I’m Not A Doctor But I Play One On Your Network

Tim Elrod and Stefan Morris

About Us

- Tim Elrod –
  - Penetration Tester for Fishnet Security
  - Over 7 years pentesting healthcare systems
- Stefan Morris –
  - Penetration Test for Fishnet Security
  - Over 4 years Pentesting healthcare systems

Technology Redux

- Common Healthcare Technologies
  - Hl7
  - Dicom
- A History of Standard Non-standard Standards

Why Would You Care?

- HIPAA Doesn’t Help: There’s no PCI for Healthcare
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Identity theft
  - Medical identity theft
- Loss of Life and Limb

PACS

- What are Picture Archiving and Communication Systems (PACS)?
- Digital Imaging and Communications in Medicine (DICOM)
  - DICOM the network protocol
  - DICOM the file format
  - Fuzzing DICOM

HL7 Interface Systems

- Health Level 7 (HL7) Protocol and Standards
  - Clear Text Protocol
  - Delimited fields contain either codes or data
  - Sub fields can also contain codes or data
- Centralized Data Storage and Structure of HL7 Systems
- HL7 Routers
- Fuzzing HL7

Electronic Health/Medical Record Systems

- Medical Record Storage
  - Most medical records are stored in multiple systems across the healthcare environment
  - Health records can exist in databases as well as unstructured data files
- Front End Interfaces and Issues
  - Common web application issues
  - Logic flaws regarding user permissions

Health Information Exchanges (HIE)

- Building a National Healthcare System and Efficiency Through Legislation
- Regional and National HIE Structure
- Vulnerabilities Introduced by the Interconnectivity of Immature Systems

Personal Health Records (PHR)

- Health Vault
- Google
- Others

Malicious Health Records (MHR)

- Records input into PHRs such as Google health and Microsoft health vault get parsed and acted upon by backend health systems such as HL7 Routers
- It is possible for an attacker to inject health records and then cause vulnerabilities to be triggered in backend systems

Medical Hardware Review

- Prescription Dispensing Cabinets
  - Omnicell

Q&A

- Hit us up in the q&a area or buy us a beer at the bar