Pestilential Protocol

how unsecure HL-7 messages threaten patient lives

maxwell bland
christian ‘quaddi’ dameff, MD
Jeff ‘r3plicant’ tully, MD

black hat USA 2018

Maxwell Bland
Security Researcher
UC San Diego

Christian Dameff, MD
Emergency Physician
UC San Diego

Jeff Tully, MD
Pediatrician &
Anesthesiologist
UC Davis

black hat
USA 2018

Disclaimer

the following presentation describes potential consequences arising from the exploitation of unsecure protocols in order to advocate for the implementation of improved security measures.

its creators do not advocate or condone the application of this material in real world environments.

the presentation includes a live Demo involving the use of needles to draw blood.

Case

LAS VEGAS GENERAL EMERGENCY DEPARTMENT

TIME: 04:00

The NIGHT SO FAR...

1 stroke
2 heart attacks
1 gunshot to the abdomen

NEW PATIENT BED 7

31 year old male comes in vomiting
Temp:37.3C Heart Rate:119
Resp:22 BP:97/70

Case

NEW PATIENT BED 7

HPI: Abd pain, N/V x1 day
No PO since buffet day prior
Excessive EtOH, decreased H20
PMH: Unknown
Allergies: None

Differential

Gallstones
Cholecystitis
Cholangitis
Hepatitis
Liver abscess
Budd-Chiari syndrome
Portal vein thrombosis
Acute myocardial infarction
Pancreatitis
Peptic ulcer disease
Functional dyspepsia
Gastroparesis

Splenic infarction
Splenomegaly
Splenic abscess
Splenic rupture
Appendicitis
Diverticulitis
Nephrolithiasis
Pyelonephritis
Acute urinary retention
Infectious colitis
Bowel obstruction
Gastric perforation

Cystitis
Ulcerative colitis
Crohn disease
Viral gastroenteritis
Bacterial peritonitis
Diverticulitis
Celiac disease
Adrenal insufficiency
Malignancy
Ketoacidosis
Abdominal migraine
Constipation

Health Level 7 Standard

International and ubiquitous

Transmits data regarding

- Orders
- Lab results
- Imaging results
- Clinical documents
- End-user management of applications

Health Level 7

A. V2 (1989) – Most common
   A. Plain text
   B. Pipe delimited
   C. Non XML Bases

B. V3 (2005) - Slow Adoption
   A. Plain text
   B. Pipe delimited
   C. XML Based

```
MSH|^~\&|Rapidcomm |Hospital|OpenEMR|Hospital|20180719164041||ORU^R01|0C0AGPD228ZGM001D808|P|2.4|||AL|AL|
PID|||99||TTT^BT|||U|
ORC|RE|
OBR|1|6|0C0AGPD228ZGM001D808|666^Venous Blood Gas|R||||||O||||BLDA^^^^^^^P|^Administrator|||||||||F|
OBX|1|ST|pH||7.12||7.350-7.450|L|||F|||20150528093432||||^^07143^RAPIDPoint 405|20150528093432|
OBX|2|ST|pCO2||27|mmHg|35.0-45.0||||F|
OBX|3|ST|pO2||77|mmHg|75.0-100.0|H|||F|
OBX|4|ST|tHb||21.5|g/dL|12.0-18.0|H|||F|
OBX|5|ST|O2Hb||97.0|%|94.0-97.0||||F|
OBX|6|ST|COHb||0.4|%|0.5-1.5|L|||F|
OBX|7|ST|MetHb||0.6|%|0.0-1.5||||F|
OBX|8|ST|HHb||2.0|%|0.0-5.0||||F|
OBX|9|ST|HCO3act||7|mmol/L|||||F|
OBX|10|ST|BE(B)||-12|mmol/L|||||F|
OBX|11|ST|sO2||98.0|%|92.0-98.5||||F|
OBX|12|ST|Samp. Type||BLDV||||||F|
```

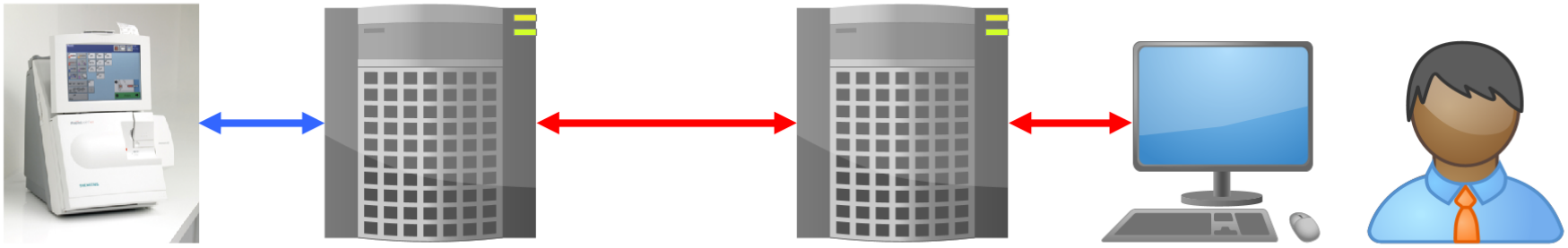
HL7- vulns

No encryption at standard level
No verification of message source
No authentication of message transmission

Yep...

Seriously.

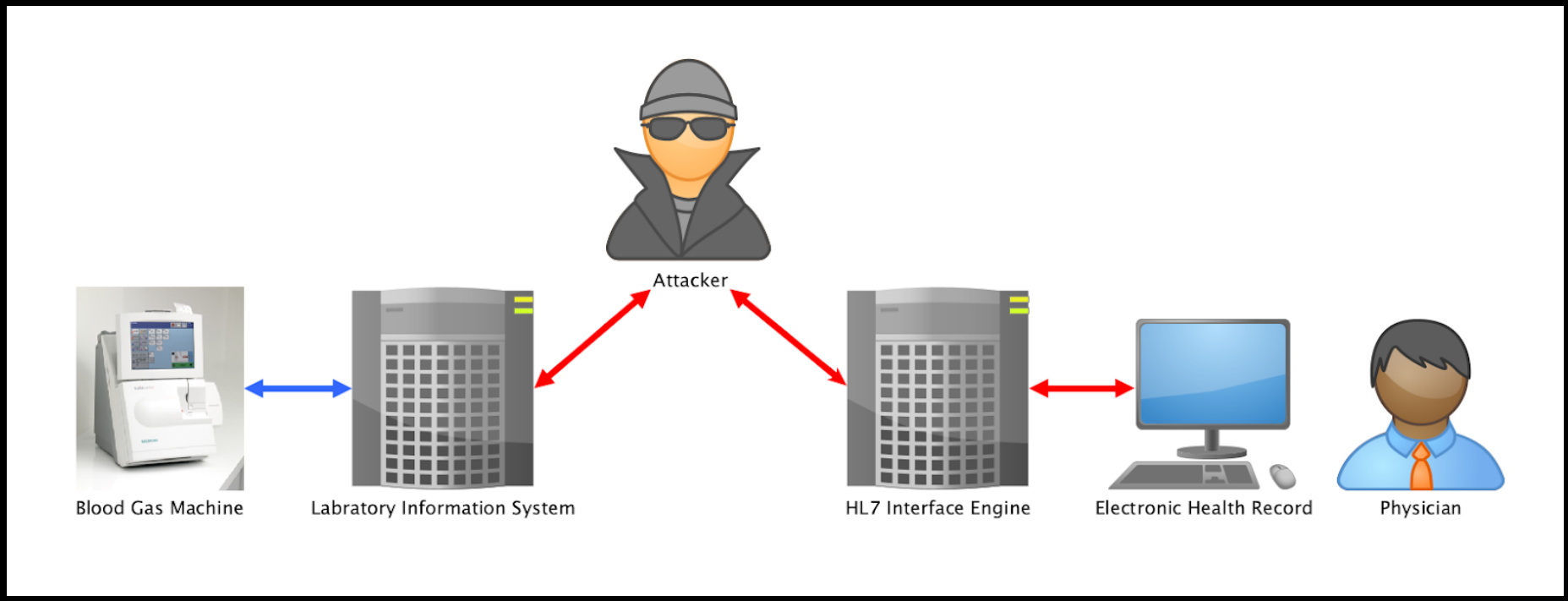
Test Bed

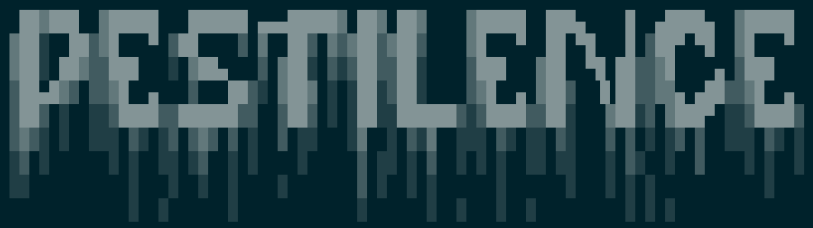


[DEMO]

Roleplay
H+P
EMR Orders -> Simple diff
Blood draw
Lab -> Rehash data flow
Results real -> Max shows
EMR results -> (split screen?)
Treatment
Death-> What happened?

MiTM





Version 1.3.3.7
Maxwell Bland, Christian Dameff, Jeff Tully
2018

VICTIM LIST (4)

P381942	Kirill Levchenko	Urinalysis
P323222	Nishant Bhaskar	Urinalysis
P348202	Yifan Li	Blood Gas
P424242	Christian Dameff	Blood Gas

PATHOLOGIC PAYLOADS (1)

VBG_BAD_THINGS — Created 2018.07.30

- pH — 7.19
- PCO2 — 29
- PO2 — 77
- O2 — 95
- HCO3 — 16
- BASE EXCESS — -8

Cultivating Crops ...
Initializing Server ...
Servers Ready ...
Poisoning ARP Tables ....
Waiting for Victims ...
Ready to go!

~ The art of communication is the language of leadership.

>>> set victim Christian

~ Alright, victim set to Christian Dameff.
~ Their current orders are Blood Gas.
~ A leader is one who knows the way, goes the way, and shows the way.

>>> set payload VBG_BAD_THINGS --times-to-infect=1 --fuzz-values-percent=0.01

~ Jesus, that one looks quite bad, are you sure about this?
~ Okay, whatever, waiting for victim ...
~ Still waiting ...
~ Still waiting ... don't you have anything better to do?
~ Lab results modified! Show pcap [Y/N]?
>>> N

~ A good leader takes a little more than his share of the blame, a little less than his share of the credit.

>>> exit

Solutions

1. Secure network deployment
2. Proper configuration
3. Security conscious protocols and ecosystems

Themes

- HIPAA Vs. Patient Safety
- Confidentiality vs Integrity vs Availability
- Legacy is Hard in Healthcare
  - Patching critical devices -> HARM
- Physicians don't know security and can harm


HIPAA
COMPLIANT
black hat
USA 2018

Q+A