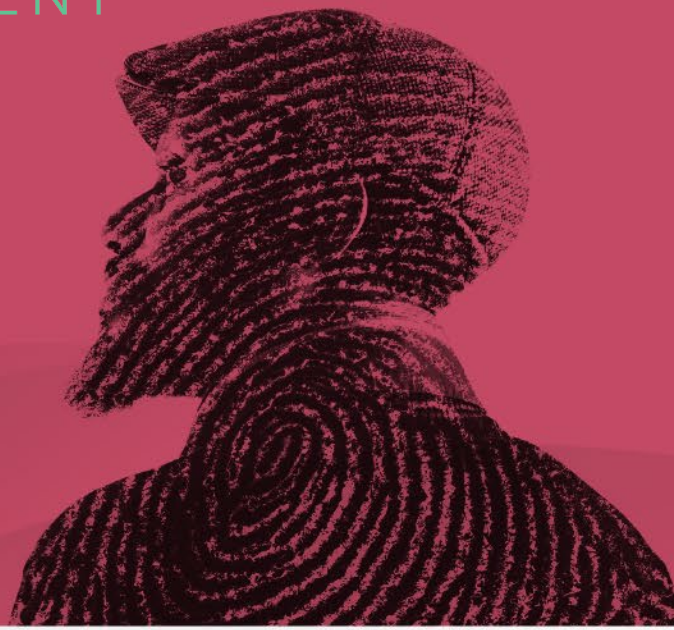
RSAC Sandbox

RSAConference2020

HUMAN ELEMENT



SESSION ID: **SBX1-R10**

What Happens During a Medical Device Attack

Mike Kijewski

CEO
MedCrypt
@mikekijewski

What's a Medical Device?

- Pacemaker
- Surgical Robot
- Vital Sign Monitor

What if a med device is hacked?

RSAC Sandbox

- Patient data can be stolen
- Hospital network compromise
- Device functionality interrupted

What if a med device is hacked?

RSAC Sandbox

- Patient data can be stolen (HIPAA Violation)
- Hospital network compromise (Hospital financial loss)
- Device Functionality interrupted (patient harm)

Attack Vector 1

Bluetooth Low Energy

What would happen?

RSAC Sandbox

- False vitals -> wrong diagnosis
- Interrupted monitoring -> missing critical event
- False vitals -> tainted data analysis algorithm

Apply:

- Don’t rely solely on BLE security
- Don’t rely solely on “proprietary protocol”
- If you’re a manufacturer, consider data integrity checks
- If you’re a hospital, ask if there are data integrity checks

Attack Vector 2

Man in the Middle

What would happen?

- Too much radiation
- Not enough radiation
- Misplaced radiation dose
- Availability disruption -> patient relocation?

Apply:

RSAC Sandbox

- Don’t rely solely on perimeter security
- Don’t rely solely on “Who would do this?”
- If you’re a manufacturer, consider security by design
- If you’re a hospital, ask if the device is secure by design

Other Attack Vectors

Other Attack Vectors

- OS Vulnerability (e.g. XP)
- User Authentication (or lack there of)
- Remote software updates (no verification)

Apply: How to mitigate these vulns during design

RSAC Sandbox

- Unique keys on each device / endpoint
- Encrypt stuff locally
- Sign stuff locally
- Verify signatures on data / commands before acting

MedCrypt: A tool

- Install Guardian library in each application
- Provision keys
- Call API to access functions
- Monitor remotely

MedCrypt: A tool

RSAC Sandbox

```
/* finding channel in system */
medcrypt::Coordinates coordinates = {"MyServiceName", "BaseSession", "MyChannelName"};
medcrypt::ChannelGuard* my_channel;
status = my_guardian->FindChannelGuard(coordinates, my_channel);

/* sending data */
std::string tx_buffer = "my data goes here";
my_channel->DataForChannel(tx_buffer);
my_guardian.Run();

/* receiveing data */
std::string rx_buffer;
my_guardian.Run();
my_channel->DataFromChannel(&rx_buffer);
```

Apply

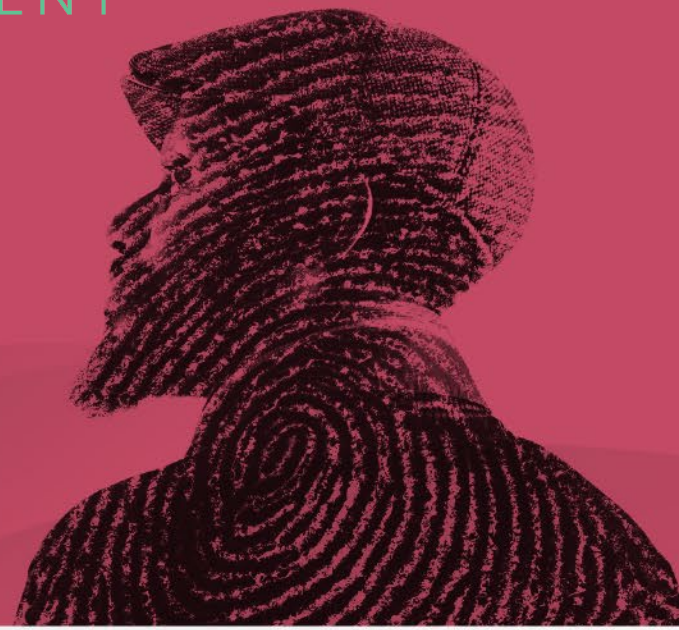
RSAC Sandbox

- If you're a manufacturer, design security features into V0.1
  - FDA: "Encrypt, Sign, Monitor"
- If you're an HDO:
  - Let vendors know security by design is a feature
  - Segment devices from network
  - Patch OS

RSAC Sandbox

RSAConference2020

HUMAN ELEMENT



SESSION ID: **SBX1-R10**

Thank you

Mike Kijewski

CEO
MedCrypt
@mikekijewski