

# Unsecured Endpoints in the Hospital Environment Securing IOT and Medical Devices

Stewart Tan  
Cisco Security Principal





## AGENDA

1. The Changing Face of Security
2. The IOT Medical Device Challenge
3. How to Secure the Un-Securable?
4. Intelligence: The Dangers of Unchecked IoT

# The Changing Face of ..... Security

A person wearing a blue hoodie is sitting at a wooden desk, looking at a silver laptop. The background is dark blue with vertical lines of white and red text, including the word 'PASSWORD' written vertically in red. The overall theme is cybersecurity and digital security.


The Internet of  
**THINGS!**

**Healthcare is under attack!**



# Hollywood hospital becomes ransomware victim

The cyberattack prompted the centre to declare an "internal emergency," with access to IT systems left locked and held for ransom.

By  Charlie Osborne for Zero Day | February 15, 2015 -- 12:23 GMT (04:23 PST) | Topic: Security



## RELATED STORIES



Security  
**Ransomware: How much would you pay to get your files back?**



Government  
**Obama's gadgets: What tech does the president use?**



CTO  
**Online security? Just let me Google that, say puzzled bosses**

# Ransomware Attackers Double-Bill Hospital

Kansas Heart Hospital Pays Ransom, Gets Told to Pay Again

Mathew J. Schwartz ([@euroinfosec](#)) • May 23, 2016  0 Comments

# BALTIMORE

## Post-Examiner

### FBI investigating computer hack, possible ransom demand at MedStar Health

BY ANTHONY C. HAYES · MARCH 28, 2016 · 1 COMMENT



# MedStar Health

The FBI is investigating a computer hack and a possible ransom demand at Baltimore area MedStar hospital, according to sources familiar with the incident.

Because of this situation, staff at the affected locations cannot get into their computers, leaving personnel to conduct business with pen and paper.

 **REUTERS**

**TECHNOLOGY**

Mon Mar 28, 2016 | 5:33 PM EDT

Washington's MedStar Health shuts down computers after virus

"The web portal is powered by the Joomla CMS, running version 2.5.6 (latest version is 3.4.8) according to a manifest file present on their server. Several vulnerabilities exist for this outdated installation, which could explain why the site has been hacked."

Canadian hospital's website hacked to serve up  
Teslacrypt ransomware





KDH operates an 86-bed hospital and physicians' office in Madison, Ind. – Hit by Locky Ransomware March 30<sup>th</sup> on a single computer but shut whole network down

March 18- two of Prime Healthcare's hospitals in California - Chino Valley Medical Center and Desert Valley Hospital shutdown because of ransomware attack

March 16<sup>th</sup>, Kentucky Methodist Hospital – forced to shutdown computer systems when hit with Locky Ransomware.

A screenshot of a web browser displaying the website for Kentucky Methodist Hospital. The browser's address bar shows the URL 'www.methodisthospital.net'. A prominent red banner at the top of the page contains the text: 'Internal State of Emergency due to a computer virus. Click here for additional information.' Below the banner, the main content area features the Methodist Hospital logo on the left, which includes a stylized cross with a flame and the text 'METHODIST HOSPITAL' and 'Our mission is your health.' In the center, there is a Google Custom Search box with a 'Search' button. On the right side, contact information is provided: '1305 North Elm Street, Henderson, Kentucky 42420' and the phone number '270-827-7700'. At the bottom right, there are social media icons for Facebook and YouTube, along with the 'FAST COMMAND' logo, which is described as 'Digital Disaster Response System'.

# Northern Lincolnshire and Goole NHS Foundation Trust cancels ALL operations after cyber attack



## MAJOR INCIDENT - UPDATE

### MAJOR INCIDENT – APPOINTMENTS CANCELLED

A virus infected our electronic systems on Sunday October 30 and we have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it.

All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday November 2 with a small number of exceptions as follows:

- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics

**Patients told not to turn up for appointments or for surgery**



[Privacy & Security](#)

## More than half of hospitals hit with ransomware in last 12 months

New research by Healthcare IT News and HIMSS Analytics found considerable uncertainty, questionable business continuity plans, and the need for more effective end-user education rampant in the industry.

By [Tom Sullivan](#) | April 07, 2016 | 07:52 AM

SHARE



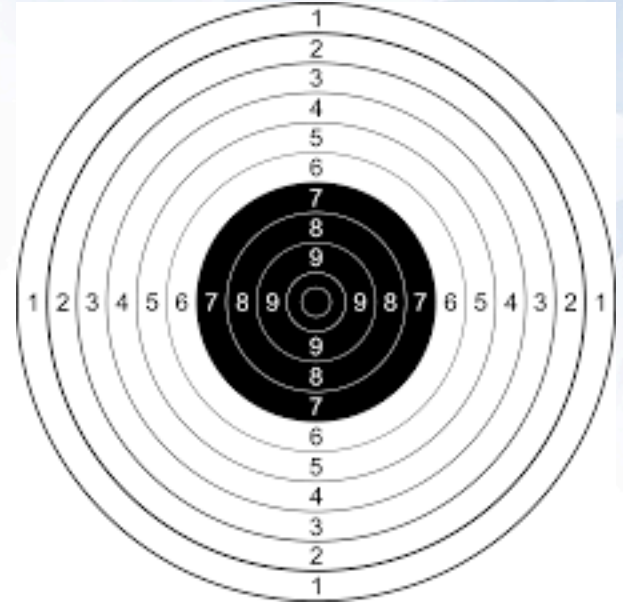
# Healthcare is Seen as an Easy Target

## Theft

- Theft of Medical Records - \$45~\$50 per
- Theft of full Identity – up to \$500
- Theft of clinical research / clinical trial data
- Theft of formulations / procedures

## Malicious Attack – DOS / Integrity /

- ICS systems – Critical hospital systems – water, air, heat, mechanicals
- Patient harm / assassination / poisoning



# The IoT / Medical Device Challenge

# The IoT / Medical Device Challenge

- 20% growth per annum in number of medical devices
- No common standards or security
- Windows Embedded 2009, (Windows XP)
- Dumb devices unable to support AV or End Point Protection
- Limited CPU and memory unable to sustain malware or DOS
- Easiest way to infiltrate a healthcare network is via a medical device / medical device network – 802.11 40 bit WEP or RJ45 port

# Legacy Medical Devices Aren't Going Away!

Half Life – Medical Devices last for up to 20 years

- 40 bit WEP anyone?
- Limited Network Stack



20% growth per annum in number of medical devices

# Converged Networks



IoT Now Being Targeted at a Hospital Near You!

The next ransom attacks will likely be leveled directly against Hospital IOT systems and Medical Devices

# IoT Now Being Targeted

- IOT services we can't do without:
  - HVAC,
  - Elevators / Lifts,
  - Water Management,
  - Electrical supply,
  - etc.



**Imagine a man-made  
Hurricane Katrina....**



**.... A Cyber Attack  
against our  
Healthcare IOT  
Systems**

# The Next Level of Ransoms...won't be against data

- Could Patient lives be held to ransom by compromised Medical Device?




In 2014, the Federal Bureau of Investigation issued a report that predicted hackers could assail medical devices

In 2015 they issued an alert warning companies and the public about cybersecurity risks to networked medical devices and wearable sensors

## Cyber Assassin

You don't need James Bond to carry out assassinations when you own the medical device targets are attached to



A man is lying in a hospital bed, appearing to be asleep or unconscious. He is wearing a light blue hospital gown with a small pattern. He has a nasal cannula in his nose and several medical sensors attached to his chest and arms. A yellow blanket is pulled up to his waist. To the left of the bed, there is a medical monitor on a stand. To the right, there are various medical devices and blue tubing. The background shows a typical hospital room setting with a light-colored wall and a wooden headboard.

Russian Oligarch,  
Mafia Boss or  
innocent victim?

**How Secure is your ICU?  
How confident are you  
about  
the security of your medical  
devices?**

What if the NICU was compromised ?



# The Weakest Link

So how can we go about protecting these simple networked devices in our healthcare environment?

How can we protect patients from malicious or unintentional harm?

# The Weakest Link

You **COULD** perform an assessment and configuration review of every IOT and medical device in each of your hospitals

- It would need to be ongoing!
- You would need an army!

Far easier to just assume the whole lot are a hopeless case and will be for the foreseeable future AT LEAST.. inherently  
**INSECURE**

# The Weakest Link

We need to **SEGMENT** them but in such a way that it doesn't impede patient care.

## Options:

1. Proxy traffic – simple, cheap, but doesn't scale
2. Infrastructure Enclaving (firewall & switch ACLs, MPLS, etc.) – inflexible, expensive to run & maintain and impedes the business
3. Dynamic policy-based segmentation – define once, apply globally



# Dynamic Policy Based Segmentation

- Easy to manage .... from one console across all sites
- Inclusive of all endpoints regardless
- Does not get in the way of the business of treating patients
- Enterprise Policy .... written once ... enforced globally
- Uses much of what you already own
- Uses your network to enforce your Policy

# Software-Defined Segmentation

## Desired Policy

- Who can talk to whom
- Who can talk to which systems
- Which systems can talk to other systems



	Patient Records	Employee Intranet	Internet
Doctor / Laptop	✓	✓	✓
Doctor / iPad	✗	✓	✓
Guest / Laptop	✗	✗	✓
Guest / iPad	✗	✗	✓

Simplifies Policy with Security Group Tagging

Reduces ACL and Firewall Rule Complexity

Allows for Segmentation without VLANs



Switch



Router



VPN &  
Firewall



DC  
Switch



Wireless  
Controller

**Flexible and Scalable Policy Enforcement**

# Questions / Comments