



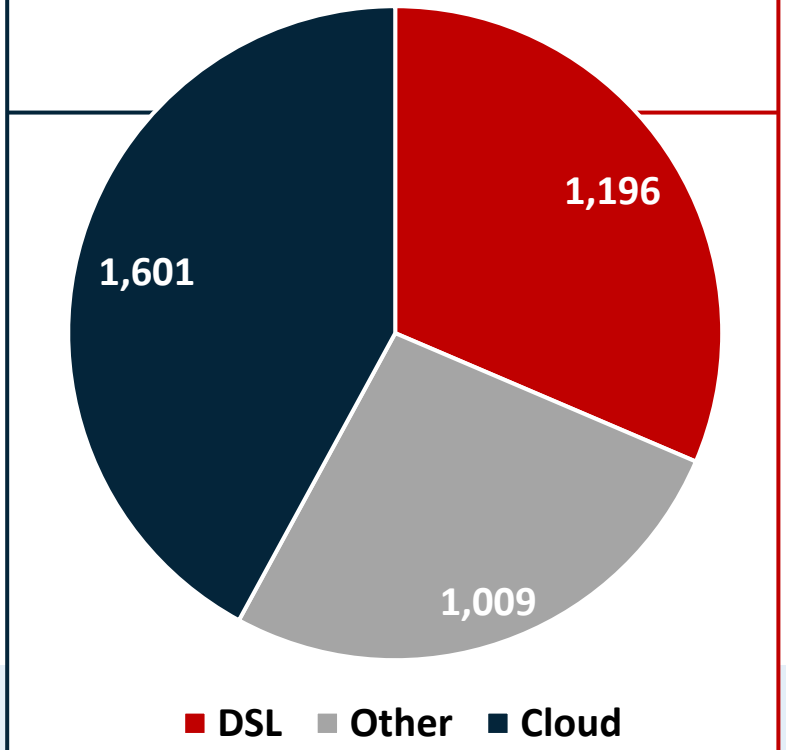
- Many small medical facilities, like imaging centers, often use on-premises solutions within their networks
- They lack expertise or resources for complex network setups

3,806 DICOM servers on the internet – over 73% hosted on the Cloud or exposed via DSL

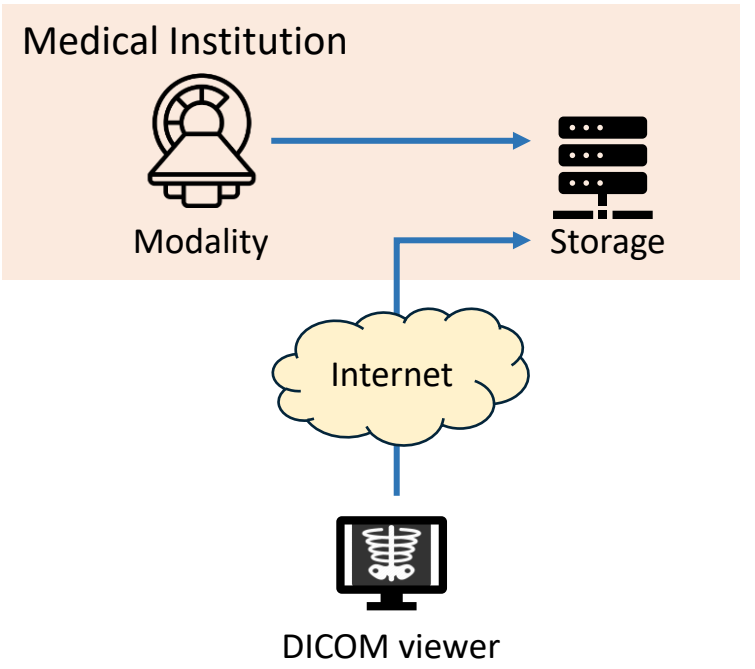
The industry is moving towards cloudification



- Many medical institutions now use the Cloud
- The Cloud-based servers are often publicly accessible due to lack of knowledge or misconfiguration



Small businesses try to adopt the new trend



- Many small medical facilities, like imaging centers, often use on-premises solutions within their networks
- They lack expertise or resources for complex network setups

We scanned the whole internet for more than six months assessing the exposure

1. Examined the protocol

- Examined DICOM protocol to uncover all possible attacks

2. Scan

- Scanned the whole internet regularly
- From different locations and networks

3. Enumeration

- Tested data retrieving methods on the discovered servers

4. Analyze

- Removed false positive results
- Removed unrelated results, e.g., honeypots, vet servers, etc.

We scanned the whole internet for more than six months assessing the exposure

1. Examined the protocol

- Examined DICOM protocol to uncover all possible attacks

2. Scan

- Scanned the whole internet regularly
- From different locations and networks

3. Enumeration

- Tested data retrieving methods on the discovered servers

4. Analyze

- Removed false positive results
- Removed unrelated results, e.g., honeypots, vet servers, etc.

Personal Identifiable (PII)

16.1 M

Information like:

- Full name
- Date of birth
- Address
- Telephone number
- Gender
- In some cases, Social Security Number (SSN)

Protected health (PHI)

43.5 M

Information like:

- Result of examination
- Place, date, and time of examination
- Referring physician
- Used modality

The permanence of this data amplifies the danger of leakage

We scanned the whole internet for more than six months assessing the exposure

1. Examined the protocol

- Examined DICOM protocol to uncover all possible attacks

2. Scan

- Scanned the whole internet regularly
- From different locations and networks

3. Enumeration

- Tested data retrieving methods on the discovered servers

4. Analyze

- Removed false positive results
- Removed unrelated results, e.g., honeypots, vet servers, etc.

Personal Identifiable (PII)

16.1 M

Information like:

- Full name
- Date of birth
- Address
- Telephone number
- Gender
- In some cases, Social Security Number (SSN)

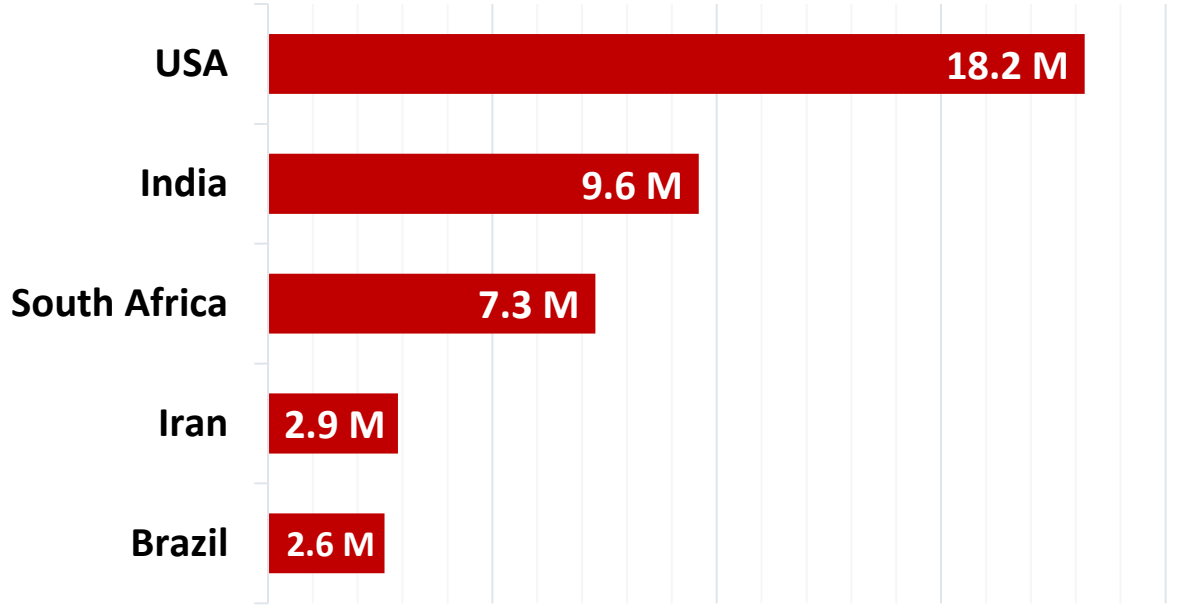
Protected health (PHI)

43.5 M

Information like:

- Result of examination
- Place, date, and time of examination
- Referring physician
- Used modality

Top 5 countries out of 111 with the most exposure



The permanence of this data amplifies the danger of leakage

Many servers hosted in the USA store data from other countries

Agenda

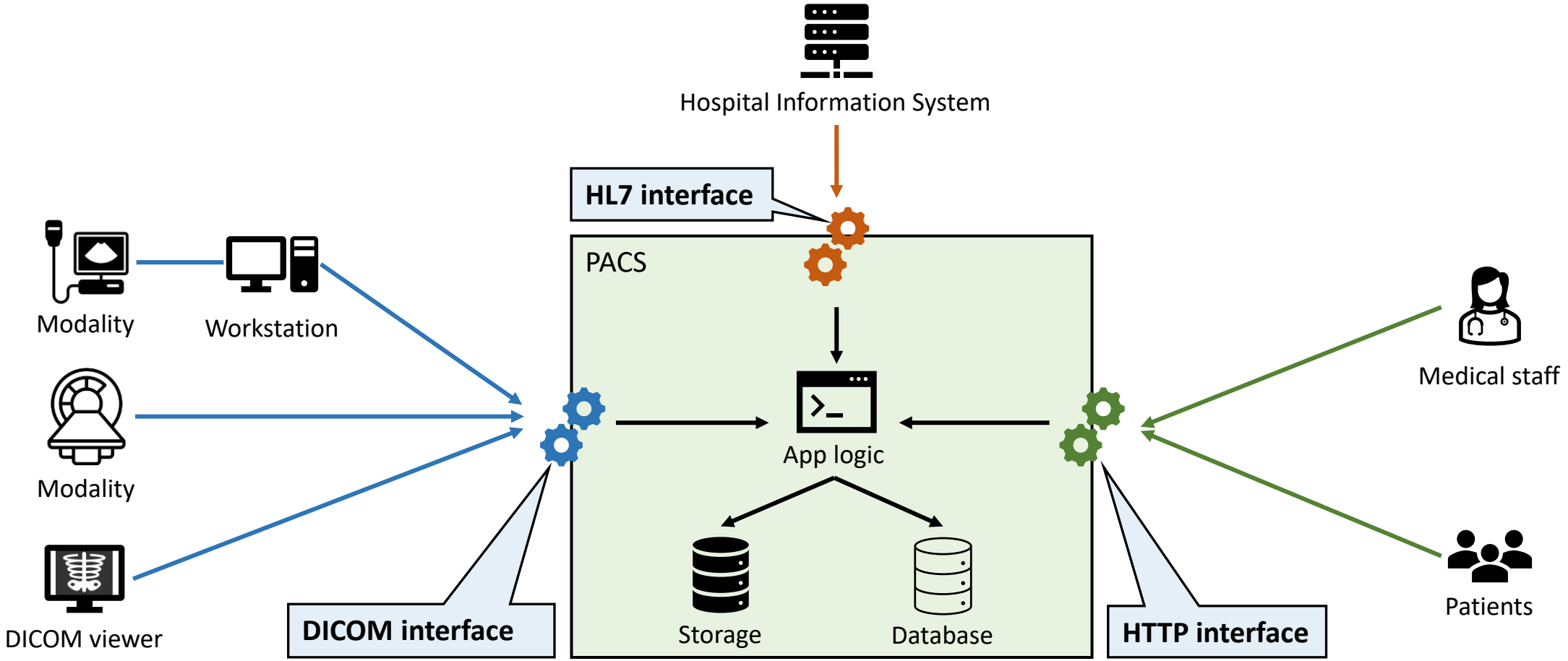
1| Introduction and results of the internet-wide research

2| DICOM: Deep dive and attack scenarios

3| Countermeasures and takeaways

PACS streamlines management and transmission of medical images

Picture Archiving and Communication System (PACS) is a medical image system that saves, finds, and shares medical images and reports



Modality = Medical imaging device — HTTP — DICOM — HL7

DICOM data model is composed of four main Information Entities

Image

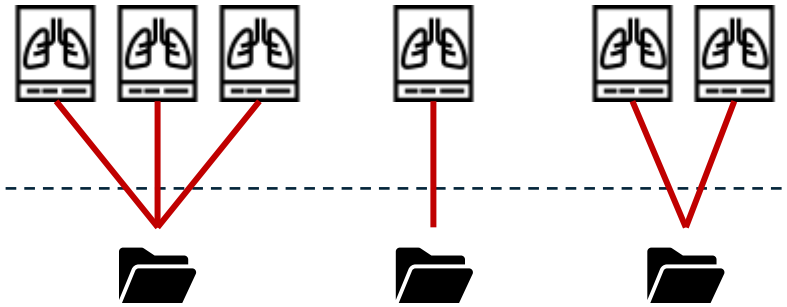
Each Information Entity (IE) represents certain data

- Individual medical images or data files
- Elements like acquisition and position attributes, image type, instance number, samples per pixel, etc.

DICOM data model is composed of four main Information Entities

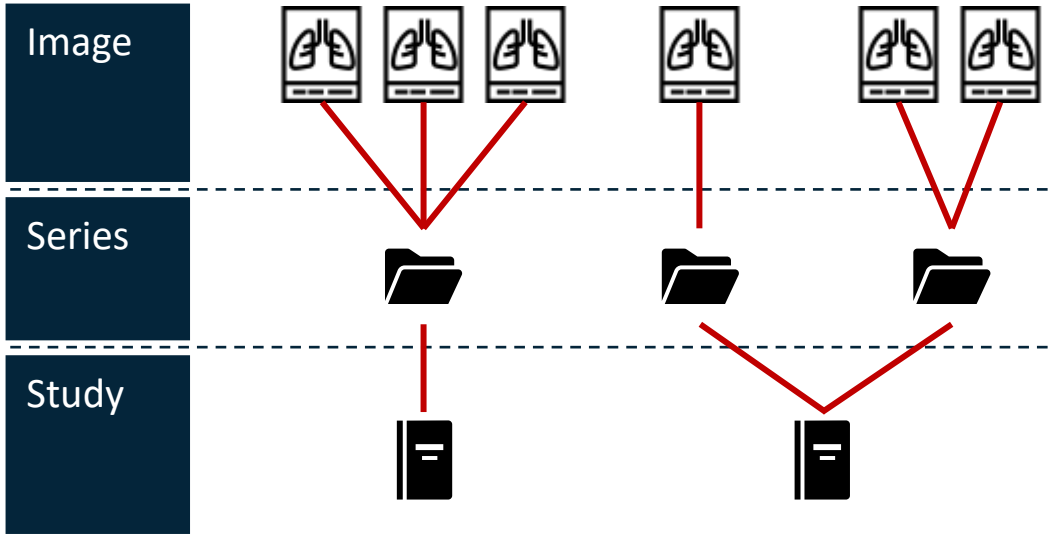
Image

Series



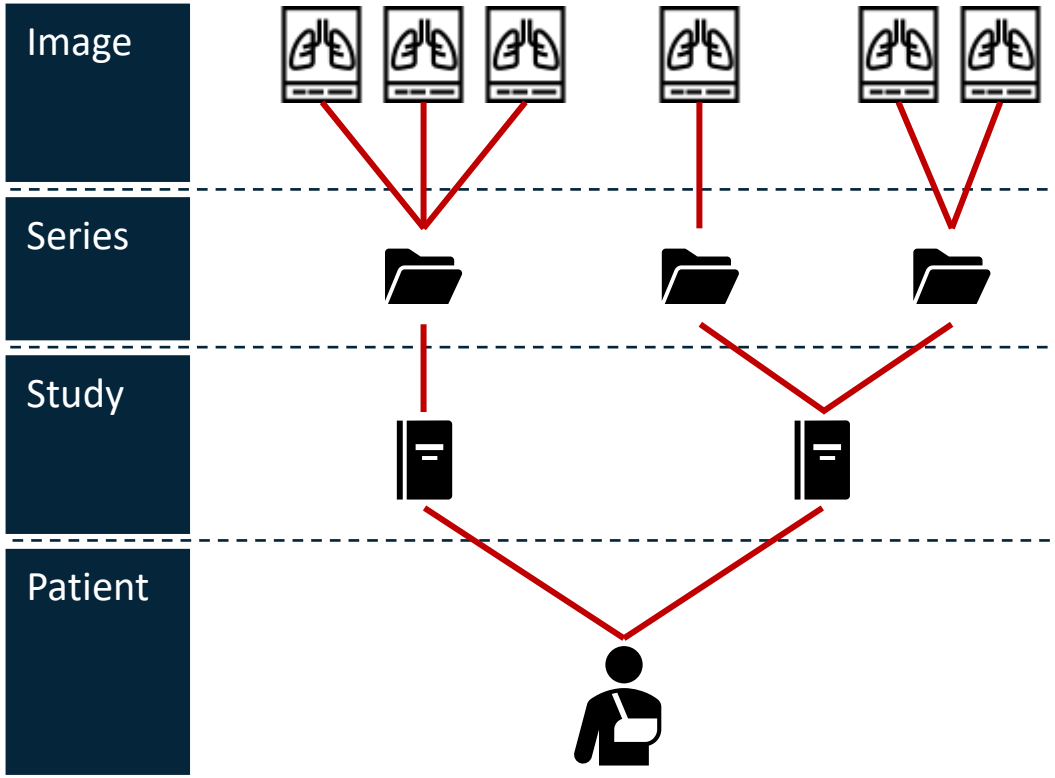
Each Information Entity (IE) represents certain data
• Individual medical images or data files • Elements like acquisition and position attributes, image type, instance number, samples per pixel, etc.
• Group of related images, e.g., a set of MRI scans • Elements like series' UID, modality type, series number, etc.

DICOM data model is composed of four main Information Entities



Each Information Entity (IE) represents certain data
• Individual medical images or data files • Elements like acquisition and position attributes, image type, instance number, samples per pixel, etc.
• Group of related images, e.g., a set of MRI scans • Elements like series' UID, modality type, series number, etc.
• Specific medical examination • Elements like study ID, date, time, referring physician, study UID, etc.

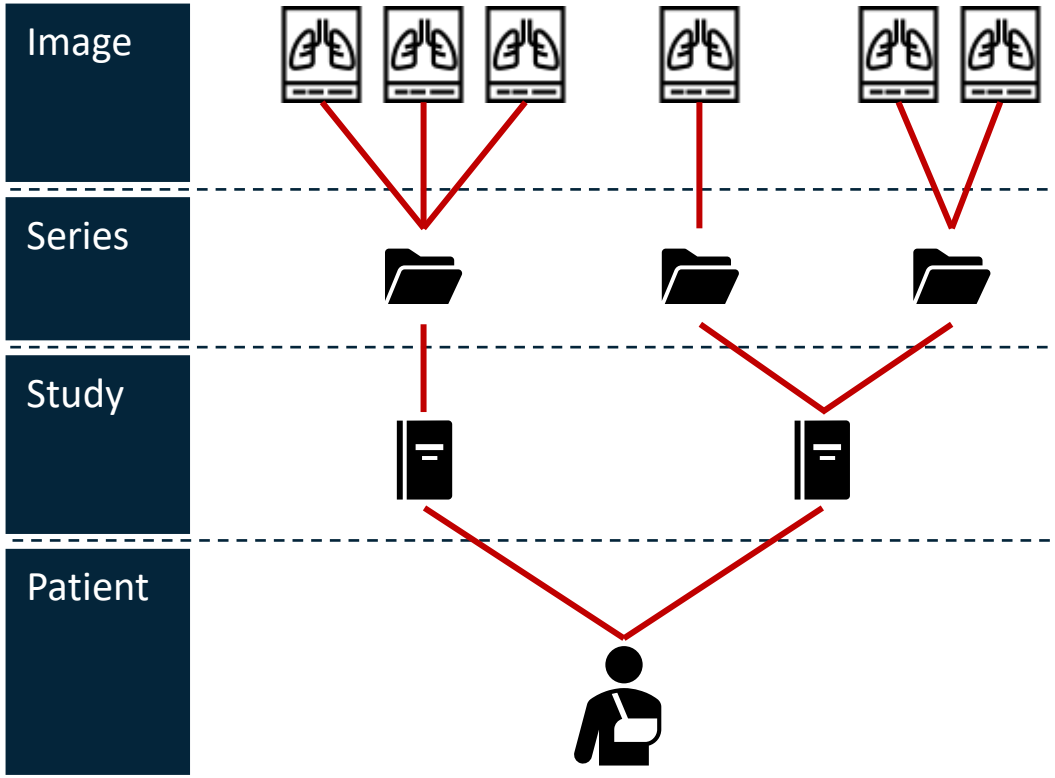
DICOM data model is composed of four main Information Entities



Each Information Entity (IE) represents certain data
• Individual medical images or data files • Elements like acquisition and position attributes, image type, instance number, samples per pixel, etc.
• Group of related images, e.g., a set of MRI scans • Elements like series' UID, modality type, series number, etc.
• Specific medical examination • Elements like study ID, date, time, referring physician, study UID, etc.

• An individual patient
• Patient's information in elements like:
  • Identification: full name, patient ID, etc.
  • Demographics: age, gender, birthdate, etc.

DICOM data model is composed of four main Information Entities



Each Information Entity (IE) represents certain data

- Individual medical images or data files
- Elements like acquisition and position attributes, image type, instance number, samples per pixel, etc.

- Group of related images, e.g., a set of MRI scans
- Elements like series' UID, modality type, series number, etc.

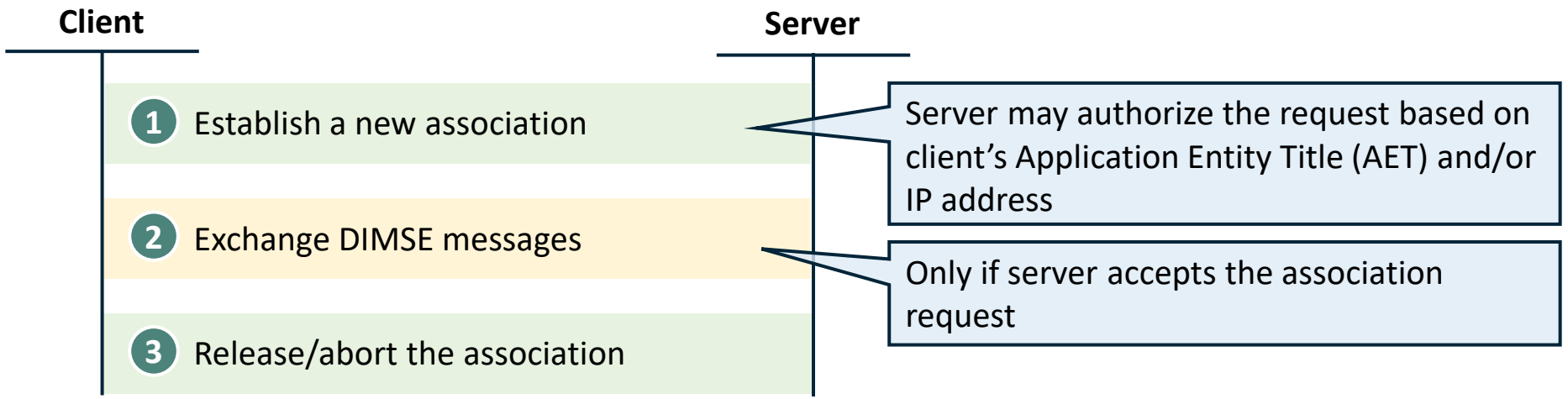
- Specific medical examination
- Elements like study ID, date, time, referring physician, study UID, etc.

- An individual patient
- Patient's information in elements like:
  - Identification: full name, patient ID, etc.
  - Demographics: age, gender, birthdate, etc.

Elements are structured by four attributes

Attribute	Description	Example
Tag	Uniquely defines the element.	(0010,0010)
VR	Defines the data type in a 2-char code.	PN (Person Name)
Length	Length of the value.	9 bytes
Value Field	Actual value	Doe^John

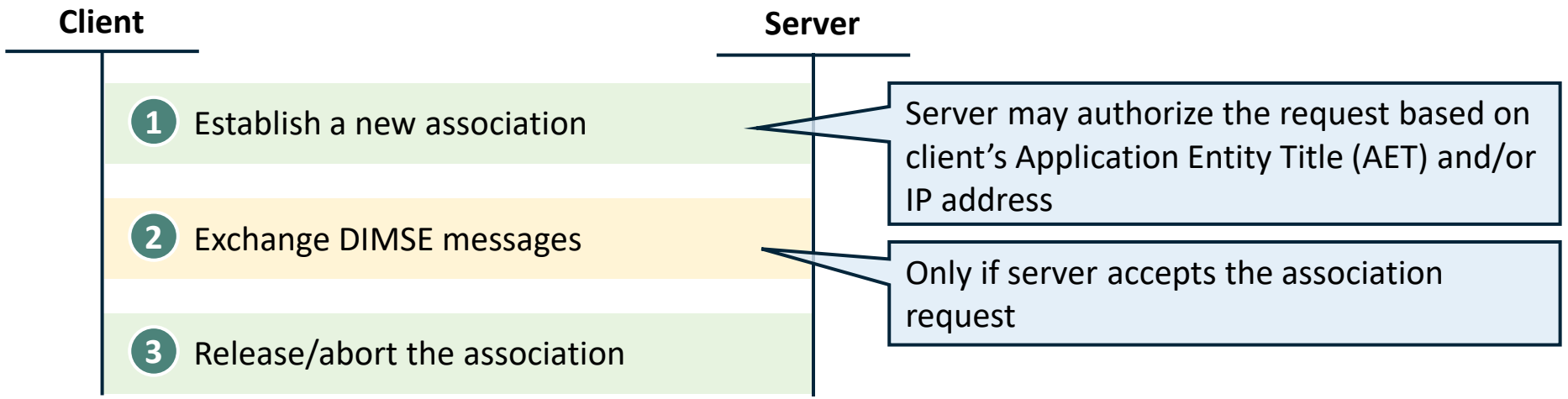
DICOM network protocol is composed of three key steps with different service elements



Association Control Service Element (ACSE)

DICOM Message Service Element (DIMSE)

DICOM network protocol is composed of three key steps with different service elements



Type	Service	Security risk
Query and retrieve	**C-FIND.** Searches for objects **C-GET.** Fetches objects completely **C-MOVE.** Moves objects to a server	**Data leakage.** An attacker can use these services to access patient's personal and medical data.
Store	**C-STORE.** Stores objects on server	**Data tampering.** An attacker can tamper existing series using this service.

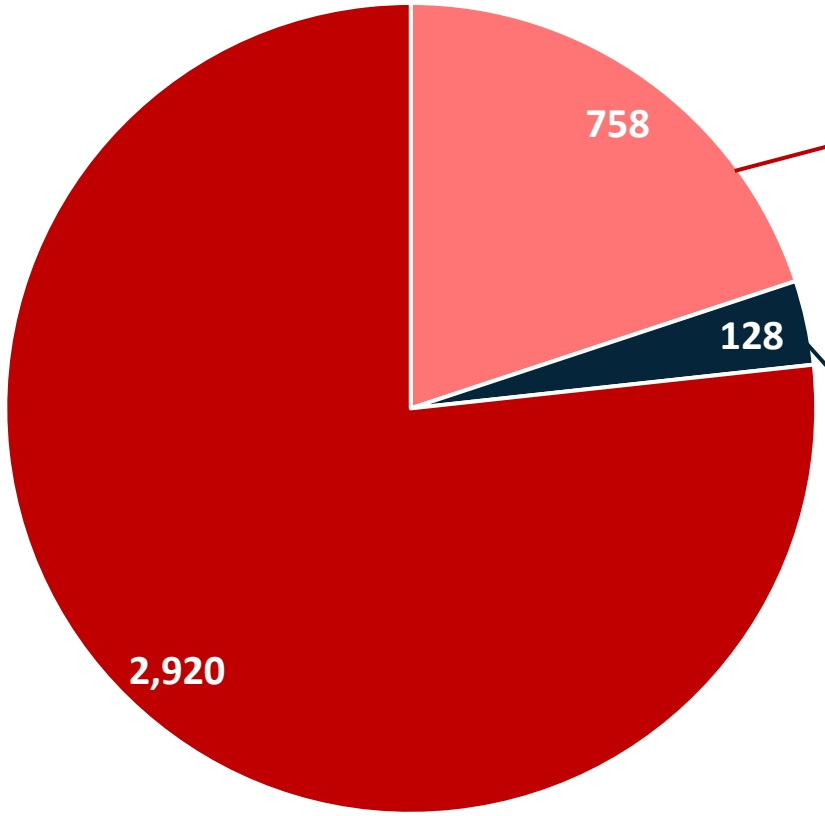
All services are highly prone to Implementation vulnerabilities due to DICOM's complexity

Association Control Service Element (ACSE)

DICOM Message Service Element (DIMSE)

Less than 1% of DICOM servers on the internet use effective authorization

Most of DICOM products do not support association- level authorization



Weak authorization Strong authorization No authorization

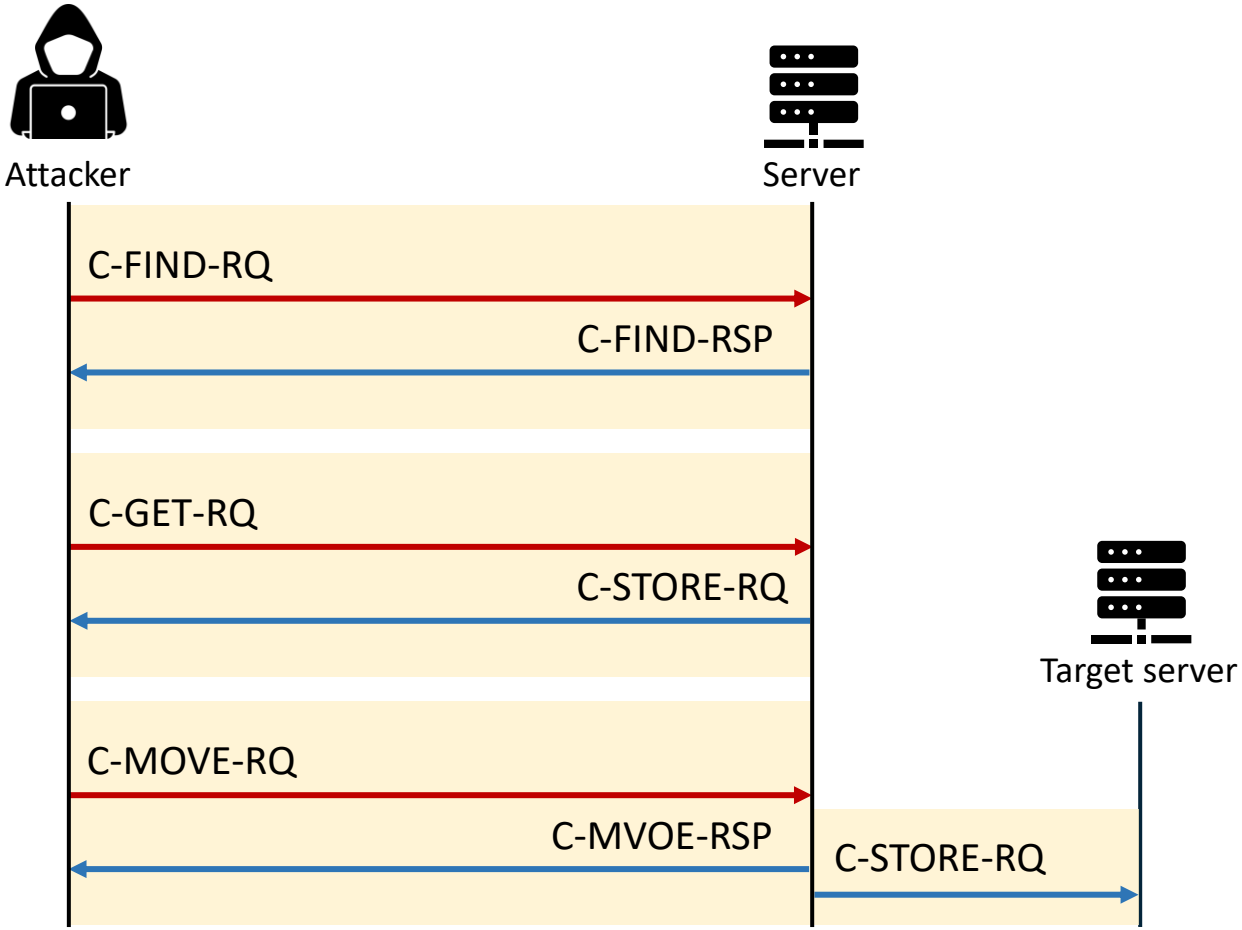
- Only AET authorization
- These servers use the product default AET or a common one
- Vendors publish default AETs in the DICOM conformance statement, section 4.4.1.1

Example of section 4.4.1.1

Application Entity	Default AE Title
Storage SCU	ADR_STORAGE_SCU
MWM SCU	ADR_MWM_SCU
MPPS SCU	ADR_MPPS_SCU
Print SCU	ADR_PRINT_SCU

- Unguessable AET and/or IP-based authorization

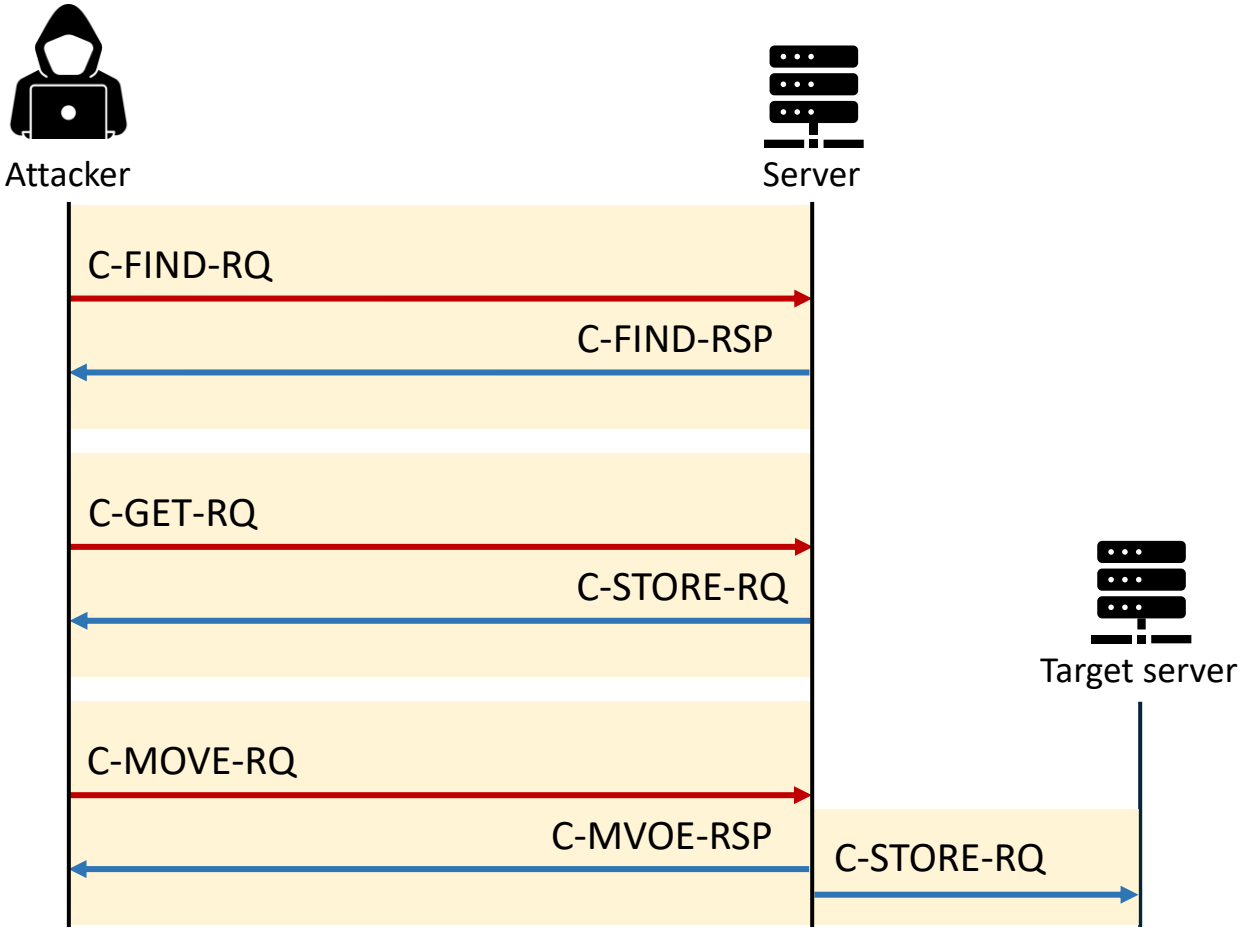
Attackers can use C-FIND, C-GET, and C-MOVE to access patients' data



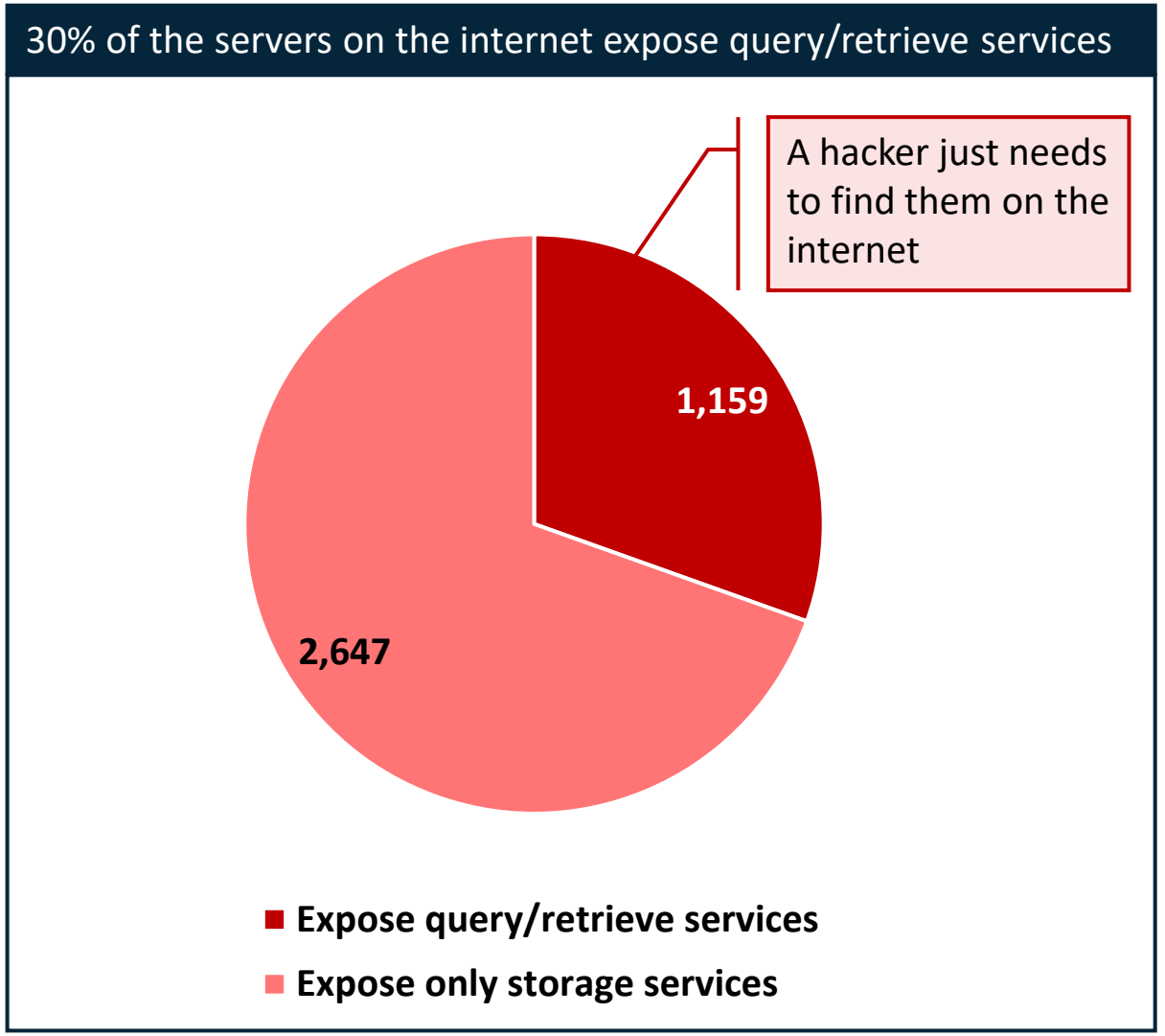
Many online resources* provide detailed explanation of these services

*Roni Zaharia – https://dicomiseasy.blogspot.com/2012/01/dicom-queryretrieve-part-i.html

Attackers can use C-FIND, C-GET, and C-MOVE to access patients' data

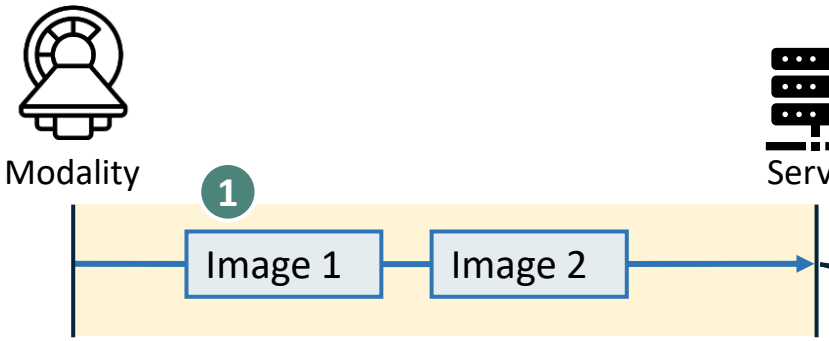


Many online resources* provide detailed explanation of these services



*Roni Zaharia – https://dicomiseasy.blogspot.com/2012/01/dicom-queryretrieve-part-i.html

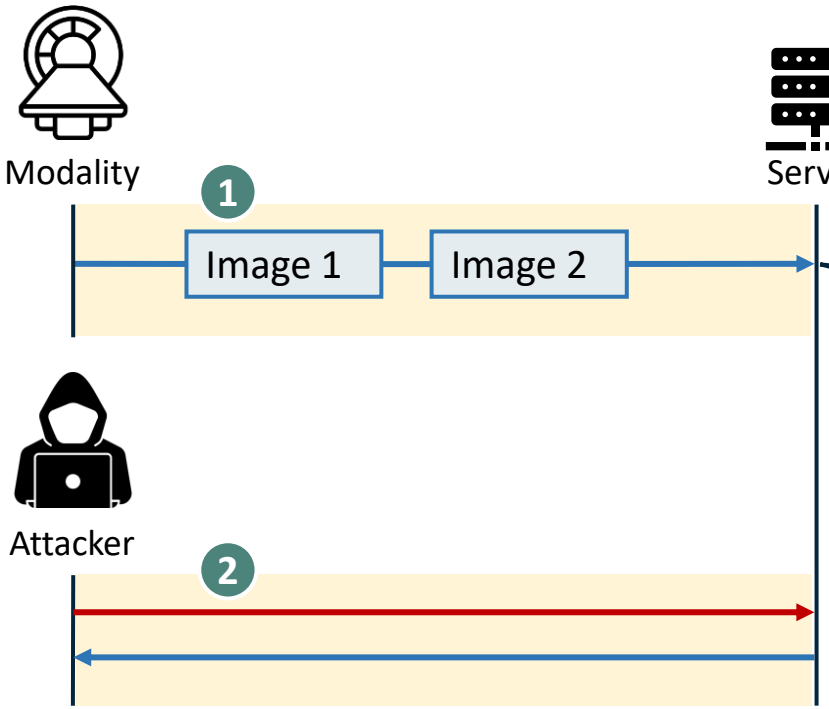
Attackers can tamper existing series using C-STORE



patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2….	1.3.12.2….	1.3.12.2….	1
P1234	1.3.12.2….	1.3.12.2….	1.3.12.2….	2

1 Modality transfers the images to the SOP

Attackers can tamper existing series using C-STORE



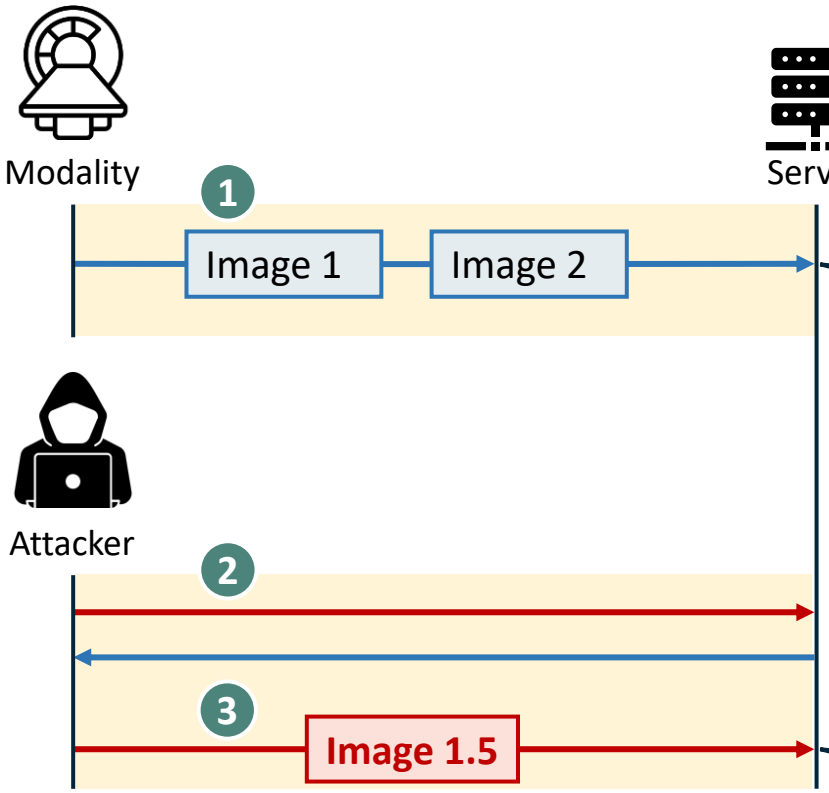
patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	1
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	2

1 Modality transfers the images to the SOP

Attack

2 Retrieve the existing series

Attackers can tamper existing series using C-STORE



patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	1
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	2

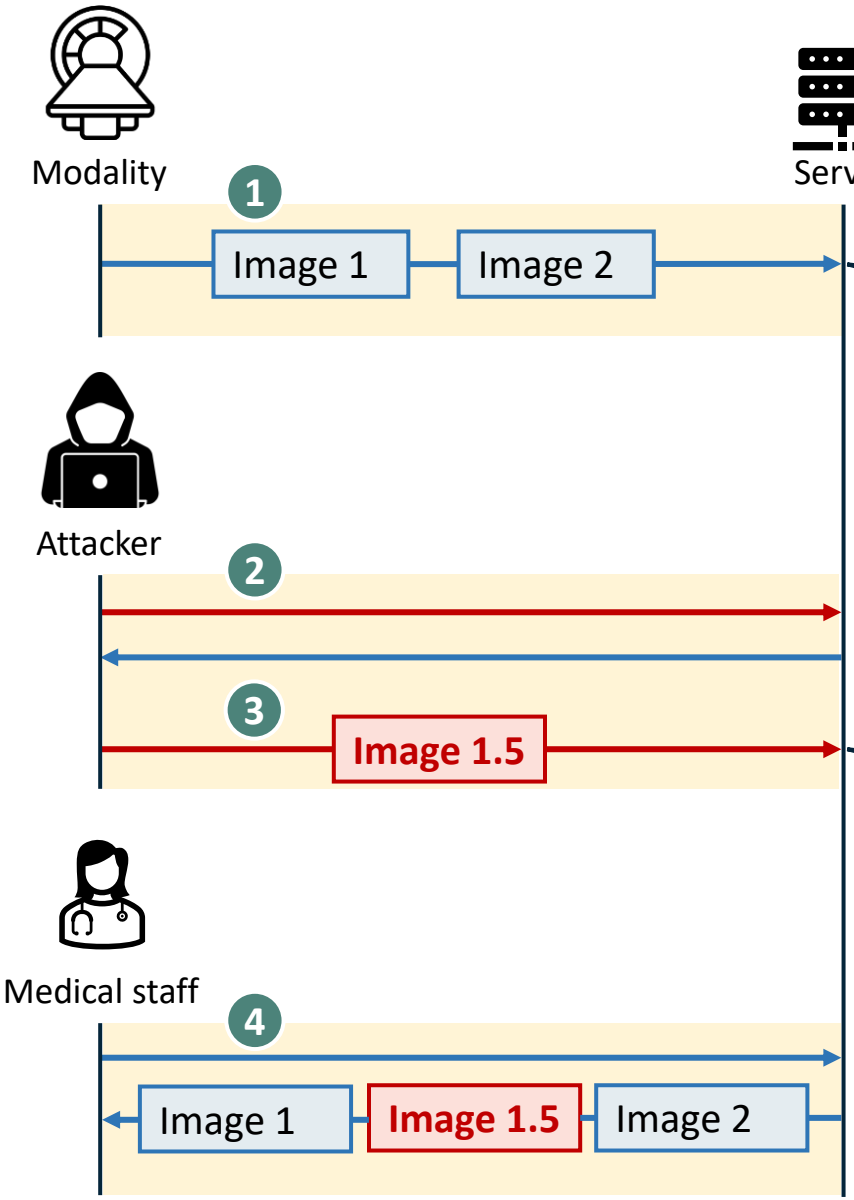
patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	1
P1234	**1.3.12.2....**	**1.3.12.2....**	**1.3.12.2....**	**1.5**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	2

1. Modality transfers the images to the SOP

Attack

2. Retrieve the existing series
3. Craft new images using retrieved study and series information, and transmit the crafted images using C-STORE

Attackers can tamper existing series using C-STORE



-Demo-

patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	1
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	2

1 Modality transfers the images to the SOP

Attack

2 Retrieve the existing series

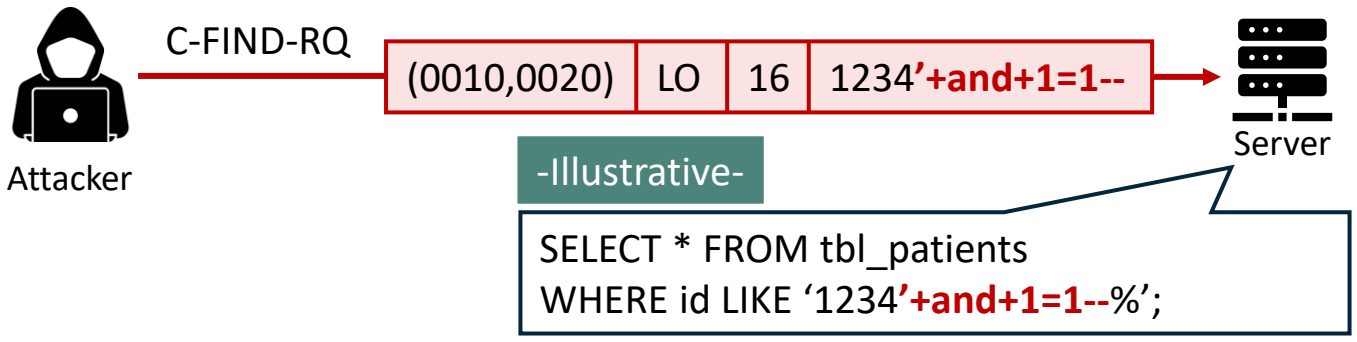
3 Craft new images using retrieved study and series information, and transmit the crafted images using C-STORE

patientID	studyUID	seriesUID	instanceUID	**number**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	1
P1234	**1.3.12.2....**	**1.3.12.2....**	**1.3.12.2....**	**1.5**
P1234	1.3.12.2....	1.3.12.2....	1.3.12.2....	2

4 Legit SCUs will receive the altered series

Attackers can exploit this issue to destroy a series, or introduce false signs of illness

Database injection is one of the most common DICOM's implementation vulnerabilities



SQL Injection vulnerability in *PatientID* exploited by C-FIND

```
sina@sina-ThinkPad:~$ python3 -m pynetdicom findscu [redacted] 104 -k QueryRetrieveLevel=PATIENT -k PatientID=0\'\ union\ select\ 1,NULL
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,concat_ws\(\'\|\',username,password\),NULL\ from\ users\ limit\ 1-- 2>&1 >/dev/null
I: Requesting Association
I: Association Accepted
I: Sending Find Request: MsgID 1
I:
I: # Request Identifier
I: (0008,0052) CS [PATIENT]                                # 1 QueryRetrieveLevel
I: (0010,0020) LO [0' union select 1,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,concat_ws('|',username,password),NULL from user
s limit 1--] # 1 PatientID
I:
I: Find SCP Response: 1 - 0xFF00 (Pending)
I:
I: # Response Identifier
I: (0000,0000) UL [0]                                      # 1 CommandGroupLength
I: (0008,0052) CS (no value available)                     # 0 QueryRetrieveLevel
I: (0008,0080) LO [ARO[redacted]|$2a$08$f47sak0I8u[redacted]] # 1 InstitutionName
I: (0010,0010) PN (no value available)                     # 0 PatientName
```

Agenda

1| Introduction and results of the internet-wide research

2| DICOM: Deep dive and attack scenarios

3| Countermeasures and takeaways

Standard organization – effective governance is essential to address these issues at their core

1. Separate versions

- Enable authorization by default in the new version
- Release the new version with mandatory implementation of access control

2. Enforcement

- Establish a deprecation date (e.g., 2026) to give vendors sufficient time for adopting the change
- Cease certification of products with the old version after the deadline

3. Audit

- Communicate this change with other relevant organization, such as ISO
- Ensure that checking DICOM security measures is incorporated into their audit checklist

Medical institution – DICOM must not be publicly accessible on the internet

Priority 1
Exposure

- Prevent public internet access
- Secure the connection between internal network and remotely hosted DICOM server using a secure channel (e.g., IPSec)
- Regularly scan TCP port 104, 11112, and 4242 for exposed assets to detect potential DICOM exposures

Medical institution – DICOM must not be publicly accessible on the internet

Priority 1

Exposure

- Prevent public internet access
- Secure the connection between internal network and remotely hosted DICOM server using a secure channel (e.g., IPSec)
- Regularly scan TCP port 104, 11112, and 4242 for exposed assets to detect potential DICOM exposures

Priority 2

Segmentation

- Create a dedicated DICOM segment, isolated from other segments
- Restrict access to this segment via DICOM protocol to only modalities
- Restrict user access to this segment exclusively through DICOMweb*
- Deploy a WAF for TLS and protect DICOMweb from attacks like database injection

* Use a DICOMweb proxy if the DICOM server does not support it

Medical institution – DICOM must not be publicly accessible on the internet

Priority 1 Exposure	• Prevent public internet access • Secure the connection between internal network and remotely hosted DICOM server using a secure channel (e.g., IPSec) • Regularly scan TCP port 104, 11112, and 4242 for exposed assets to detect potential DICOM exposures
Priority 2 Segmentation	• Create a dedicated DICOM segment, isolated from other segments • Restrict access to this segment via DICOM protocol to only modalities • Restrict user access to this segment exclusively through DICOMweb* • Deploy a WAF for TLS and protect DICOMweb from attacks like database injection
Priority 3 Access control	• Authorize only modalities' IP addresses • If applicable, implement AET authorization with random AETs • Integrate DICOMweb with IAM

* Use a DICOMweb proxy if the DICOM server does not support it

Medical institution – DICOM must not be publicly accessible on the internet

Priority 1 Exposure	• Prevent public internet access • Secure the connection between internal network and remotely hosted DICOM server using a secure channel (e.g., IPSec) • Regularly scan TCP port 104, 11112, and 4242 for exposed assets to detect potential DICOM exposures
Priority 2 Segmentation	• Create a dedicated DICOM segment, isolated from other segments • Restrict access to this segment via DICOM protocol to only modalities • Restrict user access to this segment exclusively through DICOMweb* • Deploy a WAF for TLS and protect DICOMweb from attacks like database injection
Priority 3 Access control	• Authorize only modalities' IP addresses • If applicable, implement AET authorization with random AETs • Integrate DICOMweb with IAM

Remote user access	• Do not enable remote user access if DICOMweb is not integrated with IAM
	• Permit remote access through a firewall:
	  • Implement rate limiting
	  • Apply regional source IP whitelisting

* Use a DICOMweb proxy if the DICOM server does not support it

Vendors and country CERTs – implement security measures, and monitor the exposure

Vendor

- Implement AET authorization and *extended negotiation of user identity*
- Disallow new images for an existing series after a set time, e.g., 1 hour from the last submission.
- Perform regular security tests, and mitigate the uncovered vulnerabilities:
  - Perform fuzzing test. It effectively detects insecure input handlers in a complex DICOM system
  - Conduct penetration test and code review for more in-depth security.

Country CERTs

- Scan the country's IP ranges regularly to identify DICOM servers
- Identify the IP's owner, and help them harden their DICOM setup

Takeaways

1	Continued use of legacy protocols, like DICOM, poses ongoing and significant security risks
2	Millions of patients' records face internet exposure and unauthorized tampering
3	Effective governance is essential to address these issues at their core

Questions?

Thank you!

Aplite GmbH | Tailor-made IT Security
Web: www.aplite.de
Email: hi@aplite.de