HL7 2.x Security

Hacking medical devices

Anirudh Duggal

Disclaimer:
All the views/ research done and presented is of my own and does not reflect my employer.
Do not try this on a live environment. This can harm someone.

#whoAmI

- Graduate Student at Northeastern University, Boston
- Code occasionally
- Follow null and CysInfo
- Speak at conferences
- Worked with Philips Healthcare

@secure_hospital, @duggal_Anirudh

Agenda

Security inside hospitals

Why HL7 2.x

Crash course in the protocol

Understanding message

Identifying ports

Changing information

Attacking devices

Fuzzing

Server attacks on HL7 2.x

Defending HL7 and hospitals

FHIR and changing threats

Securing hospitals

- Devices
  - Patient monitors, X-Ray, Ultrasound, MRI
- Networks
  - Administration network, Patient and guest network
- Protocols
  - DICOM, HL7 2.x, 3.x, FHIR, HTTP, FTP
- Patient Records
  - EHR / EMR – Electronic health records / Electronic medical records

HL7 = Health Level 7

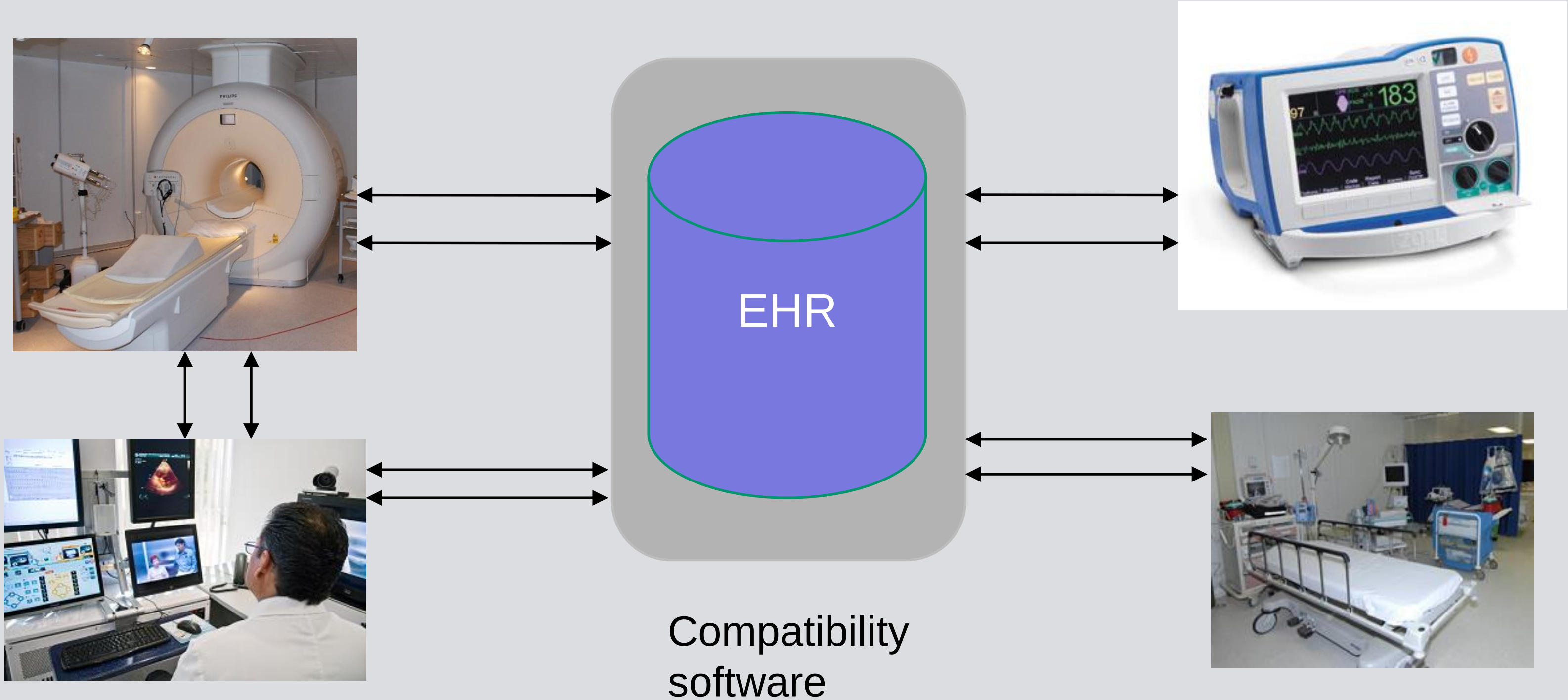
“HL7’s Version 2.x (V2) messaging standard is the workhorse of electronic data exchange in the clinical domain and arguably the most widely implemented standard for healthcare in the world. This messaging standard allows the exchange of clinical data between systems. It is designed to support a central patient care system as well as a more distributed environment where data resides in departmental systems.”

--Source: http://www.hl7.org/

In a nutshell

HL7 2.x is everywhere

Used by medical devices to support achieving interoperability

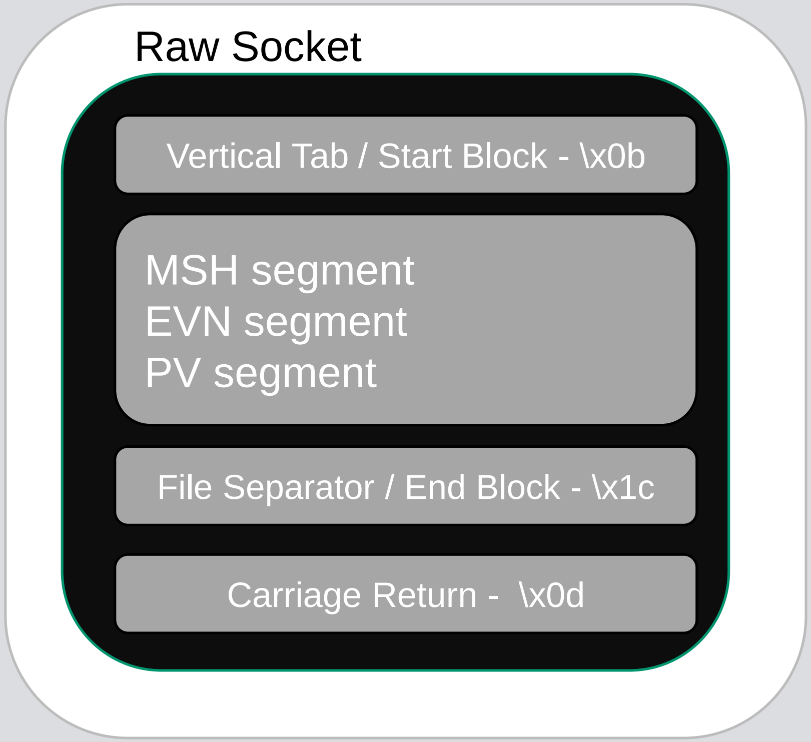


EHR

Compatibility software

HL 7 2.x crash course

A Raw HL7 2.x (MLLP) message


Raw Socket

Vertical Tab / Start Block - \x0b

MSH segment
EVN segment
PV segment

File Separator / End Block - \x1c

Carriage Return - \x0d

HL 7 2.x crash course

| is the most common delimiter / field

^ means space

MSH – message header segment

Types of message we will be covering

- ADT – Admit Discharge and Transfer
- ORM – Order message
- ORU – Observation result
- RDE – Pharmacy order message

Uses MLLP Protocol (Minimum Lower Layer Protocol) for sending messages

ADT - Admit Discharge and Transfer

```
MSH|^~\&|SendingApplication|SendingFacility|RecievingApplication|RecievingFacility|20060529090131-
0500||ADT^A01^ADT_A01|01052901|P|2.5

EVN|||||200605290900
200605290901
PID|||56782445^^^UAReg^PI||Bob^Jerry^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN
CREST DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL’S PICKLES^10000 W 100TH
AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN

PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^M
D^0010^UAMC^L|MED|||||A0||13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||20060529090
0

OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A
```

ADT - Admit Discharge and Transfer

Responsible for admit, discharge and transfer

Contains:

- Patient information (PII) – name, age, address, height, weight, allergy
- Doctor information – attending doctor, referred doctor
- Patient visit details
- Allergy and diagnostics

ADT - Potential Entry Points

Depends on the connected infrastructure

Look at JavaScript and injection attacks

Buffer overflows

EMR systems will be prime target

ORM – Order message

```
MSH|^~\&|SendingApplication|Hospital facility |RecievingApplication|Recieving Facility
|20101111111214456+0700|SECURITY|ORM^O01^ORM_O01|MSG005010|P|2.6
PID||8838|4567830^345|AAAAA|Anirud^Duggal||20011010000000|M|Test||Street&comp1&comp2^AddLine2^Seattle^WA^
98052^USA^H|USA|^^^^123^456^1111^7890|^^^^098^765^1111^4321|ENG^English|M||11111111111|111222333-SSN
number|33333333333|||Washington|Y|2|||^am|20101111111214|Y|||||L-80700^Canine|L-80900^Weimaraner|666
PV1|1|I|4E^234^A^Good Health
Hospital^^GT^^^Crowded|R|1234^4567||123^S^Sasikala^A^JR^DR^MD^|456^A^Deepshikha^S^JR^DR^MD^|789^H^Praj
akta^A^JR^DR^MD^||||R|4|||101^M^Toshan^G^JR^DR^MD^||12345777^456|||||||||||||||||10||SZ^2^Diet||||||201011111111214445
6+0700|20101111111214456+0700
PV2|||High Fever|||||||||||||P||||||||DI|1|
ORC|NW|X1234^HIS||||||||||ORC_12^test3^Practitioner3^A^^Dr||||||||||||Street&comp1&comp2^AddLine2^Seattle^WA^9805
2^USA^H
OBR|1|X1234^HIS|R578^RIS|56782^X-Ray
Chest||20101111111214456+0700|20101111111214456+0700||||||testOBR_13|||OBR_16^Check1||||||20101111111214456+
0700||AU|F
OBX|1|CWE|45^Systolic blood
pressure^LN||10.532467105262732|kPa|||||S|||20150204025500.000+0000|a0g11000001QPcdAAG||^Manual entry by
clinician
```

ORM – Order message

Used to place orders for tests – x-ray, ultrasound, MRI and others

Contains

- Patient information like ADT
- Will have order details – test to be conducted, facility location etc.

Can be used to fingerprint more devices

ORM - Potential Entry points

Changing PII

Changing initial diagnostics

Changing observations

ORU – Observation Result

```
MSH|^~\&|SendingApplication|SendingFacility|||20140715112021||ORU^R01|D0715112021550d6fff|P|2.4
PID|||P1001010101||Duggal^Anirudh||19660909|Male|||||(347)651-3404
PV1||I|CSI^15^15-A^MOSES
OBR|1|||86290005^Respiration Rate^SNM|||20140715105500||||||18 RPM RESP rgb(255,255,255) 1 STATUS
20140715145200 Resp Rate 18 RPM 15 Jul 2014 10:52 CALC
MONITOR|20140715145200|||||||||||F|||||||||||||||^^^rgb(255,255,255)||Resp Rate 18 RPM 15 Jul 2014 10:52
OBX|1|NM|86290005^Respiration Rate^SNM||18|258984001^RPM^SNM^/min^Respirations per
minute^ISO+||N|||F|||20140715105500||^Services^D
OBX|2|ST|278195005^BodySystem^SNM||RESP|||N|||F|||20140715105500||^Services^D
OBX|3|NM|224098002^DisplayOrderRow^SNM||1|||N|||F|||20140715105500||^Services^D
OBX|4|ST|39801007^GridComponent^SNM||STATUS|||N|||F|||20140715105500||^Services^D
OBX|5|ST|118170007^Source^SNM||MONITOR|||N|||F|||20140715105500||^Services^D
OBX|6|ST|226035000^DisplayLabel^SNM||Resp Rate|||N|||F|||20140715105500||^Services^D
```

ORU – Observation Result

- Most important message in a live environment
- Contains patient observation
  - Heart rate
  - Oxygen levels
  - Any other real-time / offline observation result
- Can be used to harm someone
  - Changing diagnostics
  - Blocking diagnostics

Potential entry points

The observation (OBX) segment

Specially reflected file downloads via the path

RDE – Pharmacy order message

```
MSH|^~\&|CPSI_FEED_OUT|Murphy MedicalCenter|||20150624155739765+0700||RDE^O11^RDE_O11|20150624155739-4|P|2.6||
PID||60595|60595^345|AAAAA|Test_EMR_A_ORUR01&PID_5_1_2^Test_VHR_A_Patient^A||20011010000000|M|TestPatientAliasPID_9_1||Street&comp1&comp2
^AddLine2^Seattle^WA^98052^USA|USA|||ENG^English|M^married||17121985666|111222333|33333333333|||Washington|Y|1|||^am|20150617123839|Y|||||PID_35_
1^PID_35_2|PID_36_1^PID_36_2|666
PV1|1|I|003^UCC12^Ashish|A|1234^4567|005600^HEAVNER^TERESA^MD|PV1_7_1^PV1_7_2^PV1_7_3^^^Mr|PV1_8_1^PV1_8_2^PV1_8_3^^^Miss|PV1_9_1^P
V1_9_2^PV1_9_3^^^Mrs||||R|4|||PV1_17_1^PV1_17_2^PV1_17_3||12345777^456|||||||||||||||||10||||||||20101111111214456+0700|20101112111214456+0700
ORC|FU||||HD|R||||||OP_1^OP_2^OP_3^^^Mr|
TQ1|6540|^21&&ANS+&&&MEDR|9&&CLP&&&SNM^DW^^^^^N^ACM~14&&POS&&&AS4^DW^^^^^N^ACD~8&&GMDC2006&&&I10G2004^DW^^^^^N^HS|19375
8|^12&&SNT&&&OHA|^7&&IBTnnnn&&&CD2|19891015213815|19831022072815|||Take 2 daily, supplemented with vitamin B|S|^14&&W4&&&UCUM
RXE|&10FDDXC5^^^19851019113122^19911030213625^P^^^S^S&w&CANSK&n&USHCFA&&&Z&GUID&I&HCD^12&&O301&&&GDRG2005|23^^GDRG2005^^^
CST|4413168.164632165423|561685.023164564|16^^C5^^^IBTnnnn|4^^ICD10AM^^^GMDC2008|7^^POS^^^O3012006~12^^CLP^^^ICSD|Therapy^6789^^^cleane
d^N^wing 9^11^16th St&&Wellington&Borneo&35401&16&BI|1|23165749|17^^O3012005^^^I9|235|54^HOFFMAN^ELIZA
^^I^DR^CMA^ST23^^M^2^M11^DDS^^I^9&&HI&&&SCT2^19971030014823&19841016201025^G^19831010032141^19981029135513^^5&&MDDX&&&CD2^11&&I
BT&&&I10G2005~5^COWEN^ADONIA
^^Jr^Ms^DIP^ST23^^R^3^BCV^RRI^^I^5&&NPI&&&NPI^19871014204810&19971026182037^G^19971012134729^19841010082648^^5&&GMDC2005&&&UMD^1
2&&ICD10GM2008&&&LN~8^KARCHER^SHAMIRA
^^II^Mr^BA^ST23^^N^3^M10^BC^^I^5&&POS&&&ICSD^19891011171831&19841024021823^G^19861013155710^19901010182223^^22&&SDM&&&E5^17&&UB0
4FL14&&&GDRG2008|1^INKS^VEVAY
^^III^Dr^AAS^ST23^^U^1^BCV^PCN^^I^23&&JC8&&&GMDC2004^19851024001518&19811010201949^G^19911110031553^20021028061452^^4&&I9&&&I9C^4&
&SDM&&&OPS2007~5^WILLIOUGHBY^ADRIANO
^^III^Prof^DO^ST23^^I^6^ISO^WC^^I^23&&CD2&&&HHC^19911010174034&19841120061945^G^19901023101610^19931026085639^^4&&ART&&&ISOnnnn^15
&&O301&&&NDC~58^SILVERTHORN^DILLON
^^Sr^Eng^CNS^ST23^^L^5^M11^EI^^I^7&&ALPHAID2008&&&ICDO^20001123084231&19971029212123^G^20021023211742^19951024115535^^4&&I9CP&&&H
OT^15&&MEDR&&&ACR|4649820|164|6|19931011105336|^10&&FDDX|N|||6843.4|18^^ISOnnnn^^^GMDC2008|21311654.35464613162|16^^C5^^^I9|2^^E6^^^CE
~7^^CD2^^^E7~4^^HI^^^JC10|4642311657498.431564|9^^O3012006^^^OHA|TR|4^^USPS^^^E7|20150624155739765+0700||1^^ITIS^^^HI|V^^ART^^^HPC|Y|23^^
UB04FL15^^^O3012004~7^^IUPC^^^OHA|14^^NIC^^^NIC||2^^WC^^^JJ1017|^^Italy^Borneo^35218^MMR^F^^^^I^19841010203610&19951020185444^198110121
54310^19871017153018^R&&NDA&&&OHA^N^N^M^^^^UL&&JC8&&&UMD^12&AUSHIC|Nursing unit^6540^^^cleared^H^St
Mark^10^^21&CANNS|^^Vienna^Sumatra^35218^MRT^BDL^^^^A^19861012133827&19871026095542^19921021221933^20011110191829^E&&ISO+&&&HL7nnn
n^N^N^M^^^^LI&&JC10&&&ICD10CA^19&CANNB|M
TQ1|6540|
PO|||20150723010100|||||||||||43^00483200^admin|1^20150723^12224^53|||||PHR|F
OBR||297973851-43||^^^24300^ROFLUMILAST 500 MCG TAB
RXA|||20150723010100||66612^ROFLUMILAST 500 MCG TAB PO|500.000|MCG^MICROGRAM||500.000
RXR|PO^Orally
OBX||FT|ROFLUMILAST 500 MCG TAB PO||500.000|MICROGRAM||||||||20150723010100
```

RDE – Pharmacy order message

Used for providing medicines

Contains patient information (PII)

Details of the medicine to be given / dispensed

- Pharmacy information
- Medicine and dosage

Can be used to gain access to unauthorized drugs

Can also be used to attack medicine dispensing machines

RDE - Potential entry points

Patient (PII) information

The Pharmacy/Treatment Encoded Segment (RXE)

The Pharmacy Route Segment (RXR)

The Observation Segment (OBX)

MDM - Medical Document Management

" The main purpose of the medical record is to produce an accurate, legal, and legible document that serves as a comprehensive account of healthcare services provided to a patient.“

```
MSH|^~\&|Something|Hospital^Name^here|||20160510071633||MDM^T02|12345|D|2.3

PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||20289^^HL70005^RA99113^^XYZ|260 GOODWIN CRESTDRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL’S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^ANPV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900TXA||CN||20160510071633|1173^MATTHEWS^JAMES^A^^^|||||||^^12345|||||PA|

OBX|1|TX|||Clinical summary here

OBX|2|TX|||Diagnosis here

OBX|3|TX|||Diagnosis here

OBX|4|TX|||Prescription here
```

DFT - Detail Financial Transaction

Easiest to attack

Usually created while clearing patient dues

```
MSH|^~\&|^2.16.840.1.113883.3.4337.1486.####^HL7||^OtherSoftware.OIDroot^||20141122180827||ADT^A08^ADT_A01|363d05d13b834613b5934bd005497
        581|P|2.6||||AL

EVN||20141122180827||01

PID|1|98765|12345^5^M11^&2.16.840.1.113883.3.4337.1486.####.2&HL7^PI~98765^4^M11^&OtherSoftware.PatientOID&^PI|12345|Smith^John^L||1994120
        4|M||2106-3^White^CDCREC^^^^1~2186-5^NotHispanic^CDCREC^^^^1|421 N Main St^Apt 7^Salem^OR^97302^^^^^^^^^^^^^^^Emergency Contact:
        Jane Smith\.br\Relationship: Wife\.br\Phone: (503)555-
        1234||^PRN^PH^^^503^5551234~^PRN^CP^^^503^5556789~^PRN^Internet^john@somewhere.com|^WPN^PH^^^503^3635432||M|||123456789

PV1|1|O|Clinic 1^^^&Dental
        Practice^^C||||2.16.840.1.113883.3.4337.1486.####.3.123^Abbott^Sarah^L^DDS^DrAbbott~OtherSoftware.ProviderOID.987^Abbott^Sarah^L^DDS^DrA
        bbott||||Oregon State University^^^^^^S|||||||1IN1|1|2.16.840.1.113883.3.4337.1486.####.7.14|CDOR1|ODS (Oregon Dental Service)|601 SW 2nd
        Ave^^Portland^OR^97204||^WPN^PH^^^888^2172365|7567-15|ODSoftware||Open Dental Software, Inc.|20140101|20141231||Category
        Percentage|Smith^John^L|SEL^Self|19941204|421 N Main St^Apt 7^Salem^OR^97302|Y|CO|1|||||Y||||||||123456789||||||

|||||D||123456789IN1|2|2.16.840.1.113883.3.4337.1486.####.7.15|CB850|Blue Cross of Oregon – Regence

|PO Box 30805^^Salt Lake City^UT^84130||^WPN^PH^^^800^4527390|811657167|OrStHosp||Oregon State Hospital||||PPO
        Percentage|Smith^Jane^W|SPO^Spouse|19941221|421 N Main St^Apt 7^Salem^OR^97302|Y|CO|2|||||Y||||||||987654321||||||||||D||987654321
```

Viewing these messages

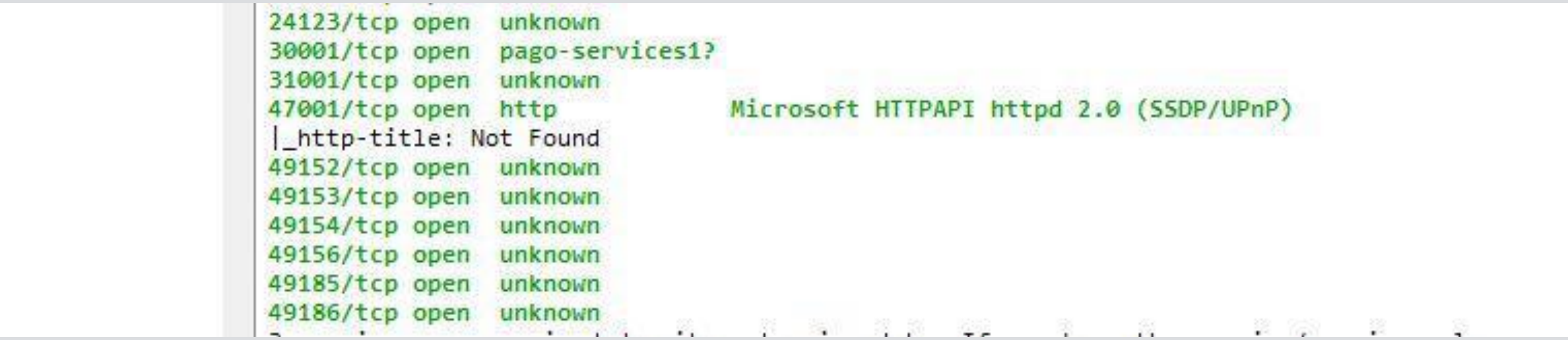
Tools

- Capture using wireshark
- Gain access to hl7 files / dumps
- Smarthl7 viewer – free , effective
- HAPI test panel for sending messages
- Demo!

Pen testing HL7 2.x messages

Recon

A simple portscan will give results



```
24123/tcp open  unknown
30001/tcp open  pago-services1?
31001/tcp open  unknown
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49185/tcp open  unknown
49186/tcp open  unknown
```

Recon

Try sending the appropriate message

- ADT for a registration desk
- RDE for a medicine dispensing machine
- And so on

Neat hack

- Try sending MSH

Demo!

Common flaws – HL7 2.x

Man in the middle attacks

Lack of encryption between devices is a common

Happens due to:

- Insecure configuration
- Lack of support
- Cost

Message source not validated

The machines do not establish a two way trust

Think of it like a broadcast over a port

Can lead to rogue messages

Unvalidated size

The size of messages is often not defined

Messages can be sent in parts

Can lead to buffer overflow

Or lead to DOS attacks

Abusing file upload / download functionality

Found with bigger, connected infrastructure

Can change the download location for the report

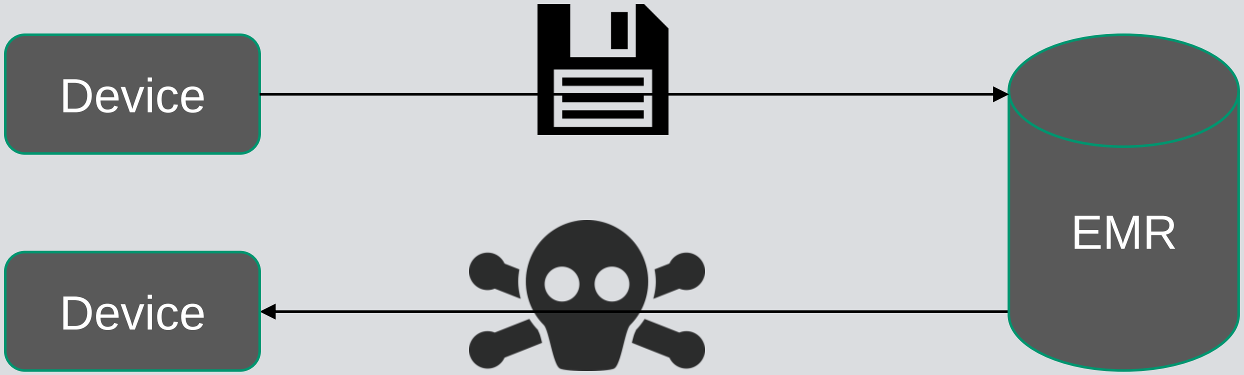
Also gain access to other system like DICOM / PACS

Demo!

Bad server attacks

The ACK message is responsible for completing the communication

A rogue server can disrupt all functionality



ACK and NACK messages

ACK indicates message has been received

NACK is an indication to send the message again

An ACK message:

```
Received 07/18/16 11:15:16
MSH|^~\&|Responder|HL7Emulator|||||ACK|0000-1|P|
MSA|AA|
```

Potential entry points

Changing the ACK sequence

ACK tool name / origin header, can be changed to

```
MSH|^~\&|VHIS|VHIS|CPSI_FEED_OUT|AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA|20160329164216||ACK^|ACKA34R
VHA7NYCB|D|2.3.1|||||
MSA|AA|20150624155739-4
```

Denial of service

The device will wait for ACK message to complete the transaction

Message will be sent again

Potential DOS if no ACK is present or a change in sequence

ACK:

```
Received 03/29/16 16:42:17
Received 03/29/16 16:42:18
Received 03/29/16 16:42:19
Received 03/29/16 16:42:120
```

Fuzzing HL7 2.x

One payload does not fit all

Fuzzing scenario will change with vendor, device, message version and fields to be fuzzed

Example scenario

Defending HL7 2.x messages

Validate message size

Enforce two way TLS connections

Unvalidated file downloads

Input sanitization

Fault tolerance – automatic purging

Anonymize HL7 messages

Add checksum – use ST segment

Beyond medical devices

Secure network – Firewall with both ingress and egress filtering

Understand network and devices

More work to come soon! Follow hospital security project!

Changing threat scenario - FHIR

Fast Healthcare Interoperability Resources (FHIR, pronounced "fire") is a draft standard describing data formats and elements (known as "resources") and an Application Programming Interface (API) for exchanging Electronic health records.

-- wiki

FHIR ≠ HL7 3.0

FHIR (cont)

```
POST http://192.168.1.6:8080/users/?applicationName=DemoApplication  HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;)
Pragma: no-cache
Cache-control: no-cache
Content-Length: 0
Host: 192.168.1.6:8080
{
"emailId": "anriudhduggal@gmail.com",
"password": "MySuperSecretPassword",
"profile": {
"givenName":"Anirudh",
"middleName":"",
"familyName":"Duggal",
"birthday":"2014-08-22",
"receiveMarketingEmail":"Yes",
"currentLocation":"india",
"displayName":"anirudh",
"locale":"en-US",
"gender":"male",
"timeZone": "10:50 GMT",
"preferredLanguage":"EN",
"height": 167,
"weight": 42,
"primaryAddress":{
"country":"india"
},
"photos": []
}
}
```

Changing threat scenario

FHIR will replace HL7

FHIR – light weight, HTTP based API

Developers are using FHIR + HL7 2.x

Questions ?

@Duggal_Anirudh

anirudhduggal@gmail.com

Google Mailing list: hospitalsecurityproject

https://github.com/anirudhduggal

Thank you!

Philips Security Centre of Excellence

Friends and family

Nullcon!