Healthcare’s Losing Battle Against the Hyper-Connected Machines

Kurt Hagerman  
CISO | Armor

Dr. Chase Cunningham  
Director of Cyber Threat Research | Armor

Will Long  
Vice President & CISO | Children’s Medical
Your Moderator

Will Long
Vice President & CISO | Children’s Medical

- MS, CISSP & CPHIMS certifications
- 30-plus years IT experience
- Veteran of payer and provider healthcare sectors
- B.S. Electronic Engineering Technology
- M.S. in Information Systems Management
- MIT Cybersecurity Training
- Active in CHIME
Security & Compliance Experts

Dr. Chase Cunningham
Director of Cyber Threat Research & Innovation

• Former Cryptologist for the National Security Agency
• U.S. Navy (Chief Ret.)
• PhD in Cybersecurity
• TRU Team Founder
• Co-Author of *The Cynja*

Kurt Hagerman
Chief Information Security Officer

• CISA- and CISSP-certified
• Frequent speaker and author on security for the payments industry, healthcare industry and cloud security
• 25-year veteran in IT, security, consulting and auditing
Is IOT Leaving Hospitals Vulnerable to the Cruelest Attack Vectors?
Inside the Healthcare Threat Landscape
Healthcare’s Exposed

- Devices Vulnerable to Legacy Software
- Inadequate Patch Management
- Lack of Threat Education

- Unique Use Cases
- Difficult Encryption Deployment
- Lack of Network Segmentation for Devices
Security Gaps Affect Real Patients
“It’s going to come to a breaking point sooner or later.”

SCOTT ERVEN
Associate Director
Protiviti

During the 2016 Kaspersky Lab Security Analyst Summit in Spain
Healthcare Threats

⚠️ Devices

“Thousands of medical devices are vulnerable to hacking, security researchers say”

— PCWorld | September 2015

⚠️ Innovation

Healthcare is “10 to 15 years” behind the retail sector when it comes to security.

— Threatpost | February 2016

⚠️ Treatment

Systems for cardiology, infusion and MRIs all showed more than 30 vulnerabilities per device. This will soon have a direct impact on treatment and patient care.

— Threatpost | February 2016
The Threat Actor Methodology
What Threat Actors Target in Healthcare

Patient Assets

- Patient Health
- Patient Records
- Service Availability
- Community Confidence

Hospital Assets

- Research / IP
- Business Advantages
- Hospital Finances
- Hospital Reputation
- Physician Reputation

“Securing Hospitals: A Research Study & Blueprint”  
How Threat Actors Select

How do threat actors choose their attacks?
It’s a simple business proposition.

Cost + Risk < Reward = Do It

If the cost and reward are the same, choose the lower risk attack.

If the risk and reward are the same, choose the lower cost attack.

“Securing Hospitals: A Research Study & Blueprint”
Why The Formula Matters

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>As healthcare becomes more connected, more devices are available.</td>
<td>As more devices are connected, there's more opportunity for compromise.</td>
<td>As more attack vectors are added, it drives down the operating cost for threat actors.</td>
<td>As the cost goes down and the value of healthcare data increases, more and more attacks will occur.</td>
</tr>
</tbody>
</table>
Why Can’t We Do Better?
Defending the Healthcare Landscape

Objectives

• Protect ePHI Data
• Build Secure Infrastructure
• Secure Medical End Points
• Enable Seamless Processes
• Make Security Easy for End-Users
  (e.g., doctors, nurses, administrators)

Challenges

• Don’t Understand My Data Landscape
• Poor Authentication
• Weak Role-Based Controls
• Stubborn End-User Adoption
• Compliance Isn’t Prescriptive
It’s Just ’Ones & Zeroes’

Simplify

Only so many ways to secure data that’s stored, transmitted, processes or accessed.

Learn

Get to know your data — where it’s stored, what it is and who is accessing it. Learn to do the big things right.

Understand

You and your organization are responsible for the data of your patients, customers and partners. Take responsibility for securing it.

Follow

Use other compliance controls — PCI or NIST — as guideposts. They are more prescriptive and will help you achieve compliance and basic security objectives.
Security Must Be Bi-Directional
Think Bi-Directionally
‘0000’
Segment & Defend
Surface Area of Attacks

Applications

Networks

Humans
Take Back the Initiative

Endpoints vs Data
Big Cloud Problems

Internet

Massive Healthcare Cloud
A Micro-Cloud Approach
The Time to Act?

Now.
Remember Three

Everything, Everywhere Is Connected

Understand Your Data

Leverage Clouds the Correct Way
QUESTIONS?
Discussion Points

• Have you discovered and/or mitigated any medical device security issues?
• What security challenges are you facing with connected medical devices?
• What is the biggest risk you foresee for network- or cloud-connected medical device security?
• How are you addressing the gap of IS security teams and knowledge of device landscape?
• How can we collaborate on challenges and solutions?
Thank You

Kurt Hagerman  CISO | Armor
Dr. Chase Cunningham  Director of Cyber Threat Research | Armor
Will Long  Vice President & CISO | Children’s Medical