RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HTA-R02**

Code Blue! Medical Devices Under Attack

Douglas McKee
Principal Engineer
Dir. Vulnerability Research
Trellix Threat Labs
@fulmetalpackets

Philippe Laulheret
Sr. Security Researcher
Trellix Threat Labs
@phlaul

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Trellix conducts research in accordance with our public Vulnerability Reasonable Disclosure Policy https://www.trellix.com/en-us/threat-center/advanced-threat-research/disclosure.html. Trellix is not responsible in anyway for the third party-products discussed. The information contained in this document is for informational purposes only, does not constitute legal advice, and should not be deemed an offer by Trellix, create obligations for Trellix, or create expectations of future releases. Trellix reserves the right to modify, discontinue, add or subtract features or functionality to its existing products and planned future releases at any time at its sole discretion.

Who Are We?

Douglas McKee

@fulmetalpackets

Philippe Laulheret

@phLaul

Today's Connected Medical Space

500K

MEDICAL TECHNOLOGIES AVAILABLE IN THE MARKET PLACE (DELOITTE)

15M

IOMT DEVICES OPERATING IN US HOSPITALS (ZINGBOX)

10B

IOMT DEVICES CONNECTED WORLDWIDE (IOT-NOW)

50B

IOMT DEVICES CONNECTED BY 2028 (DELOITTE)

Agenda

- What's happening now?
  - Attacks in Healthcare
- What's being overlooked?
  - Medical Research Case studies
- What's the next threat?
  - A vulnerability's lifespan
- How can we be ready?
  - Common pitfalls and mitigations
- What can we learn outside of healthcare?
  - Suggested industry wide improvements

RSAConference2022

Attacks in Healthcare

Underground Market

B

[SELL] Hospital DB with logins + ~ 350 SSN + DOB + DL + Medicare + etc scanned documents

Author: Brady , August 28in [Miscellaneous] - everything else

Create a topic

Brady
byte

B

User
0
14 posts
Registration
date 13.11.2011 (ID: 40682)
Activities
other

Posted by: August 28

Straight from the hospitals server.

MEDICARE ELIGIBILITY LOGIN - [redacted]
RingCentral login with hospitals phone number
sFax login
Fedex login
And some more logins, emails, hospitals cc info, etc.

Profiles containing full name, address, ssn, dob, medicare, etc. Most has DL scans low quality and more ids.
120x profiles from 2021
85x 2020
85x 2019
60x 2018

PM with offers. This forums escrow service is welcome.

C

buying medical fullz / buying medical fullz

Author: canard , May 3in [Miscellaneous] - everything else

canard
byte

C

Paid registration
0
3 publications
Registration
02.03.2021 (ID: 114649)
Hacking activities

Posted by: May 3

budget ~ 5k, more available for good work.
usa + canada only.
volume / complete bases only.
sell in one hand only.
xmr only.
if you don't have reputation we split cost of guarantor.
first contact pm only.

[redacted]

Conti's Perspective


```
"ts": "2020-10-26T02:50:59.589124",
"from": "target@q3mcco35auwcstmt.onion",
"to": "troy@q3mcco35auwcstmt.onion",
"body": "f[redacted] clinics in the usa this week"
```


CONTI MANAGER "TARGET" DIRECTED HIS IRE TOWARD U.S. CLINICS IN OCTOBER 2020, JUST BEFORE LAUNCHING A RANSOMWARE ATTACK ON MORE THAN 400 HOSPITALS. THE GROUP GENERATED AN EYE-POPPING $180 MILLION IN REVENUE LAST YEAR, ACCORDING TO THE LATEST CRYPTO CRIME REPORT PUBLISHED BY VIRTUAL CURRENCY TRACKING FIRM CHAINALYSIS.

https://therecord.media/conti-leaks-the-panama-papers-of-ransomware

Ransomware in the Medical Industry

$61M

RANSOMS PAID
21-MONTHS TIMESPAN
(FBI)

>850

ATTACKS ON HOSPITALS
JAN-SEPT 21
(NBC)

TOP 3

TARGETED SECTOR
Q3 2021
(COVEWARE)

HIGHEST

COST OF BREACH
11 CONSECUTIVE YEARS
(IBM)

Springhill Medical Center

July 16th, 2019

"Tasks that were previously automated, such as recording vital signs, were suddenly arduous and unfamiliar, particularly for younger nursing staff who had never worked without modern technology, according to two workers at the time."

—The Wall Street Journal

https://en.wikipedia.org/wiki/Springhill_Medical_Center#/media/File:Springhill_Medical_Center_2018.jpg

University of Vermont Medical Center

October 28th, 2020

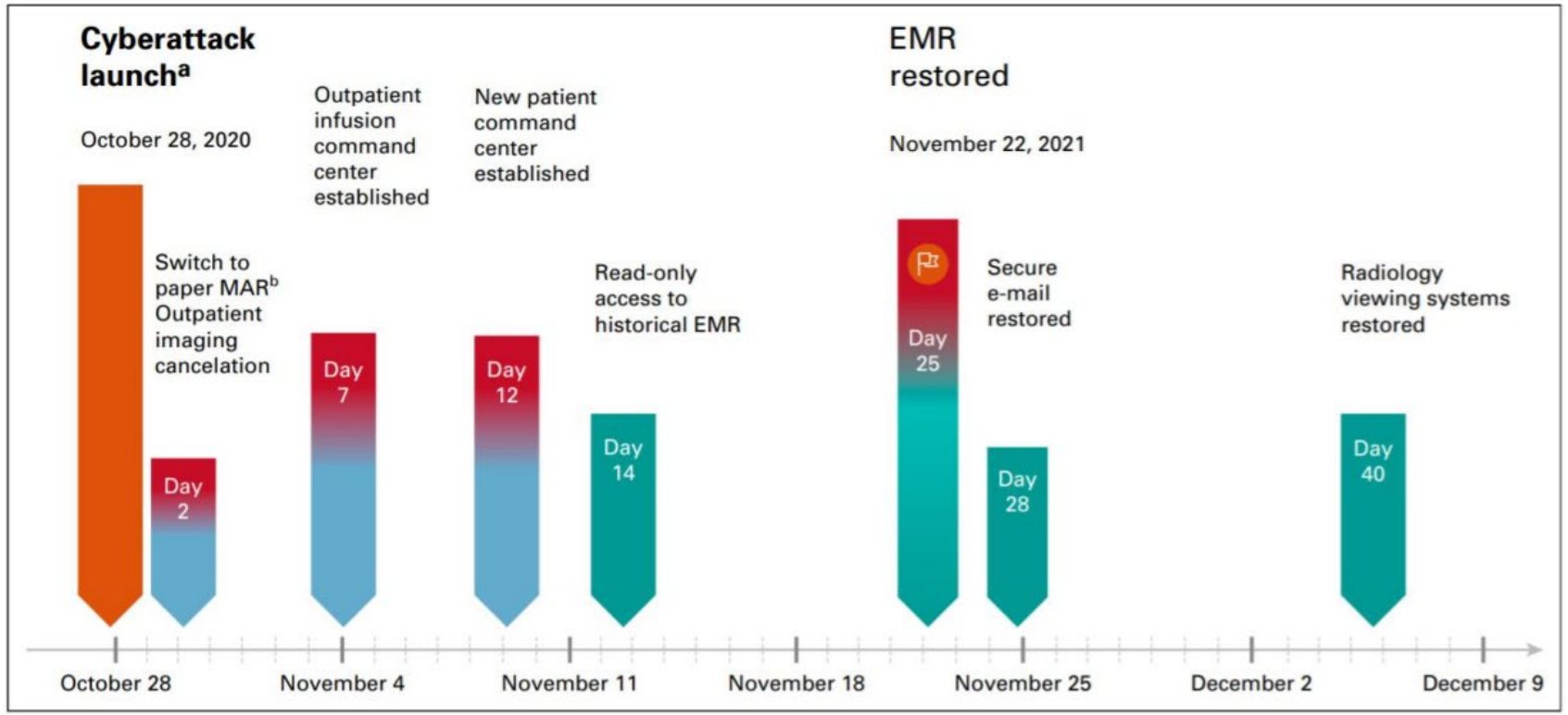
"To look someone in the eye, and tell them they cannot have their life-extending or lifesaving treatment, it was horrible, and totally heart-wrenching"

—Colleen Cargill, Nurse

https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html

University of Vermont Medical Center

October 28th, 2020



Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect
https://ascopubs.org/doi/pdf/10.1200/OP.21.00116

Ransomware Impact on Healthcare

- Difficulties to communicate about the on-going attack:
  - For the staff: mental toll, miscalculation of risk
  - For the patients: risks aren't c
  - For the institution: failing to
- Going back to pre-computerization process during the attack:
  - Junior staff unaware of the old ways
  - Loss of redundancy, safety nets & the recent advances in computerization
  - Increased risk of harm, death.
- Weeks to months to recover from the attack.

Industry Perspective

Disruption of communication was at the heart of the damage induced by the cyberattack and highlighted the multiple nonredundant ways used by physicians and staff to provide high-level multidisciplinary cancer care.

[T]he immediate need for updated standardized processes to address the host of challenges that we faced with loss of EMR and communication systems and the realization that IT cannot be our only solution in the face of a cyberattack.

Cancer Care in the Wake of a Cyberattack: How to Prepare and What to Expect (JCO Oncology Practice)
https://ascopubs.org/doi/pdf/10.1200/OP.21.00116

Other Threats

- How to Hack Medical Imaging Applications via DICOM (2020)
- CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning (Jan 2019)
- Orangeworm (2015 - 2018?)
- Triple Extortion (e.g., Vastaamo clinic attack (2020))

The Need of Planning against Future Threats

- Cyber security is working on preventing Ransomware attacks…
- … but threat actors will try to stay a step ahead.
- Non-standard solutions might become their next target:
  - Custom protocols
  - Embedded devices difficult to integrate to an EDR/XDR ecosystem
  - Legacy systems
- Highlight & address threats now to stop attackers in their track!

RSAConference2022

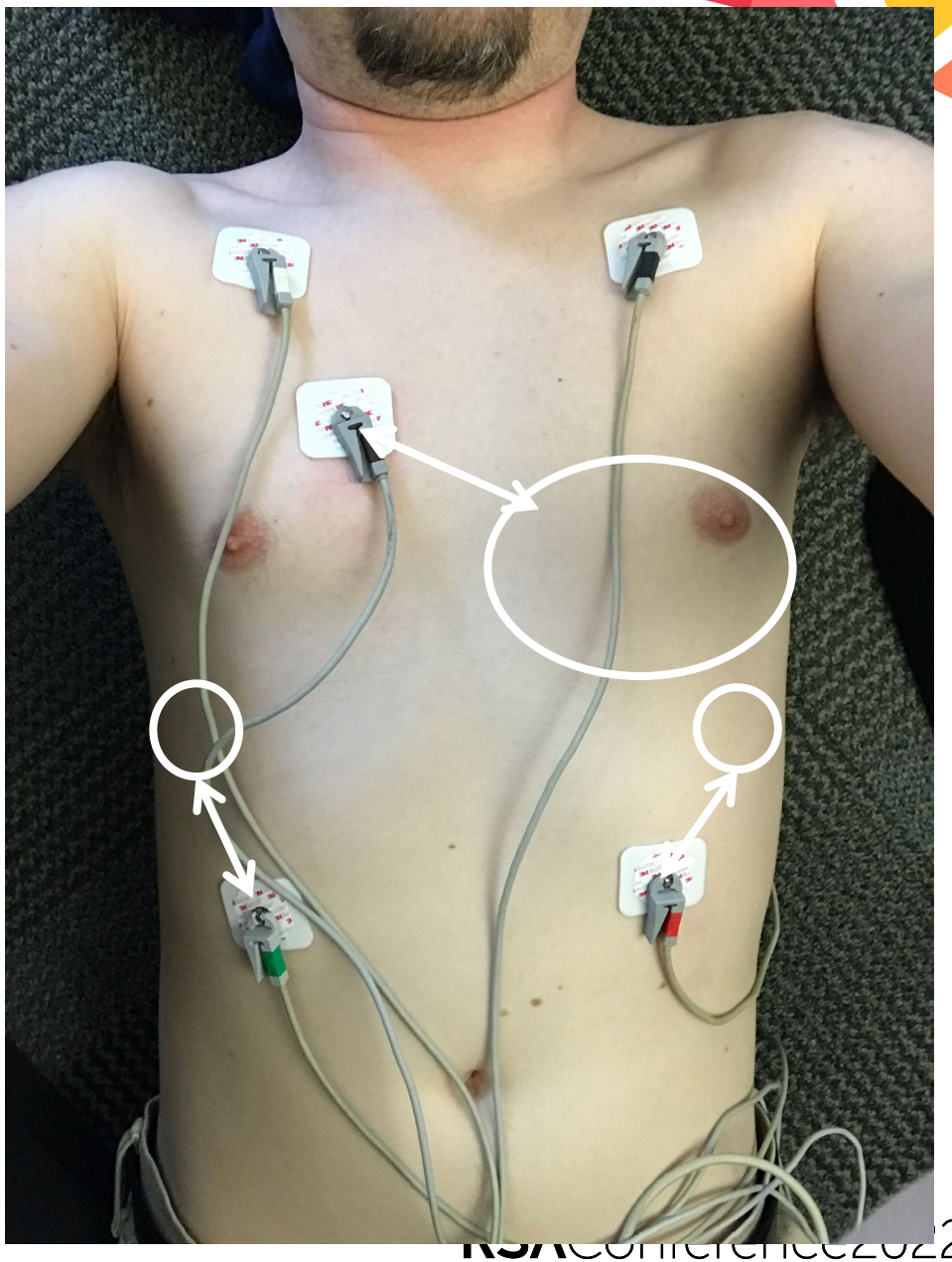
Medical Case Studies

Hacking a Patient Vitals

GE Dash 3000 Patient Monitor

- Bedside monitor
- Monitors patient's vitals – Heartrate, Blood pressure, O2 levels, etc
- Has wired and wireless (optional) networking
- Contains Personal Identifiable Information (PII)
- Sends data to a central monitoring station

Testing Setup



Improved Testing setup

ECG Simulator

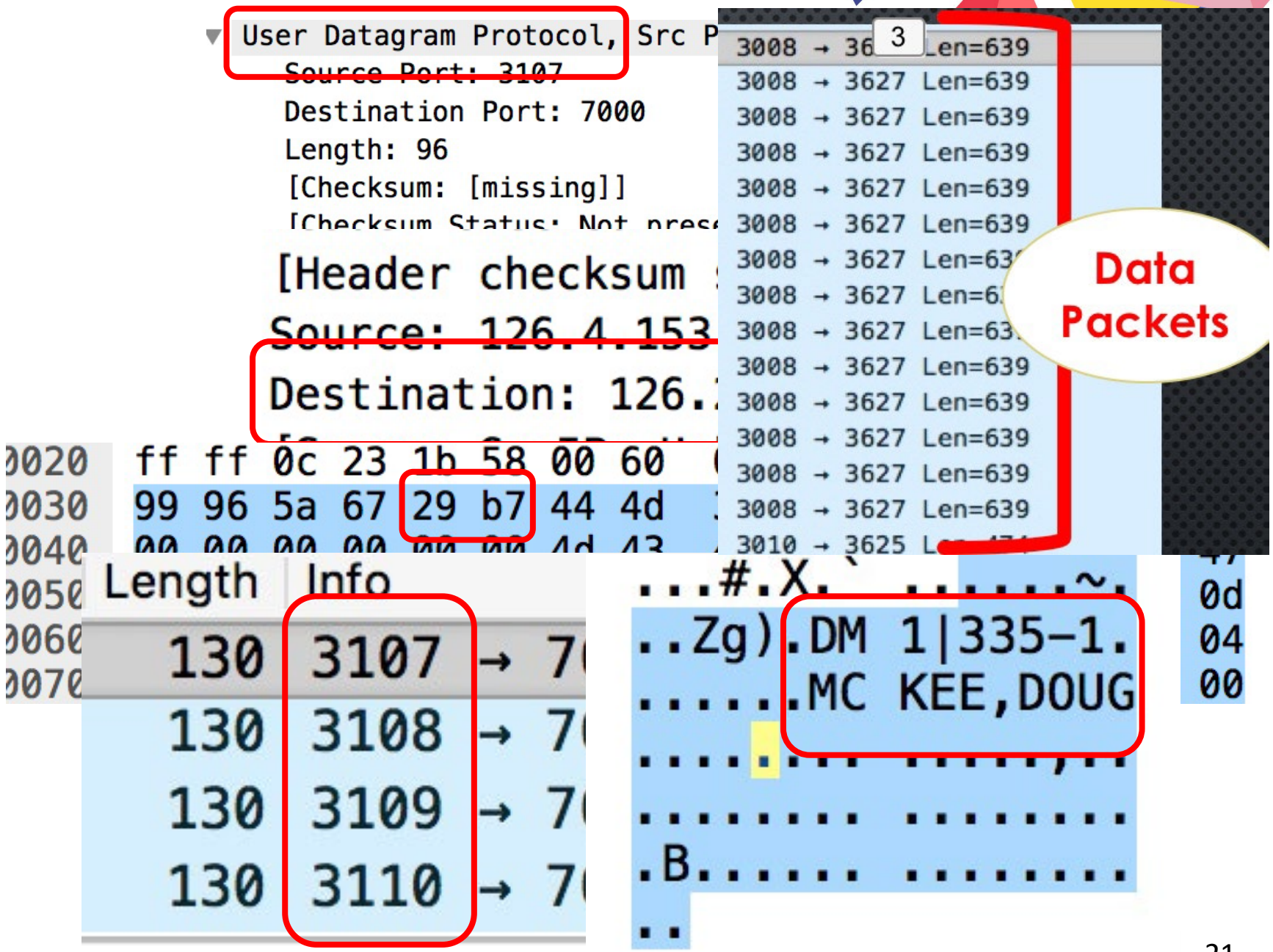
GE Dash 3000

RWHAT Protocol

Central Monitoring

Observations

- UDP Packets
- Broadcast address
- Counters
- Incrementing Ports
- Unencrypted
- Identifiable Data



Demo Video

Impact scenario

- Power of misinformation
- Smaller changes, larger impact
- Unconscious patient
- Reliance on technology
- Inside Job?

"Fictitious cardiac rhythms, even intermittent, could lead to extended hospitalization, additional testing, and side effects from medications to control heart rhythm and/or prevent clots. The hospital could also suffer resource consumption."

—Dr. Shaun Nordeck

Arrhythmia Management Guidelines

Amer. Heart assoc. & Amer. College of cardiology

Fictitious intermittent cardiac rhythms

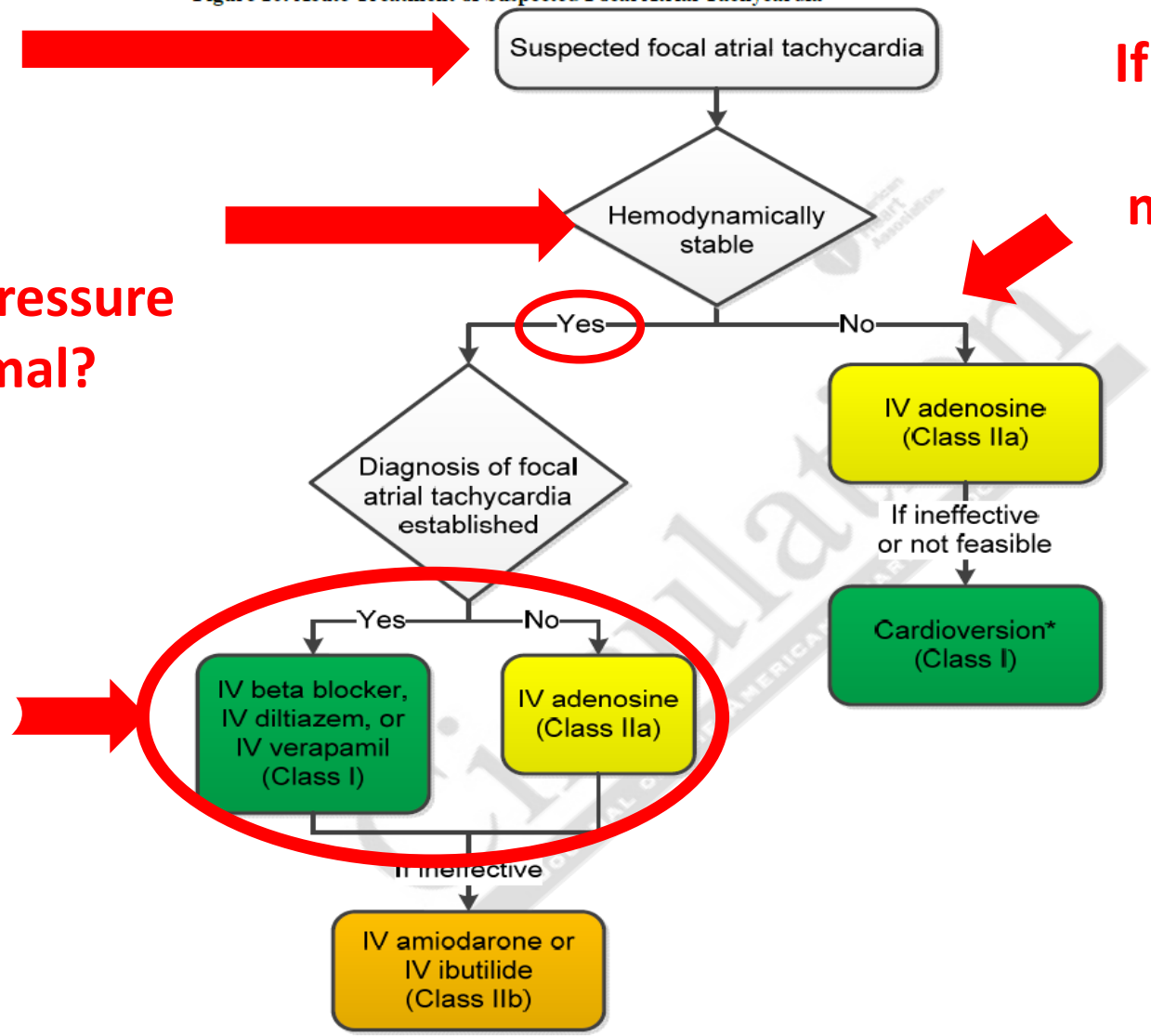
Blood Pressure Normal?

Medications Administered

If monitor was modified

Page RL, et al.
2015 ACC/AHA/HRS SVT Guideline

Figure 10. Acute Treatment of Suspected Focal Atrial Tachycardia



It’s critical to understand ALL traffic

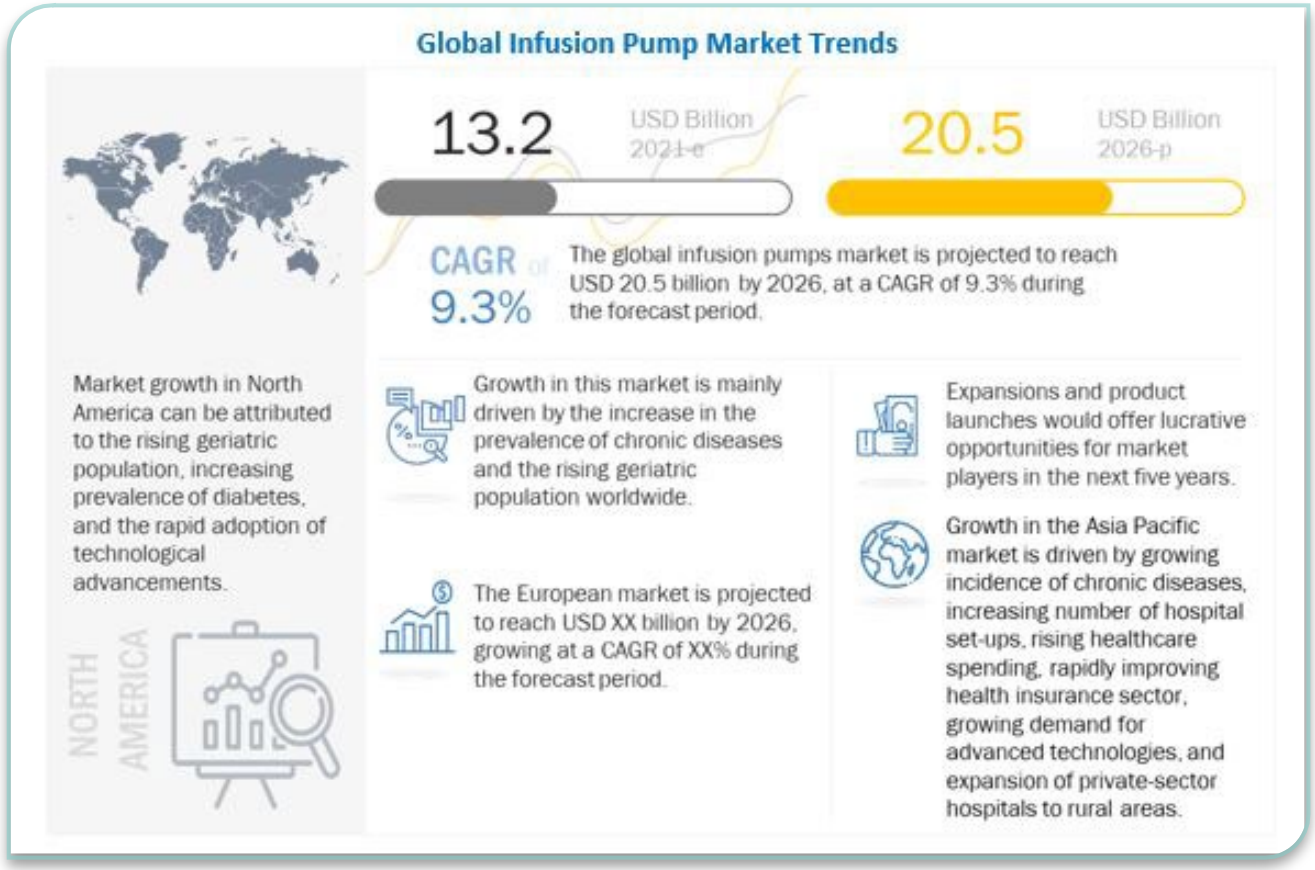
RSAConference2022

Medical Case Studies

Overmedicated: Hacking an Infusion Pump

Strategic context

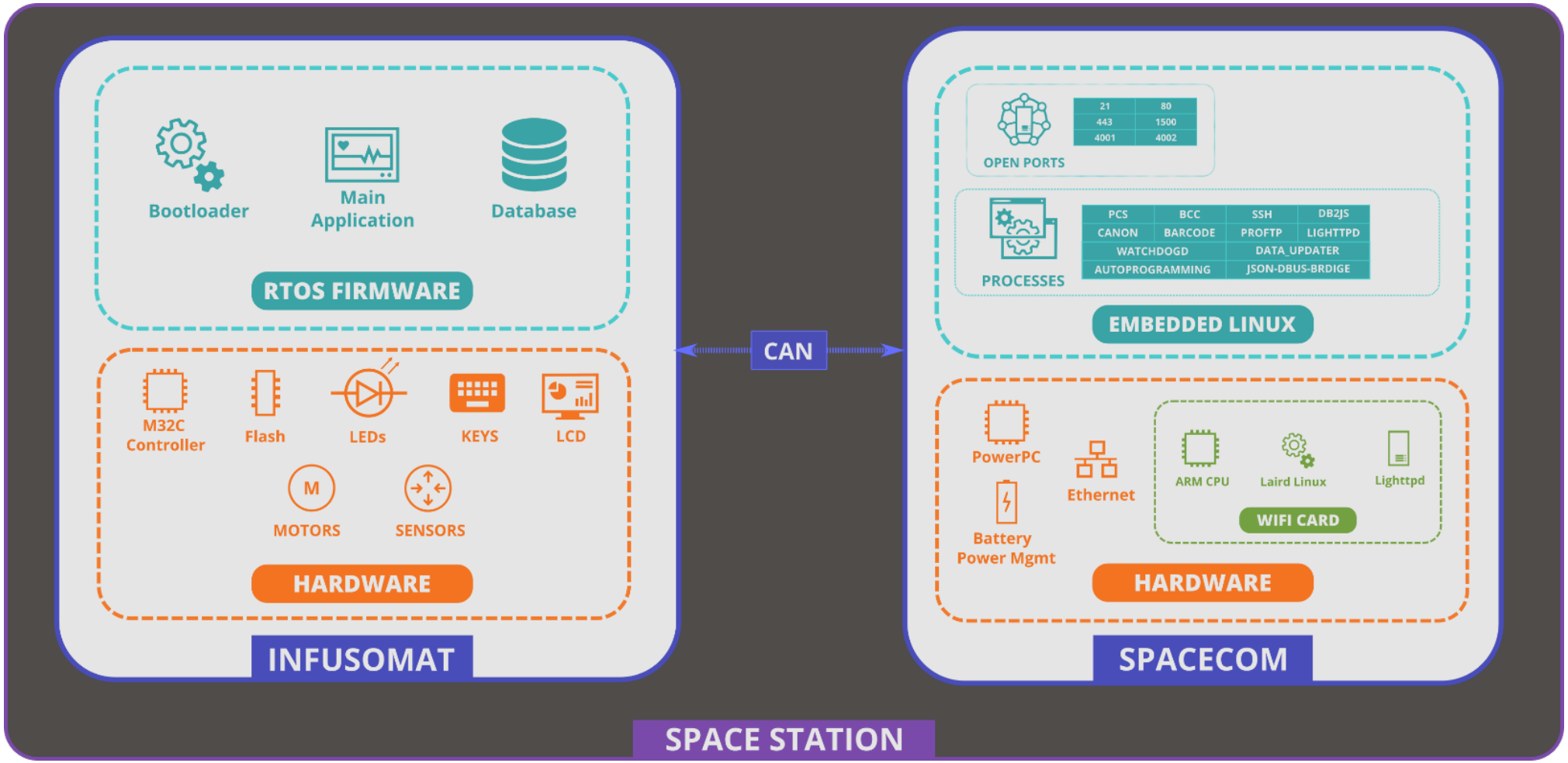
- Infusion market
  - 200M IV infusion per year
  - $13.2B US sales in 2020
  - $54B in sales worldwide



Target Device

- B. Braun Infusomat Large Volume Pump
- SpaceStation with SpaceCom
- Released in 2017

System Architecture



[bridge_request] Fix sending json containing percent characters

Browse files

master

v1.1.6 v1.1.5 v1.1.4

elrafoon committed on Mar 19, 2015 — 1 parent 569cb01 — commit 79ff62e918b182eca783944b0fbb74b6299f489b

Showing 1 changed file with 6 additions and 6 deletions.

Unified | Split

12 src/bridge_request.c

```
@@ -70,11 +70,11 @@ int bridge_request_getinput(bridge_request_t *self, char **data)
70 70                return EINVAL;
71 71
72 72        if ((buffer = malloc((size_t)len+1)) == 0) {
73    -               FCGX_FPrintF(self->request.err, "out of memory!");
   73 +               FCGX_PutS("out of memory!", self->request.err);
74 74                return ENOMEM;
75 75        }
76 76        if (FCGX_GetStr(buffer, len, self->request.in) != len) {
77    -               FCGX_FPrintF(self->request.err, "Got less data than expected.");
   77 +               FCGX_PutS("Got less data than expected.", self->request.err);
78 78                return EINVAL;
79 79        }
80 80        buffer[len] = '\0';
@@ -84,14 +84,14 @@ int bridge_request_getinput(bridge_request_t *self, char **data)
84 84
85 85  void bridge_request_transmit(bridge_request_t *self, struct json_object *obj)
86 86  {
87    -       FCGX_FPrintF(self->request.out, "Content-type: application/json\r\n\r\n");
88    -       FCGX_FPrintF(self->request.out, json_object_to_json_string(obj));
   87 +       FCGX_PutS("Content-type: application/json\r\n\r\n", self->request.out);
```

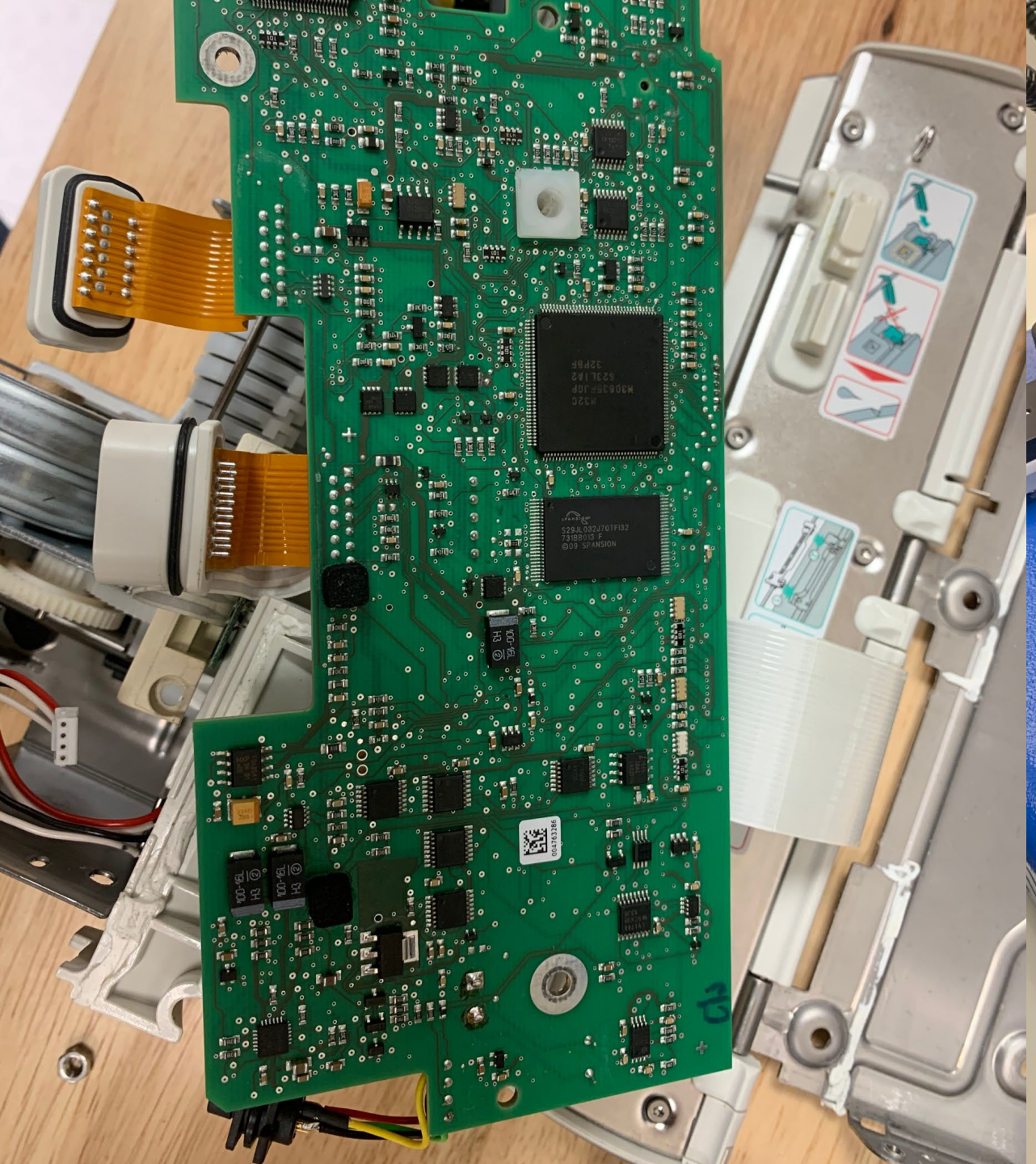
Format string exploitation

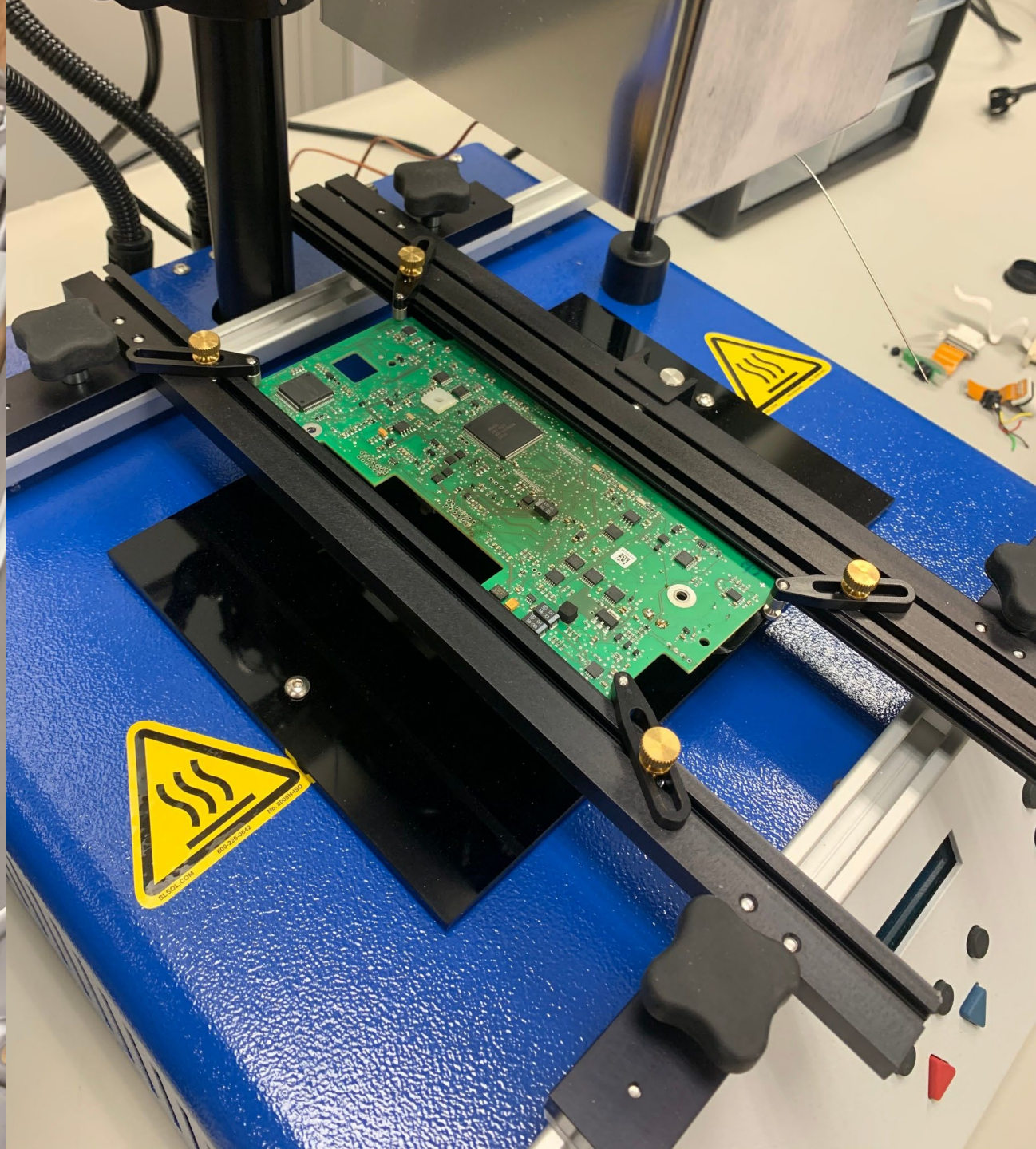
```
#Testing Format String Vuln with multiple %x
┌─[Hacker@Hackers-MacBook-Pro:~/D/b/g/sbin]
└─>$ curl --header "Content-Type: application/json" --header "Expect:" -d "
{\"service\":\"org.freedesktop.DBus|/org/freedesktop/DBus\",\"method\":\"org.freedesktop.DBus.StartServiceByName\",\
"id\":0,\"params\":[\"su\",\"%x%x%x\",0]}" http://192.168.7.120/rpc
{ "id": 0, "error": { "origin": 1, "code": 1, "message": "The name 1fa901d6a018a88 was not provided by any .service
files" }, "result": null }⏎
```

… a couple of CVEs later …

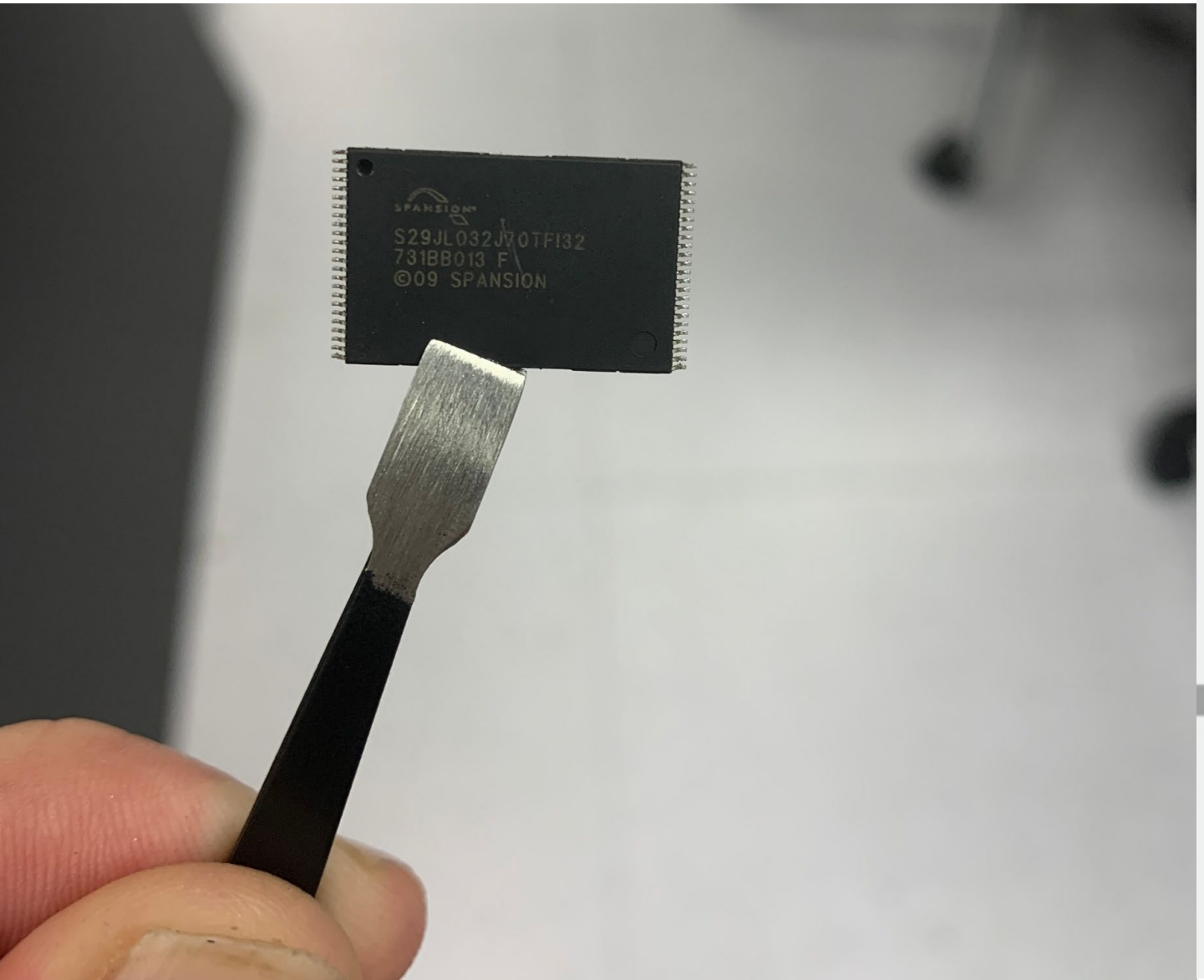
We got Root! Are we done yet?

- Previous reports:
  “root access cannot cause patient harm”
  …can’t it?
- How do we control the pump’s critical OS having root access on SpaceCom?


S29JL032J70TFI32
731BB013 F
©09 SPANSION



GETTING THE FIRMWARE OUT




```
      0001 0203 0405 0607 0809 0A0B 0C0D 0E0F  01234 6789ABCDEF
00000 0000 0001 DC00 FFFF 0000 0000 0000 8D02  ....Ü.ÿÿ..... .
00010 300B E40B 0900 CA00 6D02 3A0B 260B 0900  0.ä...Ê.m.:.&...
00020 8001 1002 440B 300B 0900 1002 8001 4E0B   ...D.0..... .N.
00030 3A0B 0901 6D02 CA00 580B 440B 0900 8D02  :...m.Ê.X.D... .
00040 0000 620B 4E0B 0500 6D02 CA00 6C0B 580B  ..b.N...m.Ê.l.X.
00050 0500 1002 8001 760B 620B 0500 8001 1002  .... .v.b... ...
00060 800B 6C0B 0501 CA00 6D02 8A0B 760B 0500   .l...Ê.m. .v...
00070 0000 8D02 940B 800B 0600 CA00 6D02 9E0B  .. . . ...Ê.m. .
00080 8A0B 0600 8001 1002 A80B 940B 0600 1002   ... ...¨. .....
00090 8001 B20B 9E0B 0601 6D02 CA00 BC0B A80B   .². ...m.Ê.¼.¨.
000A0 0600 8D02 0000 C60B B20B 0A00 6D02 CA00  .. ...Æ.²...m.Ê.
000B0 D00B BC0B 0A00 1002 8001 DA0B C60B 0A00  Ð.¼..... .Ú.Æ...
000C0 8001 1002 E40B D00B 0A01 CA00 6D02 260B   ...ä.Ð...Ê.m.&.
000D0 DA0B 0A00 ED85 0000 9B80 0000 B177 0000  Ú...í ..  ..±w..
000E0 CD69 0000 375B 0000 BA4D 0000 1A42 0000  Íi..7[..ºM...B..
000F0 3238 0000 6D30 0000 322A 0000 0A25 0000  28..m0..2*...%..
00100 DA20 0000 721D 0000 A91A 0000 5F18 0000  Ú ..r...©..._...
00110 7C16 0000 EF14 0000 A713 0000 9A12 0000  |...ï...§... ...
00120 BF11 0000 1011 0000 8710 0000 2010 0000  ¿....... ... ...
00130 D80F 0000 AD0F 0000 A00F 0000 260B 0000  Ø...-... ...&...
00140 0000 000A 0100 0001 2802 E001 E001 3002  ........(.à.à.0.
00150 00FF 9EFF 0020 2020 2020 2020 2020 2828  .ÿ ÿ.          ((
00160 2828 2820 2020 2020 2020 2020 2020 2020  (((
00170 2020 2020 2088 1010 1010 1010 1010 1010           ..........
00180 1010 1010 1004 0404 0404 0404 0404 0410  ................
00190 1010 1010 1010 4141 4141 4141 0101 0101  ......AAAAAA....
001A0 0101 0101 0101 0101 0101 0101 0101 0101  ................
001B0 1010 1010 1010 4242 4242 4242 0202 0202  ......BBBBBB....
001C0 0202 0202 0202 0202 0202 0202 0202 0202  ................
001D0 1010 1010 2030 3132 3334 3536 3738 3941  .... 0123456789A
001E0 4243 4445 4600 286E 756C 6C20 706F 696E  BCDEF.(null poin
001F0 7465 7229 0030 3132 3334 3536 3738 3961  ter).0123456789a
00200 6263 6465 6600 3F3F 3F00 00FF 0220 E000  bcdef.???..ÿ. à.
00210 0200 0100 0820 E000 0400 0000 0C20 E000  ..... à..... à.
00220 0100 0000 2120 E000 0100 0000 2A20 E000  ....! à.....* à.
00230 0100 0000 3320 E000 0100 0000 3D20 E000  ....3 à.....= à.
00240 0100 0000 3F20 E000 0100 0000 4120 E000  ....? à.....A à.
```

…many months of reversing later…

Critical data

- Tube sizes
  - Bigger → more c
    squeeze
  - Wrong size → pu
    slow/fast
- Can be altered by an attacker from SpaceCom
- May lead to an overdose

```
Example2: Disposable data
[COMMON0]
TUBETABCHKSUM=35443
TUBETABSIZE=3140
DISPDATA_VERSION=506
TUBECRCKUP=63207
TUBETABSIZE_KUP=688
TUBERELEASE_TABCHKSUM=20106
TUBERELEASE_TABSIZE=22
TUBERELEASE_KUP_TABSIZE=22
TUBERELEASE_KUP_TABCRC=18226
TUBE_COUNT=3
[TUBE0]
TUBENAME_A=
TUBE_HEADVOLUME_A=0
//... snipped out since empty section ...
[TUBE1]
TUBENAME_A=Intrafix PVC
TUBE_HEADVOLUME_A=204
TUBE_MAXBOLVOL_A=500
TUBEPRESSURESURFACE_A=1131
TUBE_AIRALARMLEVEL_A=23
TUBE_DRIPCHAMBER_A=20
TUBE_MAXRATE_A=120000
TUBE_MAXBOLRATE_A=120000
TUBECRCFUP_A=41266
```

"Something as routine as correcting a person's high blood sugar or sodium level too quickly can cause the brain to swell or damage the nerves which can lead to permanent disability or even death."

—Dr. Shaun Nordeck

Never trust data from an unverified source!

RSAConference2022

No ransomware, why should I care?

Industry Perspective

"We have an implicit trust in these types of technologies," Tully says. "We don't ever get any cybersecurity training in medical school. It's not something that ever comes up in our literature."

—Dr. Jeff Tully

"The ability to manipulate medical equipment in a way that is potentially harmful to patients, without end-user detection, is effectively weaponizing the device and something only previously conceived by Hollywood yet, Trellix has confirmed it is plausible."

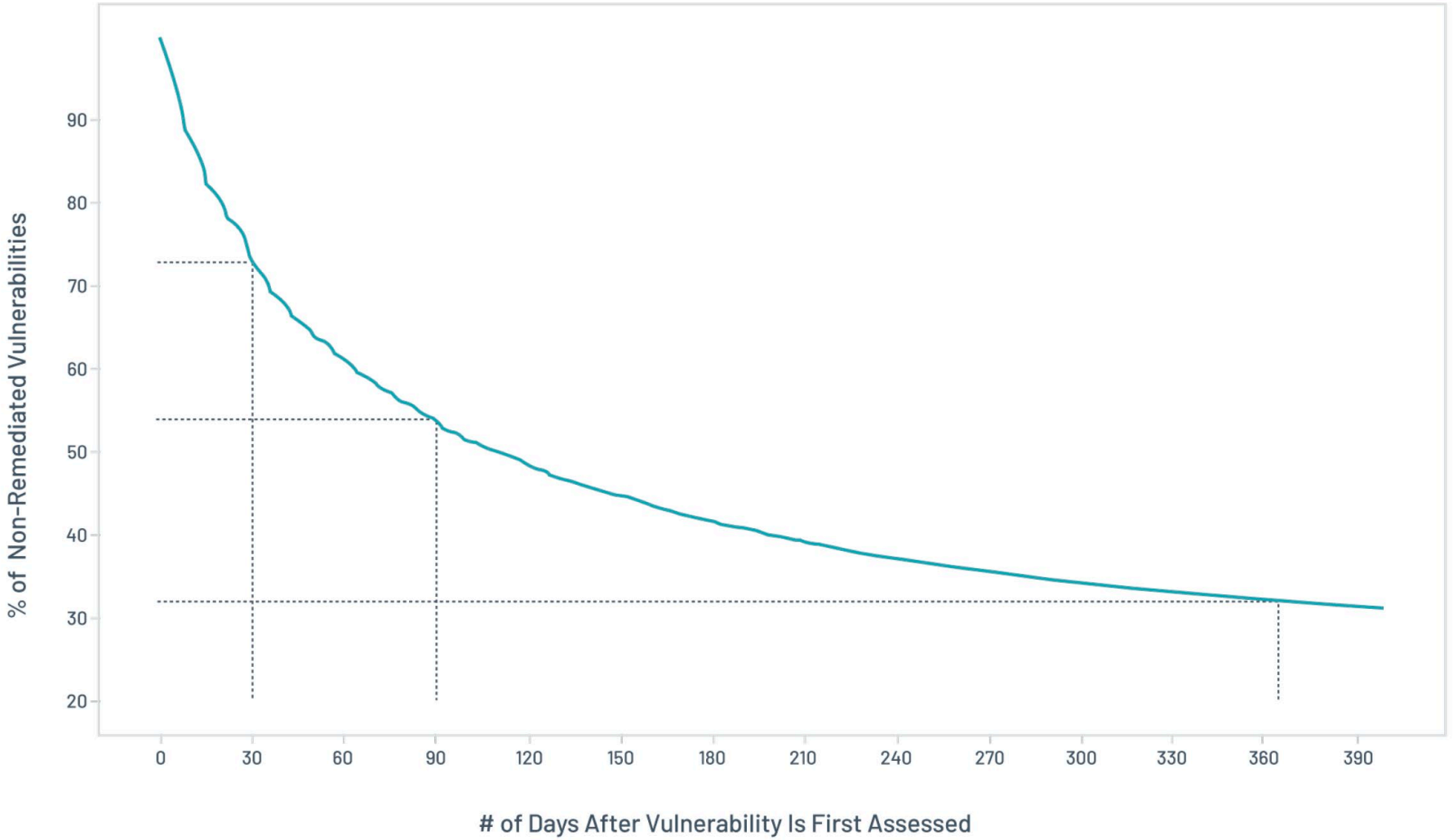
—Dr. Shaun Nordeck

"32% of healthcare leaders admit to never auditing their medical devices."

—Sensato

https://www.hpe.com/us/en/insights/articles/medical-device-security-hacking-prevention-measures-1806.html
https://www.sensato.co/post/will-recent-iot-medical-device-concerns-make-a-change-in-healthcare-in-2020

Vulnerability lifespan in an organization



Source: What Is the Lifespan of a Vulnerability? - Blog | Tenable®

Do they exist?

6.9 yrs

Average lifespan of Zero Day (RAND Corp)

26%

Vulnerabilities found never patched (All industries) (Tenable)

7-10 yrs

Medical device lifecycle (CyberMDX)

2,270

Medical Devices near EOL in use per hospital (CyberMDX)

RSAConference2022

Medical Industry Pitfalls & Solutions

Apply This!

Medical Industry Common Pitfalls

OLDER TECHNOLOGY

EXPENSIVE PATCHING

EXCESSIVE TRUST

How to Overcome these Hurdles? (Medical IoT Vendors)

- Use secure coding practices and modernize existing architecture
  - Authentication
  - Encryption of DaR/DiM
  - Security Audits
- Embrace security researchers providing deep vuln research
- Improve “patchability” of the devices
  - Zero-patch
  - Virtual-patch

How to Overcome these Hurdles? (Medical Organizations)

- Network Segmentation and Monitoring (risk mitigation/minimization)
- Follow vendor and FDA/CISA guidelines
- Maintain constant awareness of potentials threats

What US institutions recommend to Healthcare

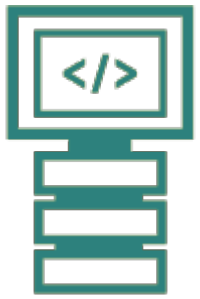
- CISA's ransomware Best Practices
  - Read and follow the advices p18-19
  - https://www.cisa.gov/uscert/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
- FDA recommendations
  - Read the whitepapers/playbooks/guidance that apply to your situation
  - https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity
- Keep a pulse on HC3 Threats briefs
  - https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#threat-briefs

RSAConference2022

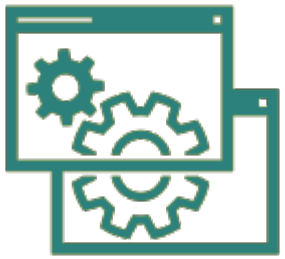
Beyond Healthcare

Apply This!

How Does It Matter Beyond Healthcare?



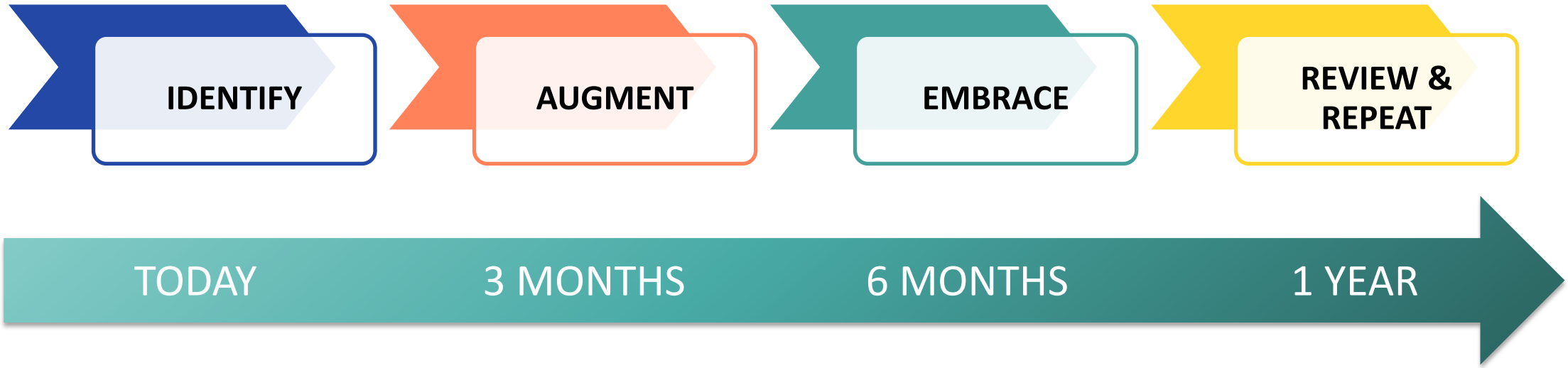
TECH STACK BLINDSPOT



UNITENDED FEATURES

CUSTOMER IMPACT

Actionable Items for You!



Actionable Items for You!

- **Identify** key shareholders in your organization responsible for mitigation & recovery plan
- **Augment** this plan with an analysis of potential blind spots within legacy systems.
- **Embrace** offensive security testing in all forms
- **Review** and feed results to the shareholders and act upon it.
- **Rinse &Repeat**

Summary

- Ransomware can hit hard if you're not ready…
- …and less obvious vectors can still get you when you are.
- A patch is meaningless if it is too hard/costly for your customers to deploy.
- E M E R G E N T P R O P E R T I E S
- Think RED / Act BLUE