Medical device security

-- Anirudh Duggal

Disclaimer:
The views in the presentation are entirely my own and do not reflect the views of my employer.

Before we begin

- Thank you HITCON
- Specially thank the organizing team
- Jal , Pineapple, Turkey, Shanny, Shang and all the people whom I’ve troubled till now

About me

- Senior Software Engineer at Philips health tech
- anirudhduggal@gmail.com
- Sustainability enthusiast
- Interested in medical devices, IOT devices and hardened OS
- Part of Null community

Nullcon CFP is out!

nullcon

www.nullcon.net

the neXt security thing!

Agenda

- What is a medical device?
- Range of medical devices
- Medical record value and breaches
- Challenges
- Besides challenges
- Hl7 messaging

What is a medical device?

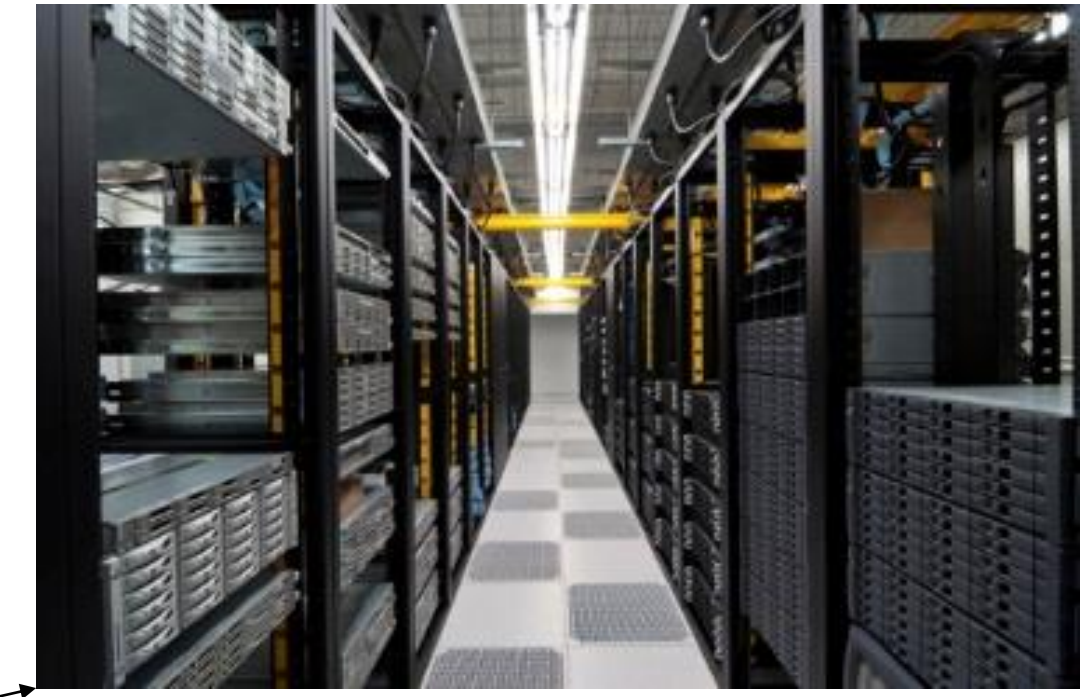
- A **medical device** is an instrument, apparatus, implant, in vitro reagent, or similar or related article that is used to diagnose, prevent, or treat disease or other conditions, and does not achieve its purposes through chemical action within or on the body (which would make it a drug) -- wiki

Range of devices

Cost: ~~5~~ 2$ (50% off)
Fits in pocket

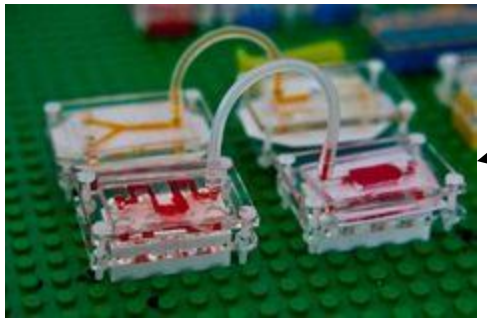
Cost: can reach up to 3 million $
Size: about the size of a truck (don't ask the weight ;))

And the memory



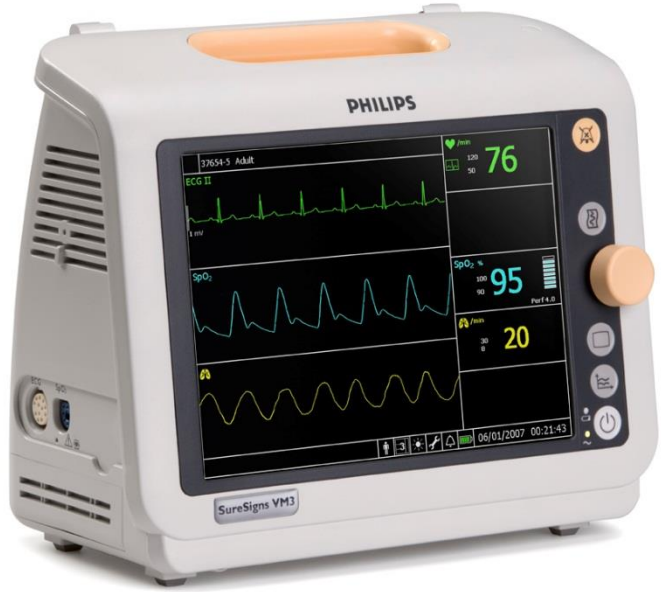
A hospital data center…

A simple DIY device



And……

- Patient monitors
- Insulin monitors
- Pacemakers
- Heart rate devices
- “smart bands”
- Home monitoring solutions



Rapid Innovation

- Everyone wants mobility (patient, doctors, nurses, clinicians)
- Diagnostics
- Big data analysis
- Information gathering

Why hospitals and medical devices?

- Easy targets
- Many entry points
- Good payoff
- Medical records

The impact of an attack

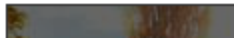
- Privacy
- Financial – a medical record fetches 32x a credit card record
- Physical?

2015 is already the year of the health-care hack — and it's only going to get worse.

Why Medical Identity Theft Is Rising And How To Protect Yourself

+ Comment Now + Follow Comments

Anthem. Premera. Carefirst.



Technology | Tue Feb 24, 2015 7:58pm EST

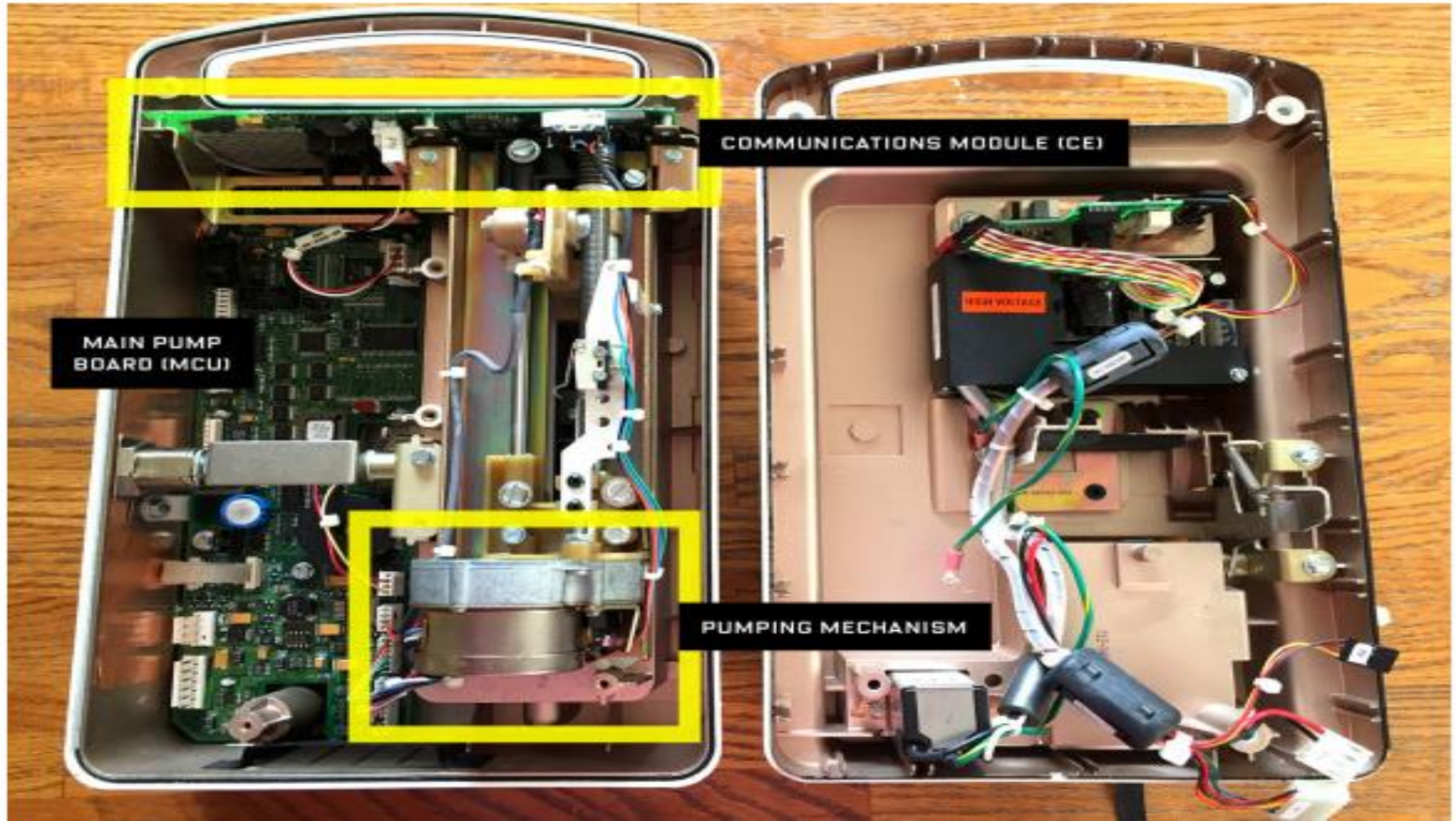
Related: TECH

Anthem says hack may affect more than 8.8 million other BCBS members

NEW YORK | BY CAROLINE HUMER

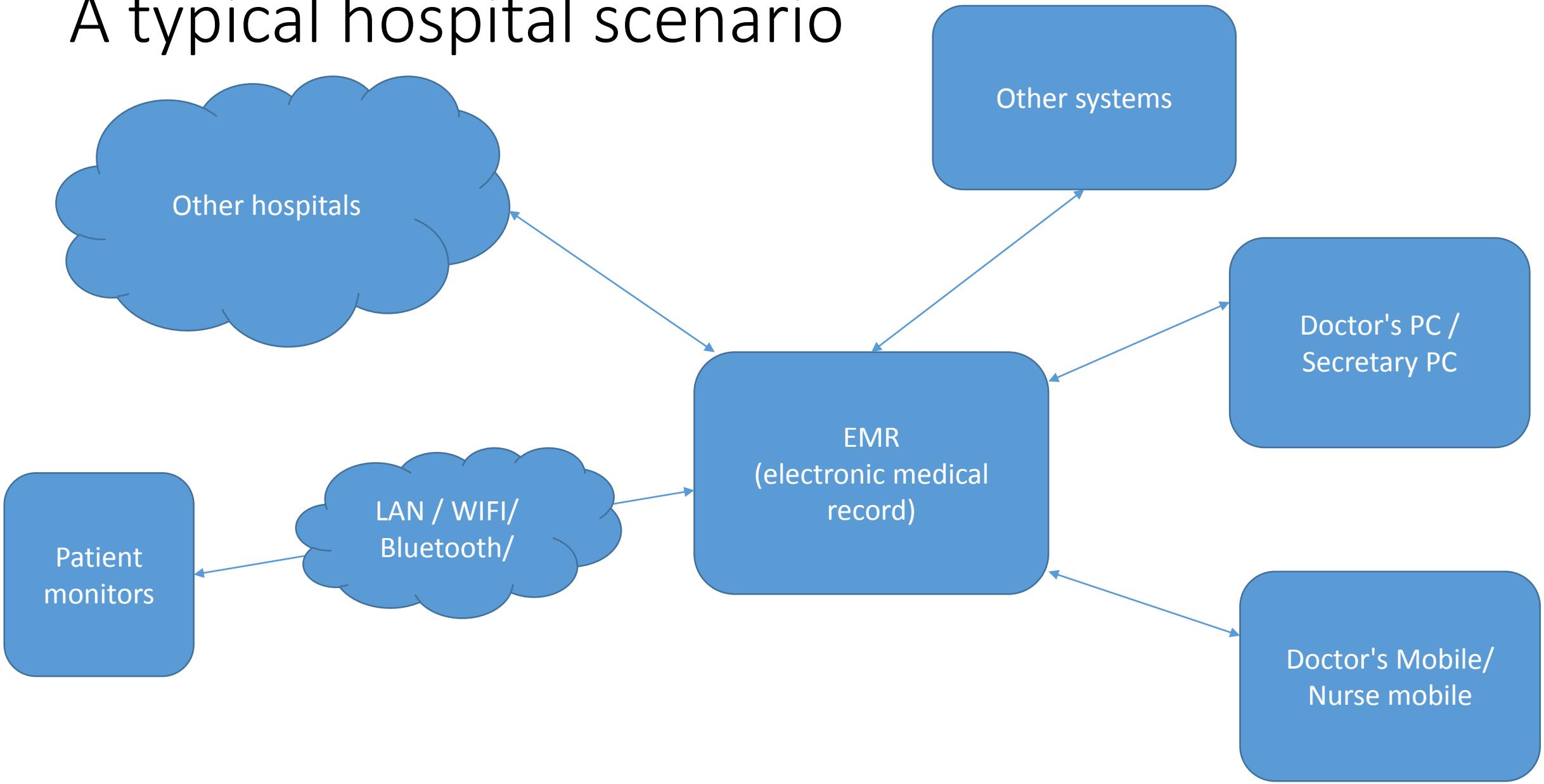
Lets take a case study

DRUG PUMP'S SECURITY FLAW LETS HACKERS RAISE DOSE LIMITS

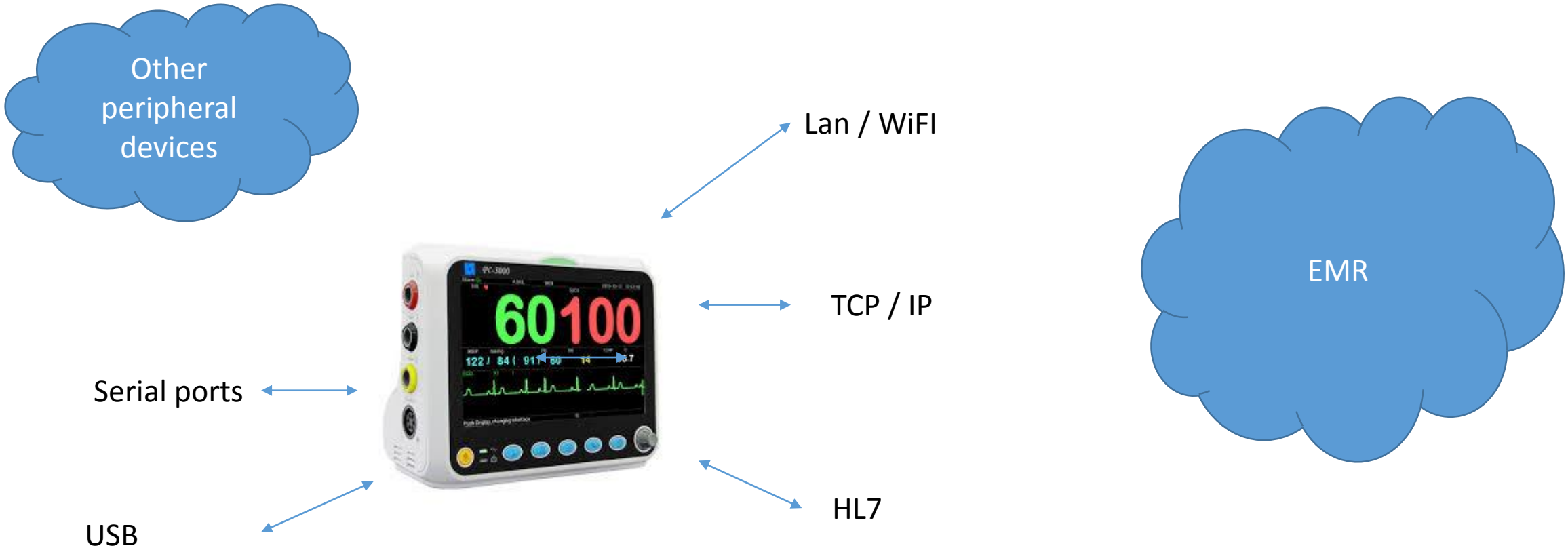


Analyzing a hospital scenario

A typical hospital scenario



A typical patient monitor



Diving into medical devices

- They have an OS (sometimes ☺)
- They have connectivity (Fuzzers ;))
- They do have logical errors
- Protocols
- Compare the low end devices to IOT infrastructure
- Can crash / misbehave
- Known to have APT’s discovered in them

Trapx discovered a APT recently – google

Potential entry points

- Wifi / Lan
- Serial ports
- USB - Firmware
- The sensors
- Keyboard / mouse
- Firewire
- Protocols

Challenges with these devices

- Patching
- Servicing
- Uptime
- Cost
- Longevity

Technical issues observed on the ground

- Lack of encryption between the devices
- Lack of skilled personnel

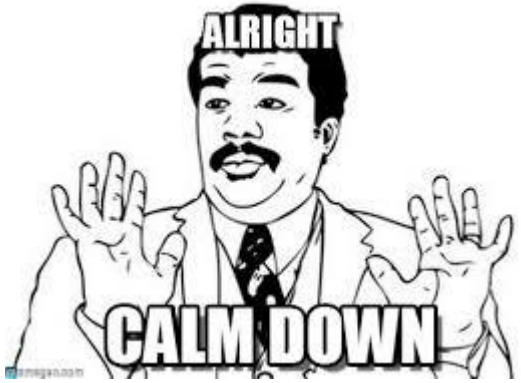
From a manufacturer perspective

- Support – 10 years and counting!
- How do you define a device to be vulnerable?
- Security – a joint exercise between hospitals and the vendors

From a hospital perspective

- If it works – its all good
- Cybersecurity needs more investment and skilled individuals
- Vendors should take care of all security issues
- “why will someone attack a hospital computer – go hack NASA”
- “we are doctors, not cyber warriors”

Hospitals need to understand



- Cybersecurity != more money

BUT Cybersecurity == better functioning

- Risks of a cyber attack
- Patching is a problem, but absolutely worth it
- Having IDS / IPS
- Say no to outdated infrastructure (this is changing rapidly ☺)

Securing these devices

- Having a policy in place – cybersecurity policy anyone ?
- DO NOT CONNECT THESE DEVICES TO THE INTERNET unless intended
- Make sure the systems are patched
- Know your hospital (public and private networks anyone?)

Policies / agencies in place

- FDA
- HIPAA

WHAT IS THE PENALTY FOR A HIPAA VIOLATION?

BY MORGAN BROWN • JANUARY 9 2014

HIPAA violations are expensive. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time.

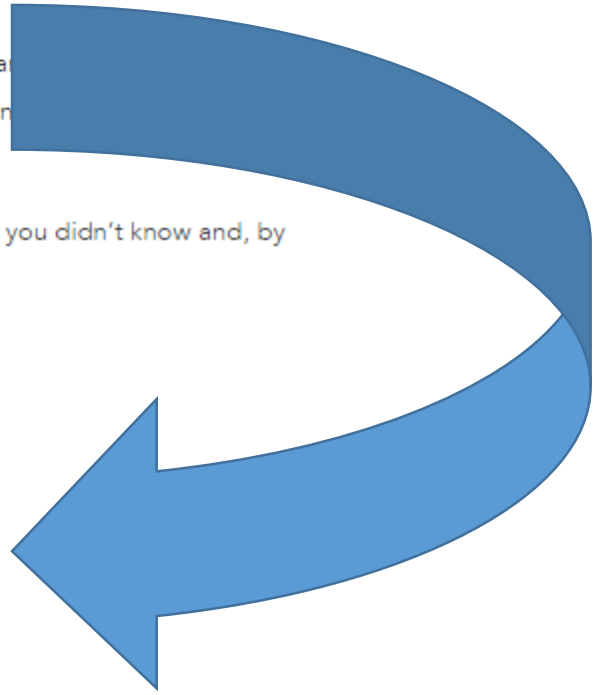
Fines will increase with the number of patients and the amount of neglect. Starting with a breach where you didn't know and, by

WHAT IS THE PENALTY FOR A HIPAA VIOLATION?

BY MORGAN BROWN • JANUARY 9 2014

HIPAA violations are expensive. The penalties for noncompliance are based on the level of negligence a
$50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an
Violations can also carry criminal charges that can result in jail time.

Fines will increase with the number of patients and the amount of neglect. Starting with a breach where you didn't know and, by



$100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for violations of an identical provision

My opinion

- We need better regulations - now!
- Awareness
- A working group towards security (lets take things global too)
- More research on the APT and exploits

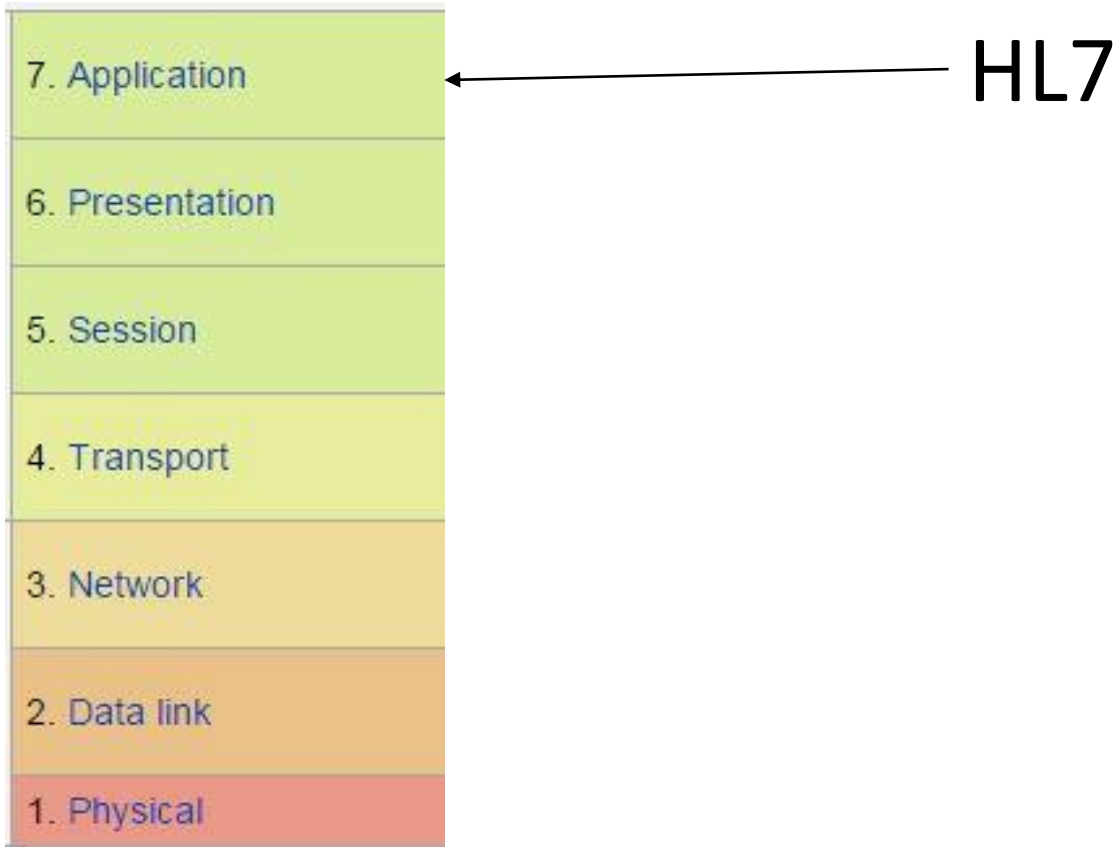
What is HL7?

- Healthcare level standards
- Most popular in healthcare devices (HL7 2.x)
- Quite old – designed in 1989
- FHIR is the next gen

HL7 2.x

- Most popular HL7 version
- New messages / fields added

HL7 (only for v2 messaging and CDA)



Things to know

- MSH – message header segment defines the delimiters

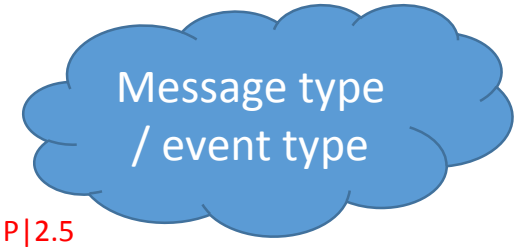
e.g. MSH|^~\&

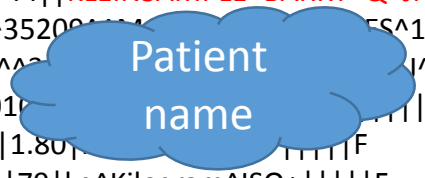
- The primary delimiter is | and sub delimiters in the order they are present after |
- The standards define the message structure – not the implementation

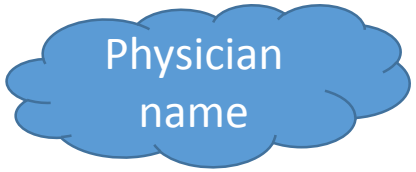
An HL7 message

MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTT
ER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTT
ER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A







MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
[illegible]2445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
[illegible]INGHAM^AL^352[illegible]ES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O|||||||0105I30001^^^99DEF^AN
[illegible]89^1^UABH^^^^[illegible]^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTT
[illegible]SHERMAN^T^^^MD^001[illegible]||||||||||||200605290900
OBX|1|NM|^Body Height||1.80[illegible]|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||67890^GRAINGER^LUCY^X^^^MD^0010^UAMC^L|MED|||||A0||13579^POTT
ER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||79|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

Potential Entry Point

MSH|^~\&|MegaReg|XYZHospC|SuperOE|XYZImgCtr|20060529090131-0500||ADT^A01^ADT_A01|01052901|P|2.5
EVN||200605290901||||200605290900
PID|||56782445^^^UAReg^PI||KLEINSAMPLE^BARRY^Q^JR||19620910|M||2028-9^^HL70005^RA99113^^XYZ|260 GOODWIN CREST
DRIVE^^BIRMINGHAM^AL^35209^^M~NICKELL'S PICKLES^10000 W 100TH AVE^BIRMINGHAM^AL^35200^^O||||||0105I30001^^^99DEF^AN
PV1||I|W^389^1^UABH^^^^3||||12345^MORGAN^REX^J^^^MD^0010^UAMC^L||or my evil script
|MED|||||A0||13579^POTTER^SHERMAN^T^^^MD^0010^UAMC^L|||||||||||||||||||||||||200605290900
OBX|1|NM|^Body Height||1.80|m^Meter^ISO+|||||F
OBX|2|NM|^Body Weight||7999999999999999999999999999999999999999999|kg^Kilogram^ISO+|||||F
AL1|1||^ASPIRIN
DG1|1||786.50^CHEST PAIN, UNSPECIFIED^I9|||A

Time for a demo ☺

Questions

Thank you!

- Minatee Mishra
- Ben Kokx
- Christopher Melo
- Sanjog Panda
- Ajay Pratap Singh
- Geethu Aravind
- Michael Mc Neil
- Shashank Shekhar
- Madhu
- Jiggyasu Sharma
- Pardhiv Reddy
- My uptown friends ;)