Spring 3-27-2019

Detecting and Mitigating Cyberattacks Targeting Healthcare Transactions

Robert Cannistra
Dakota State University

Josh Stroschein
Dakota State University

Yong Wang
Dakota State University

Recommended Citation

Cannistra, Robert; Stroschein, Josh; and Wang, Yong, "Detecting and Mitigating Cyberattacks Targeting Healthcare Transactions" (2019). *Annual Research Symposium*. 8.
https://scholar.dsu.edu/research-symposium/8

Detecting and Mitigating Cyberattacks Targeting Healthcare Transactions

Student Robert M. Cannistra
Faculty Dr. Josh Stroschein
Dr. Yong Wang

Motivation

Healthcare networks are vulnerable. A critical healthcare messaging protocol is insecure, vulnerable, and susceptible to cyber attacks.

Problem

Current Healthcare Organizations are exposing Protected Health Information (PHI) to insider attacks in healthcare transactions using Health Level Seven (HL7) interfacing. These transactions occur between internal healthcare systems such as Electronic Medical Record (EMR) systems, Picture Archiving and Communications System (PACS), Voice Recognition (VR), and external business partners such as referring physicians and affiliated healthcare providers and partners. HL7 message types send data in clear text across the network posing a cyber security risk where anyone listening has the ability to acquire sensitive PHI including name, address, phone number, email address, social security number, medical record number, date of birth, race, gender, patient history, credit card information, and medical records, among other things.

All Healthcare Transactions interact with an HL7 Interface Engine that acts as a gateway for sending and receiving messages to all systems within the medical workflow. The primary HL7 message types used are:

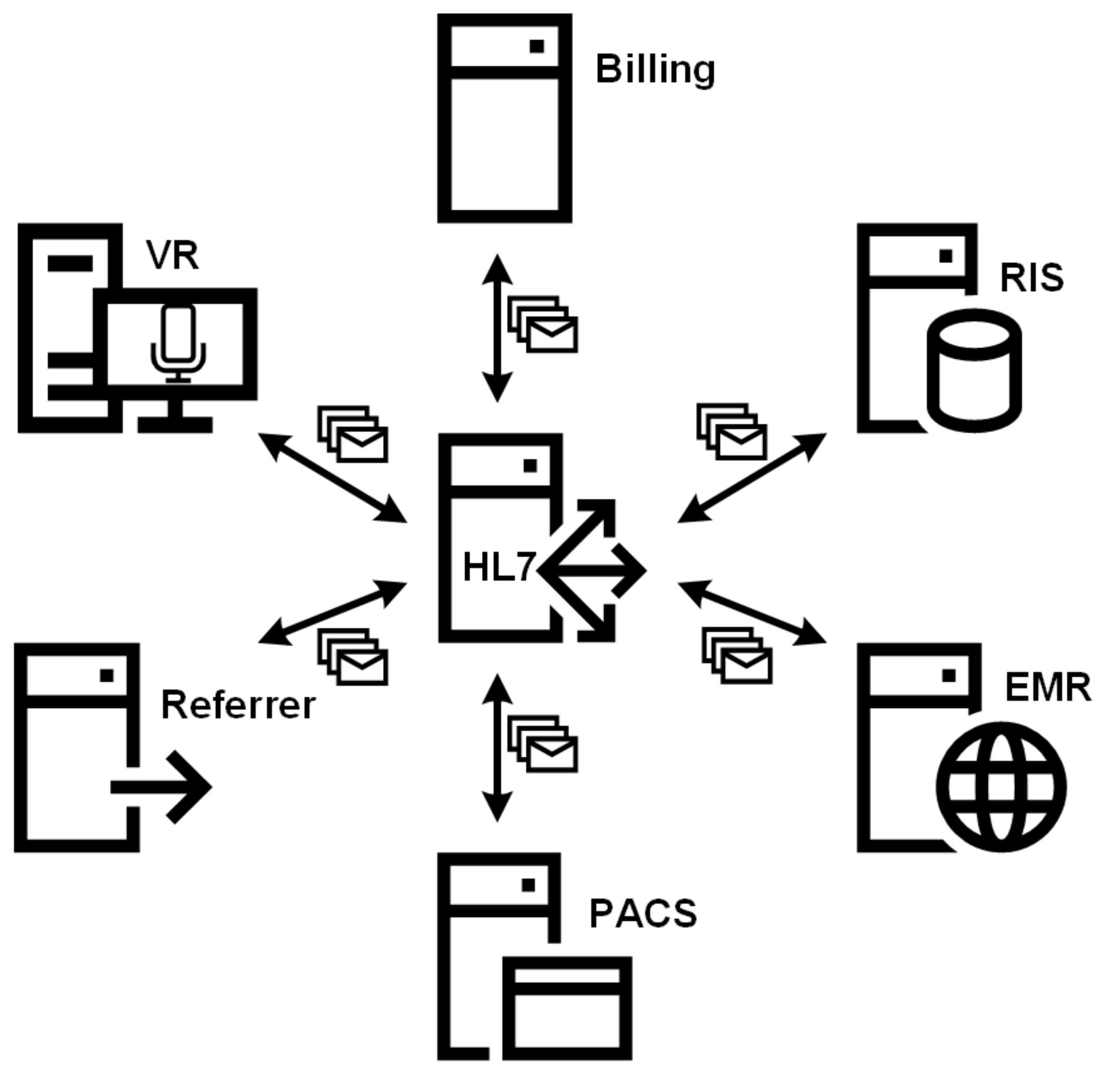
ADT (Admissions, Discharges, and Transfers)
ORM (Order)
ORU (Order Results)

ADT-A04 Patient Registration Message

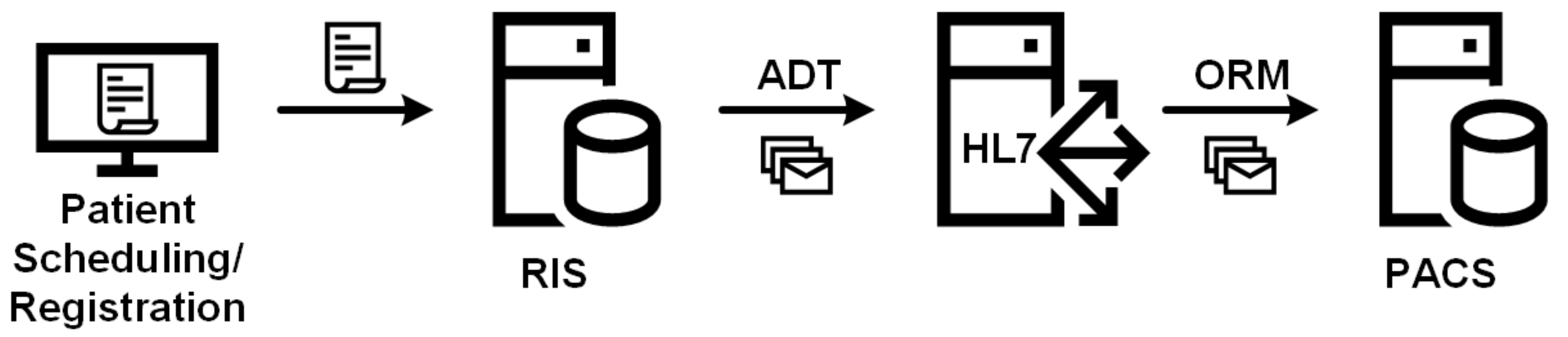
```
MSH|^~\&|ADT1|MCM|LABADT|MCM|198808181126|SECURITY|ADT^A04|MSG00001|P|2.4
EVN|A01-|198808181123
PID|||PATID1234^5^M11||ROCKS^SURI^CON^III||19610615|M-||2106-3|1200 MAIN STREET^^MADISON^SD^57042-
0000|GL|(605)256-5799|(605)256-5799~(605)256-5799||S||PATID12345001^2^M10|123456789|9-87654^NC
NK1|1|ROCKS^KARA^A|SPO|||||20011105
NK1|1|ROCKS^LUCA^R|FTH
PV1|1|I|2000^2012^01||||004777^LEBAUER^SIDNEY^J.|||SUR||-||1|A0-
AL1|1||^PENICILLIN||PRODUCES HIVES~RASH
AL1|2||^CAT DANDER
DG1|001|I9|1550|MAL NEO LIVER, PRIMARY|19880501103005|F||
PR1|2234|M11|111^CODE151|COMMON PROCEDURES|198809081123
ROL|45^RECORDER^ROLE MASTER LIST|AD|CP|KATE^SMITH^ELLEN|199505011201
GT1|1122|1519|BILL^GATES^A
IN1|001|A357|1234|BCMD|||||132987
IN2|ID1551001|SSN12345678
ROL|45^RECORDER^ROLE MASTER LIST|AD|CP|KATE^ELLEN|199505011201
```

Healthcare Transaction Systems

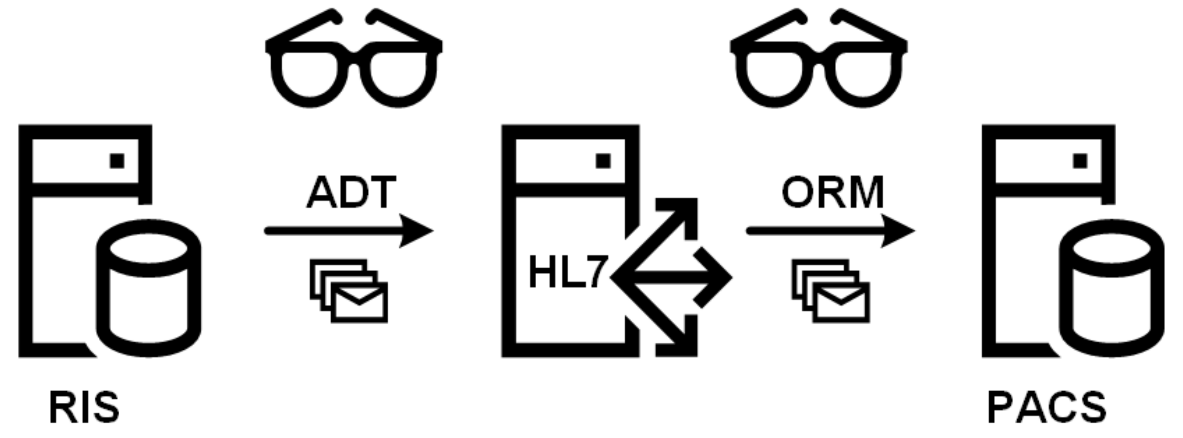
Healthcare Transactions occur to and from HL7 Interface Engine



Initiating Medical Workflow Transaction from RIS to PACS



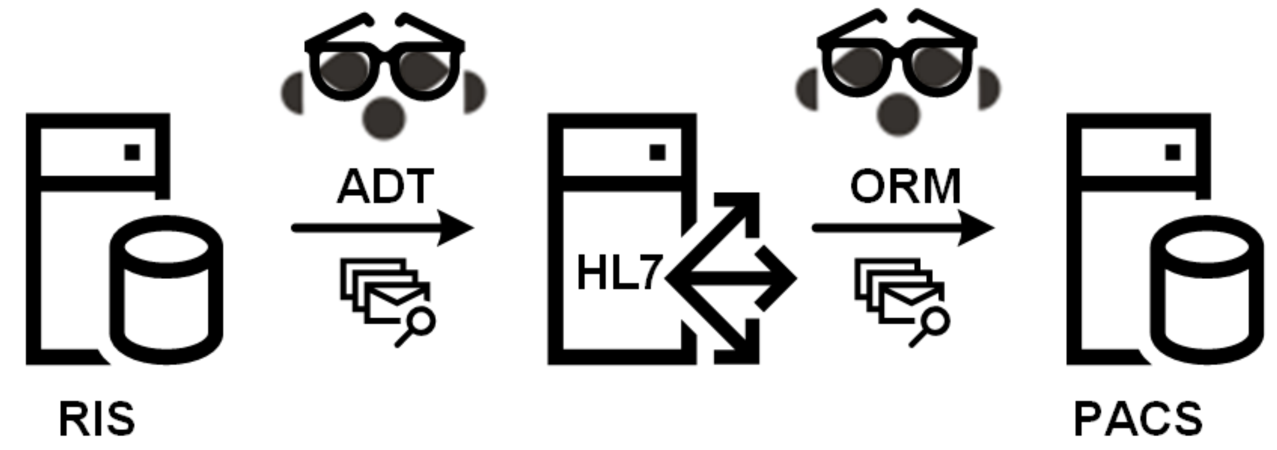
Insider Attack on HL7 ADT and ORM Message Types



Solution

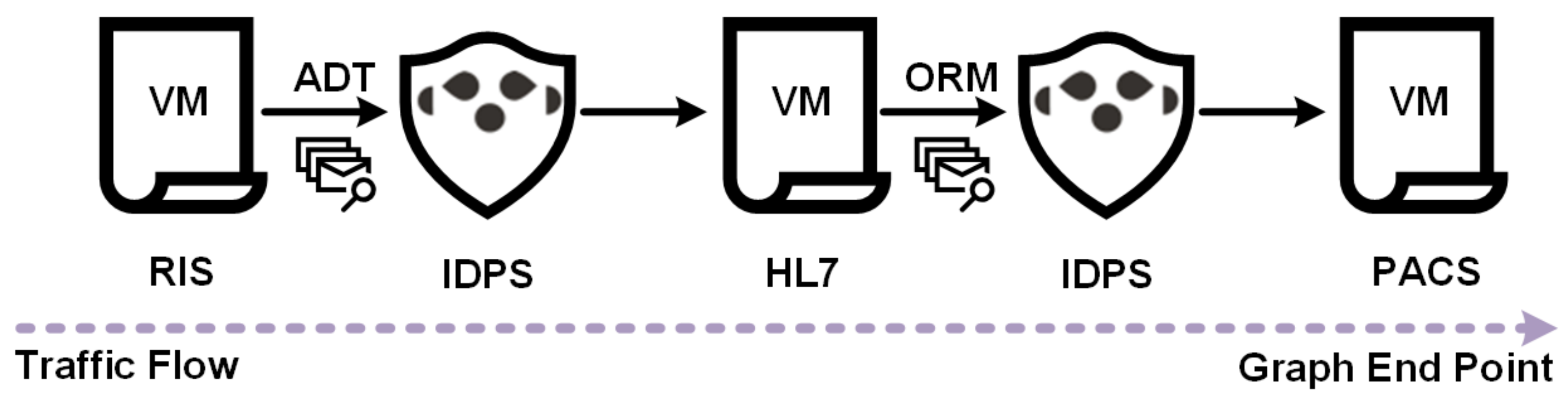
Utilizing the Suricata IDPS provisioned as a VNF (Virtual Network Function) based on the ETSI NFV MANO Architecture, insider attacks targeting HL7 ADT, ORM, and ORU message types are detected, classified, and mitigated before sensitive PHI is stolen. This uses the concept of a network service as a subset of the end-to-end service formed by VNF and virtual links instantiated for the medical workflow using the HL7 message type, source IP Address, destination IP Address, and TCP port number.

Suricata Mitigating Insider Attacks on HL7 ADT and ORM Message Types



By introducing abstraction in terms of virtual functions, virtual links, and connection points, a network service graph is formed for cyber threat protection.

Virtualized Medical Workflow utilizing ETSI Architecture



Future Work

Design an IDPS analysis framework to improve upon the overall effectiveness and efficiency of bad actor threat detection, classification and mitigation to uphold patient confidentiality, integrity, and availability of Protected Health Information (PHI).

robert.cannistra@trojans.dsu.edu
joshua.stroschein@dsu.edu
yong.wang@dsu.edu