HL7Magic: Medical Data Hacking Made Easy

Katie Inns @J3lly____



WITH secure

Hello!

Katie Inns

Security Consultant @ WithSecure
Attack Surface Management

@J3lly____



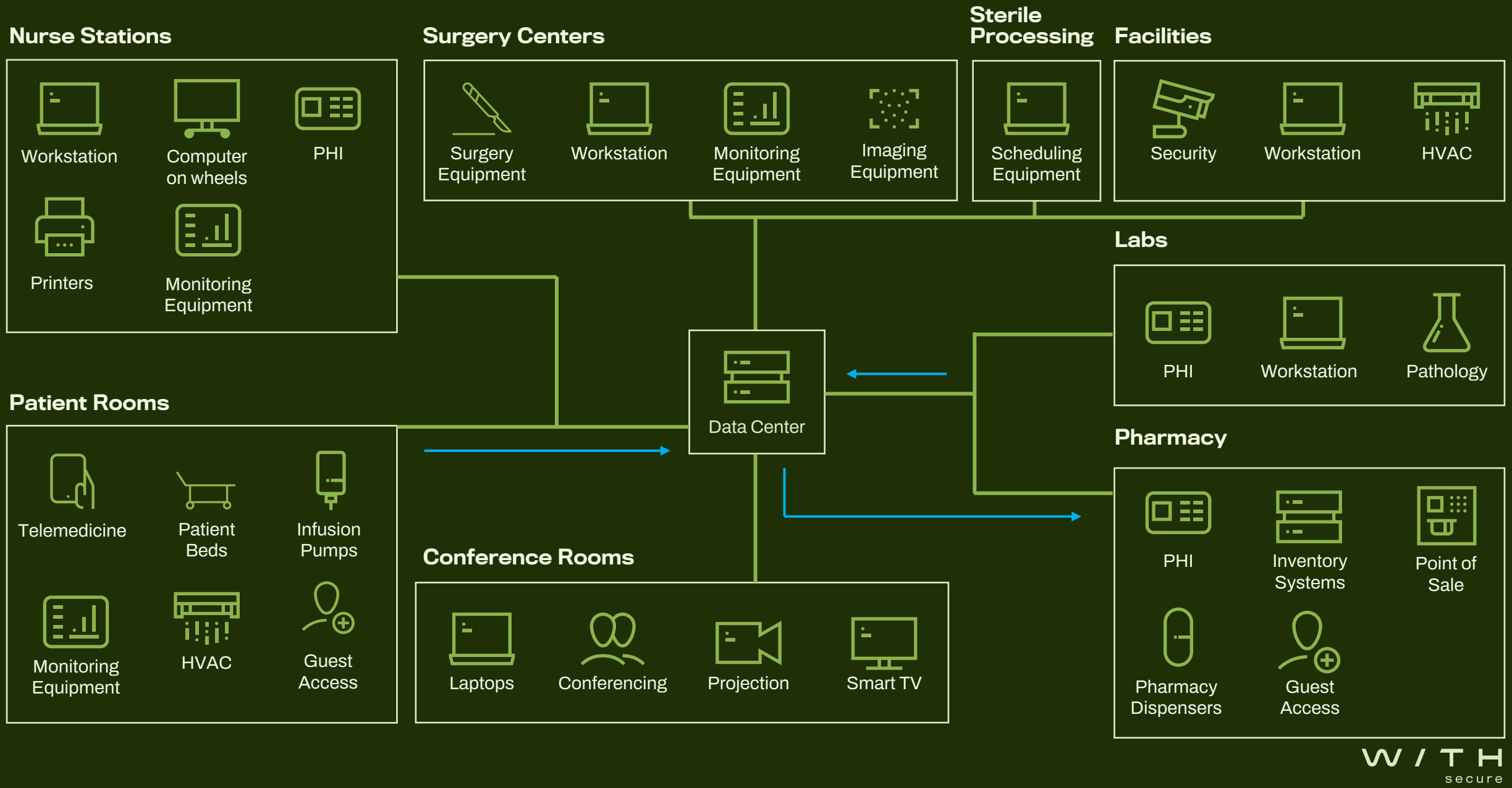




Tech in Healthcare



Tech in Healthcare



WITH secure

HL7	Health Level Seven
DIAP	Datascope Improved ASCII Protocol
DICOM	Digital Imaging and Communications in Medicine
LIS01/2	Lab Instruments and Computer Systems
FHIR	Fast Healthcare Interoperability Resources

HL7

Version 1	Released in 1979, considered obsolete
Version 2	Designed in 1989 (non-XML based), most common in healthcare
Version 3	implemented in 2005 (XML-based), less widely adopted, not backward compatible
Common transport methods	Lower Layer Protocol (LLP), Minimal Lower Layer Protocol (MLLP), Hybrid Lower Layer Protocol (HLLP), FTP, SOAP, SMTP
	Messages transmitted in plain text

HL7

Admissions, Discharges and Transfers:
ADT-A01 – standard admission
ADT-A02 – transfer
ADT-A08 – patient update

Message Header

```
MSH|^~\&|SENDING_APPLICATION|SENDING FACILITY|RECEIVING APPLICATION|RECEIVING_FACILITY|20170613083617||ADT^A01|911576
160110613083617|P|2.3||||
EVN|A01|20170613083617|||
PID|1||135769||MOUSE^MICKEY^||19281118|M|||123 Main St.^^Lake Buena Vista^FL^ 32830||(407)939-
5555^^^ohtoodles@notdisney.com|||||1719|999999999|||  |MOUSETOWN||||||||||||||||
NK1|1|MOUSE^MINNIE|WIFE||||||NK
AL1|1||^Penicillin||Anaphylactic shock
AL1|2||^Cat dander|Skin rash
```

Event Segment

Allergy

Patient Identifier

Next of Kin

WITH secure

Minimal Lower Layer Protocol (MLLP)

Communicates HL7 messages using TCP/IP

Wraps messages in the following:

Start block: 1 byte - 0x0B
End block: 1 byte - 0x1C
Carriage return: 1 byte - 0x0D

```
\x0bMSH|^~\&|SENDING_APPLICATION|SENDING_FACILITY|RECEIVING_APPLICATION|RECEIVING_FACILITY|20170613083617||ADT^A01|911576
160110613083617|P|2.3||||
EVN|A01|20170613083617|||
PID|1||135769||MOUSE^MICKEY^||19281118|M|||123 Main St.^^Lake Buena Vista^FL^ 32830||(407)939-
5555^^^ohtoodles@notdisney.com|||||1719|999999999||| |MOUSETOWN||||||||||||||||
NK1|1|MOUSE^MINNIE|WIFE||||||NK
AL1|1||^Penicillin||Anaphylactic shock
AL1|2||^Cat dander|Skin rash
\x1c\x0d
```

WITH secure

Common Vulnerabilities



Vulnerabilities

No authentication Anyone can send/amend messages

No tamper detection Amending without detection

Denial of Service Connections kept open + maximum connections

Cleartext Person-in-the-Middle + ARP Spoofing

Forescout: https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/
Dallas Haselhorst: https://linuxincluded.com/hl7-medical-attacking-defending/

W/TH secure

Impact

Access to patient data

Changing patient records

Removing allergen information

Injecting into HL7 segments and fields

Causing a medical device to crash

Challenges with Testing HL7

WITH secure

Fingerprinting HL7

Non-default ports Not predictable

No reliable fingerprinting in port scanning tools

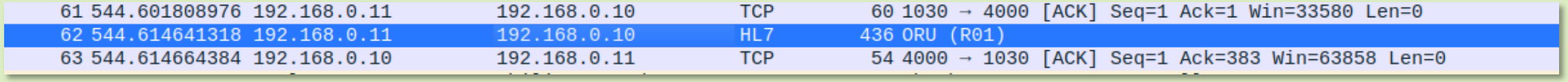
Default ports at device level

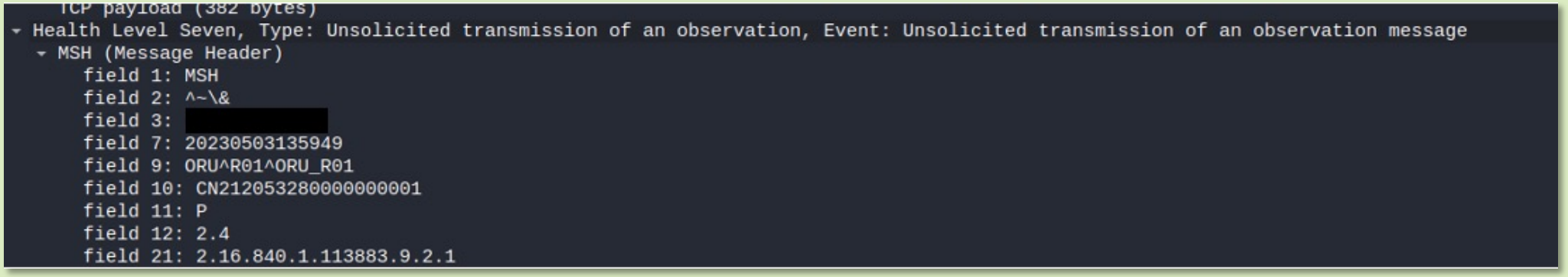
DoS? 😅

Intercepting Traffic

Cleartext protocol unless SSL has been manually configured

Mostly sent through M/LLP -> No easy way to proxy traffic





WITH secure

Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.0.11	192.168.0.10	TCP	62	1171 → 4000 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM=1
2	0.000056331	192.168.0.10	192.168.0.11	TCP	62	4000 → 1171 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1
3	0.001933119	192.168.0.11	192.168.0.10	TCP	60	1171 → 4000 [ACK] Seq=1 Ack=1 Win=33580 Len=0
4	0.011842022	192.168.0.11	192.168.0.10	HL7	453	ORU (R01)
5	0.011876926	192.168.0.10	192.168.0.11	TCP	54	4000 → 1171 [ACK] Seq=1 Ack=400 Win=63841 Len=0

eth1: <live capture in progress>

Packets: 5 · Displayed: 5 (100.0%)



Readability

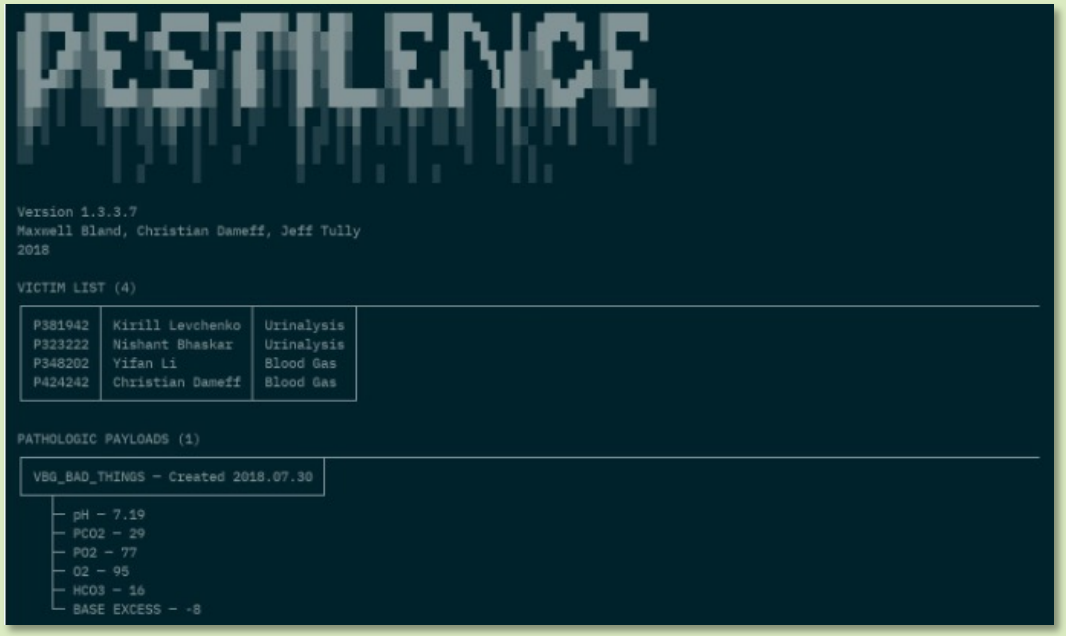
MSH|^~\&#|^372520^L|^372521^L||^372523^L|20150926140551||ORU^R01^ORU_R01|LRI_3.0_1.1-NG|D|2.5.1|||AL|AL|||||LRI_Common_Component^^2.16.840.1.113883.9.16^ISO~LRI_NG_Component^^2.16.840.1.113883.9.13^ISO~LRI_FRU_Component^^2.16.840.1.113883.9.83^ISO
PID|1||PATID1234^^^NIST MPI^MR||Jones^William^A^^^^L||19610627|M||2106-3^White^HL70005|||||||PATID1234^^^NIST MPI^AN
ORC|RE|ORD777888^NIST EHR|R-220713^NIST Lab Filler|GORD874244^NIST EHR|||||||5742200012^Radon^Nicholas^^^^^^NPI^L^^^NPI
OBR|1|ORD777888^NIST EHR|R-220713^NIST Lab Filler|24331-1^Lipid 1996 panel in Serum or Plasma^LN^345789^Lipid Panel^99USL^2.52^^Lipid 1996 panel in Serum or Plasma|||20150925||||||F^Patient was fasting prior to the procedure.^HL70916^^^^2.7.1^^fasting 12 hours|||5742200012^Radon^Nicholas^^^^^^NPI^L^^^NPI||||||20150926140551|||F|||10092000194^Hamlin^Pafford^^^^^^NPI^L^^^NPI||||||||||||||||||||CC^Copies Requested^HL70507
OBX|1|NM|2093-3^Cholesterol [Mass/volume] in Serum or Plasma^LN^^^^2.52^^Cholesterol [Mass/volume] in Serum or Plasma||196|mg/dL^milligrams per deciliter^UCUM^^^^1.9|Recommended: <200; Moderate Risk: 200-239 ; High Risk: >240|N|||F|||20150925|||||201509261400||||Century Hospital^^^^^CLIA^XX^^^24D9871327|2070 Test Park^^Los Angeles^CA^90067^^B|5432178916^Knowsalot^Phil^^^Dr.^^^NPI^L^^^NPI||||RSLT
OBX|2|NM|2571-8^Triglyceride [Mass/volume] in Serum or Plasma^LN^^^^2.52^^Triglyceride [Mass/volume] in Serum or Plasma||100|mg/dL^milligrams per deciliter^UCUM^^^^1.9|40 to 160|N|||F|||20150925|||||201509261400||||Century Hospital^^^^^CLIA^XX^^^24D9871327|2070 Test Park^^Los Angeles^CA^90067^^B|5432178916^Knowsalot^Phil^^^Dr.^^^NPI^L^^^NPI||||RSLT
OBX|3|NM|2085-9^Cholesterol in HDL [Mass/volume] in Serum or Plasma^LN^^^^2.52^^Cholesterol in HDL [Mass/volume] in Serum or Plasma||60|mg/dL^milligrams per deciliter^UCUM^^^^1.9|29 to 72|N|||F|||20150925|||||201509261400||||Century Hospital^^^^^CLIA^XX^^^24D9871327|2070 Test Park^^Los Angeles^CA^90067|5432178916^Knowsalot^Phil^^^Dr.^^^NPI^L^^^NPI||||RSLT
OBX|4|NM|2089-1^Cholesterol in LDL [Mass/volume] in Serum or Plasma^LN^^^^2.52^^Cholesterol in LDL [Mass/volume] in Serum or Plasma||116|mg/dL^milligrams per deciliter^UCUM^^^^1.9|Recommended: <130; Moderate Risk: 130-159; High Risk: >160|N|||F|||20150925|||||201509261400||||Century Hospital^^^^^CLIA^XX^^^24D9871327|2070 Test Park^^Los Angeles^CA^90067^^B|5432178916^Knowsalot^Phil^^^Dr.^^^NPI^L^^^NPI||||RSLT
SPM|1|S2015-777888&NIST EHR^S-220713-1&NIST Lab Filler||119297000^BLD^SCT^^^^201509USEd^^Blood||||||||||||20150925

Overcoming Challenges with HL7Magic

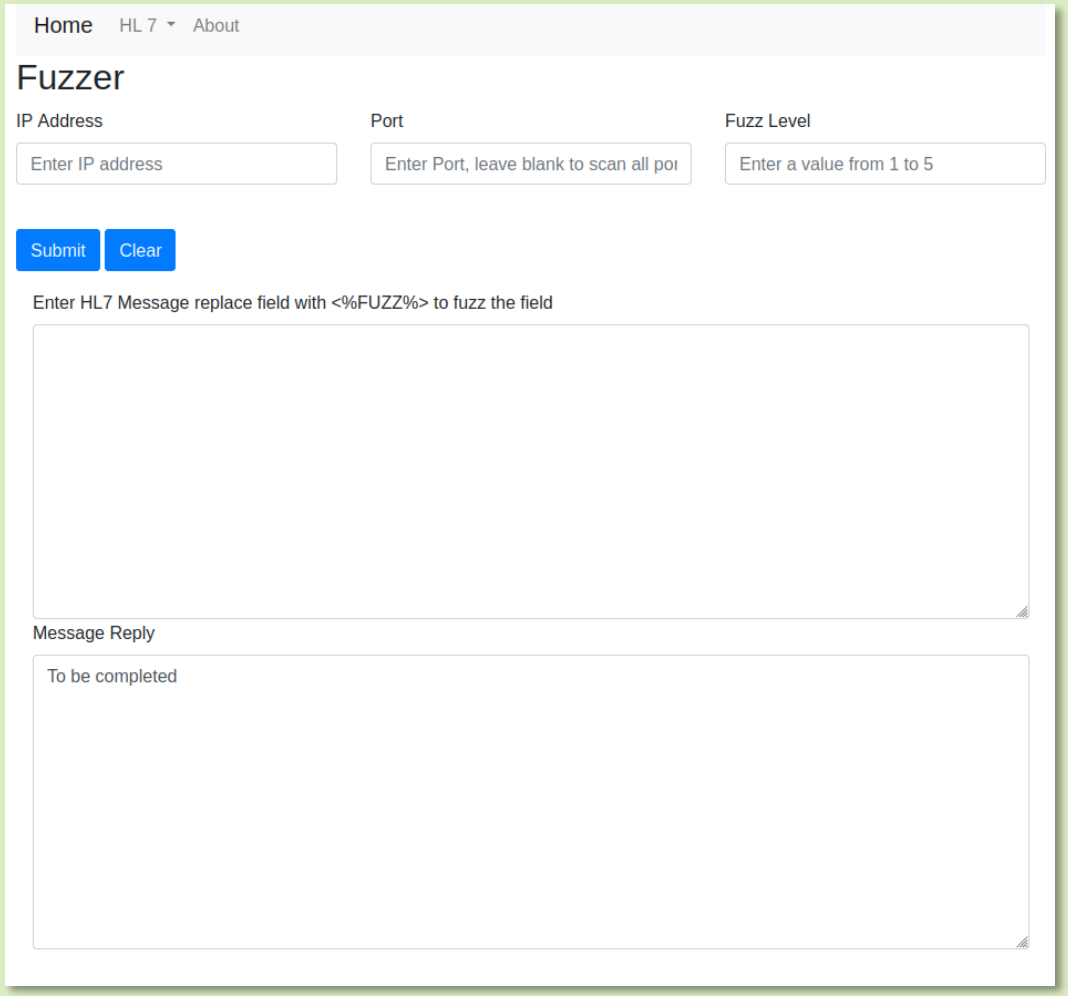


Existing Tooling

Pestilence (not released)



MedAudit



Christian Dameff, Maxwell Bland, Kirill Levchenko, Jeff Tully - Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives: https://i.blackhat.com/us-18/Thu-August-9/us-18-Dameff-Pestilential-Protocol-How-Unsecure-HL7-Messages-Threaten-Patient-Lives-wp.pdf
MedAudit - Anirudh Duggal: https://github.com/anirudhduggal/medaudit

Tooling Requirements

Ability to parse HL7 messages (of varying versions)

Integration with existing security tools

Ability to intercept messages

Ability to easily read message contents

Ability to change message contents

Ability to inject into fields or fuzz fields

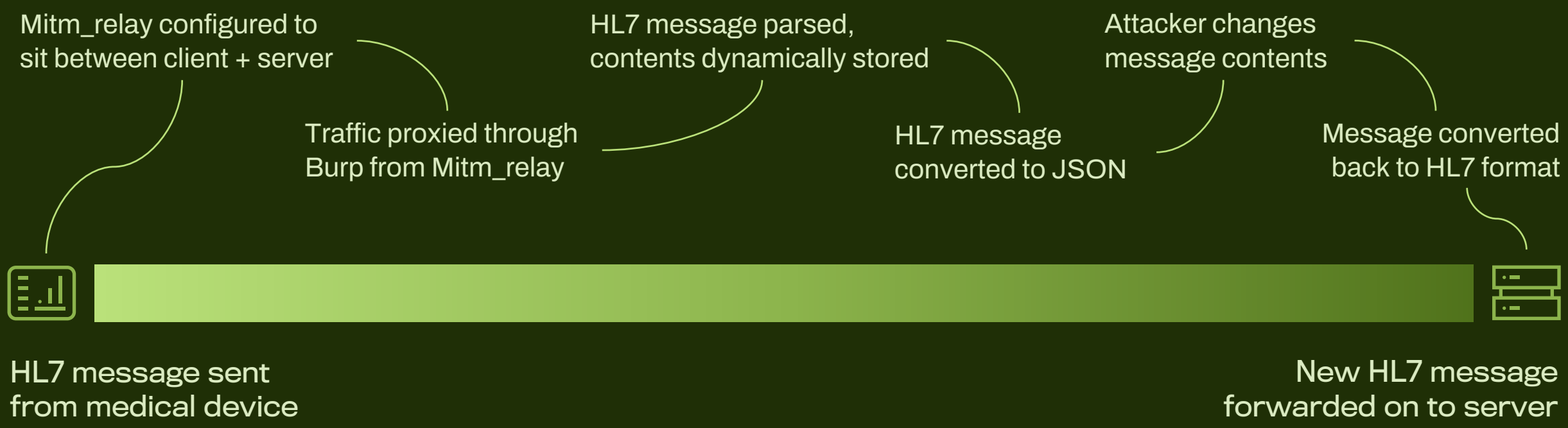
HL7Magic



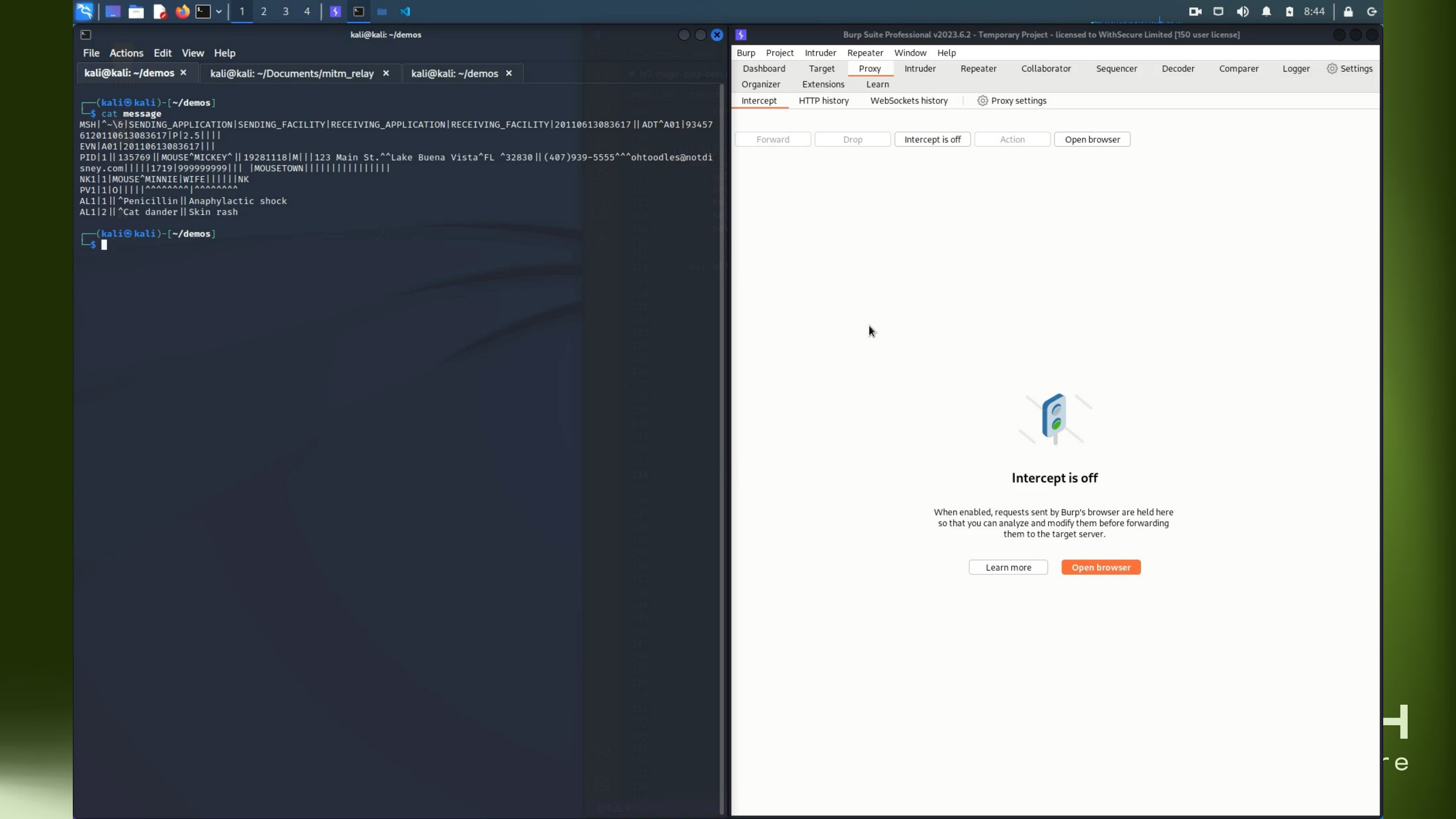
Burp Suite Extension
HL7apy Python library
Designed to make intercepting &
manipulating HL7 message easier

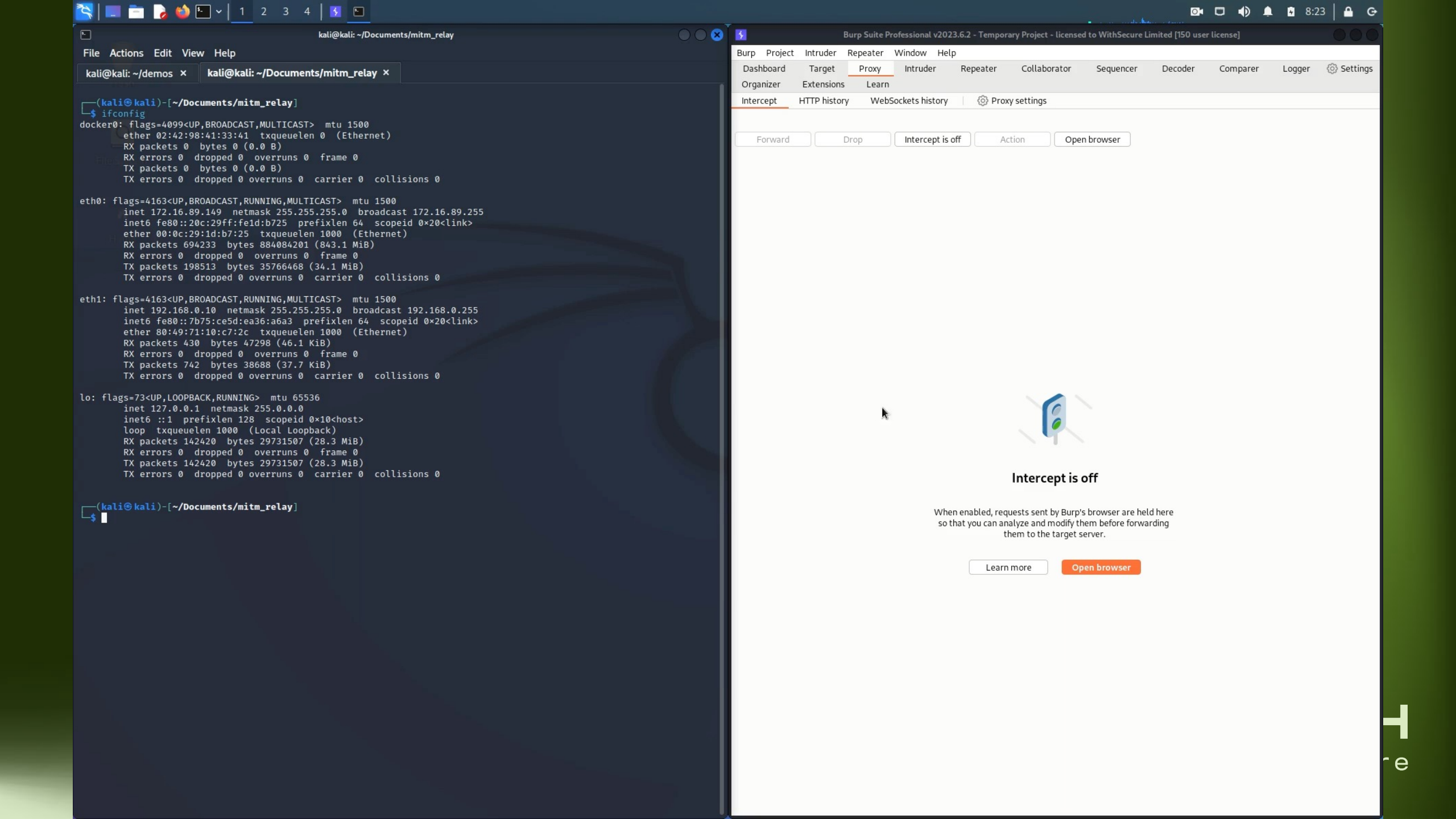


HL7Magic


Mitm_relay configured to sit between client + server
Traffic proxied through Burp from Mitm_relay
HL7 message parsed, contents dynamically stored
HL7 message converted to JSON
Attacker changes message contents
Message converted back to HL7 format
HL7 message sent from medical device
New HL7 message forwarded on to server

Demo


kali@kali: ~/demos
File Actions Edit View Help
kali@kali: ~/demos
kali@kali: ~/Documents/mitm_relay
kali@kali: ~/demos
(kali㉿kali)-[~/demos]
$ cat message
MSH|^~\&|SENDING_APPLICATION|SENDING_FACILITY|RECEIVING_APPLICATION|RECEIVING_FACILITY|20110613083617||ADT^A01|934576120110613083617|P|2.5||||
EVN|A01|20110613083617|||
PID|1||135769||MOUSE^MICKEY^||19281118|M|||123 Main St.^^Lake Buena Vista^FL ^32830||(407)939-5555^^^ohtoodles@notdisney.com|||||1719|999999999||| |MOUSETOWN||||||||||||||||
NK1|1|MOUSE^MINNIE|WIFE||||||NK
PV1|1|O|||||^^^^^^^^|^^^^^^^^
AL1|1||^Penicillin||Anaphylactic shock
AL1|2||^Cat dander||Skin rash
(kali㉿kali)-[~/demos]
$
Burp Suite Professional v2023.6.2 - Temporary Project - licensed to WithSecure Limited [150 user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Intercept is off
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser


kali@kali: ~/Documents/mitm_relay
File Actions Edit View Help
kali@kali: ~/demos
kali@kali: ~/Documents/mitm_relay
(kali㉿kali)-[~/Documents/mitm_relay]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
ether 02:42:98:41:33:41 txqueuelen 0 (Ethernet)
RX packets 0 bytes 0 (0.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 0 bytes 0 (0.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 172.16.89.149 netmask 255.255.255.0 broadcast 172.16.89.255
inet6 fe80::20c:29ff:fe1d:b725 prefixlen 64 scopeid 0x20<link>
ether 00:0c:29:1d:b7:25 txqueuelen 1000 (Ethernet)
RX packets 694233 bytes 884084201 (843.1 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 198513 bytes 35766468 (34.1 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.0.10 netmask 255.255.255.0 broadcast 192.168.0.255
inet6 fe80::7b75:ce5d:ea36:a6a3 prefixlen 64 scopeid 0x20<link>
ether 80:49:71:10:c7:2c txqueuelen 1000 (Ethernet)
RX packets 430 bytes 47298 (46.1 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 742 bytes 38688 (37.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 142420 bytes 29731507 (28.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 142420 bytes 29731507 (28.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
(kali㉿kali)-[~/Documents/mitm_relay]
$
Burp Suite Professional v2023.6.2 - Temporary Project - licensed to WithSecure Limited [150 user license]
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Settings
Organizer Extensions Learn
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is off Action Open browser
Intercept is off
When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.
Learn more
Open browser

Takeaways

HL7 is the most commonly used protocol in the healthcare industry

HL7 is difficult to test from a security perspective

HL7Magic can provide testers with an easier method of testing devices using HL7

WITH secure

Thank you ☺

Katie Inns

WITH secure

References

- **Forescout - Connected Medical Device Security:** https://www.forescout.com/resources/connected-medical-device-security-a-deep-dive-into-healthcare-networks/
- **Dallas Haselhorst - HL7 Medical Attacking and Defending:** https://linuxincluded.com/hl7-medical-attacking-defending/
- **Anirudh Duggal - Understanding HL7 2.X Standards, Pen Testing and Defending HL7 2.X Messages:** https://www.youtube.com/watch?v=MR7cH44fjrc
- **Saurabh Harit - Breaking Bad: Stealing Patient Data Through Medical Devices:** https://www.blackhat.com/docs/eu-17/materials/eu-17-Harit-Breaking-Bad-Stealing-Patient-Data-Through-Medical-Devices.pdf
- **Christian Dameff, Maxwell Bland, Kirill Levchenko, Jeff Tully - Pestilential Protocol:** How Unsecure HL7 Messages Threaten Patient Lives: https://i.blackhat.com/us-18/Thu-August-9/us-18-Dameff-Pestilential-Protocol-How-Unsecure-HL7-Messages-Threaten-Patient-Lives-wp.pdf
- **HL7apy:** https://crs4.github.io/hl7apy/tutorial/index.html
- **CheckPoint - Global Cyber Attacks Continue to Rise:** https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/
- **Approov, Alissa Knight – Playing with FHIR:** https://approov.io/for/playing-with-fhir/

W / T H secure