FIPS, IoT Medical Devices and VA/DoD

Allegro

Beyond Certification and Validation

- Focus on reaching Common Criteria Certification and FIPS 140-2 Validation

- After achieving one or both – then what ......

Specific Application – VA and DoD

- IoT / IoMT poised to change the healthcare industry:
  - Allied Market Research – $136.8 Billion by 2021
  - Potential to dramatically affect quality of life

- National VA hospital system represents 150+ Medical Centers and over 1400 Clinics nationwide.

Allegro

IoT / IoMT Trends in Healthcare

- Focus on “value-based” care or ”patient outcomes” is shifting financial incentives:
  - Compensated on how patients fare
  - Not how many tests or procedures they can order

- IoMT and larger IoT ecosystems now enable the ability to track patient progress and outcomes.

- VA and DoD are very interested.

IoT / IoMT Trends in Healthcare

- For IoT / IoMT devices to be viable for VA / DoD market:
  - Device Security
  - FIPS Requirments

- Medical devices and larger healthcare ecosystems (IoMT solutions) that employ FIPS 140-2 encryption meet procurement requirements for Veterans Affairs (VA) and Department of Defense (DoD).

IoT / IoMT Device Security is far more than a single ***PRODUCT*** ….

It is a ***PROCESS*** that is supported by a collection of technologies and products that enforce a security model.

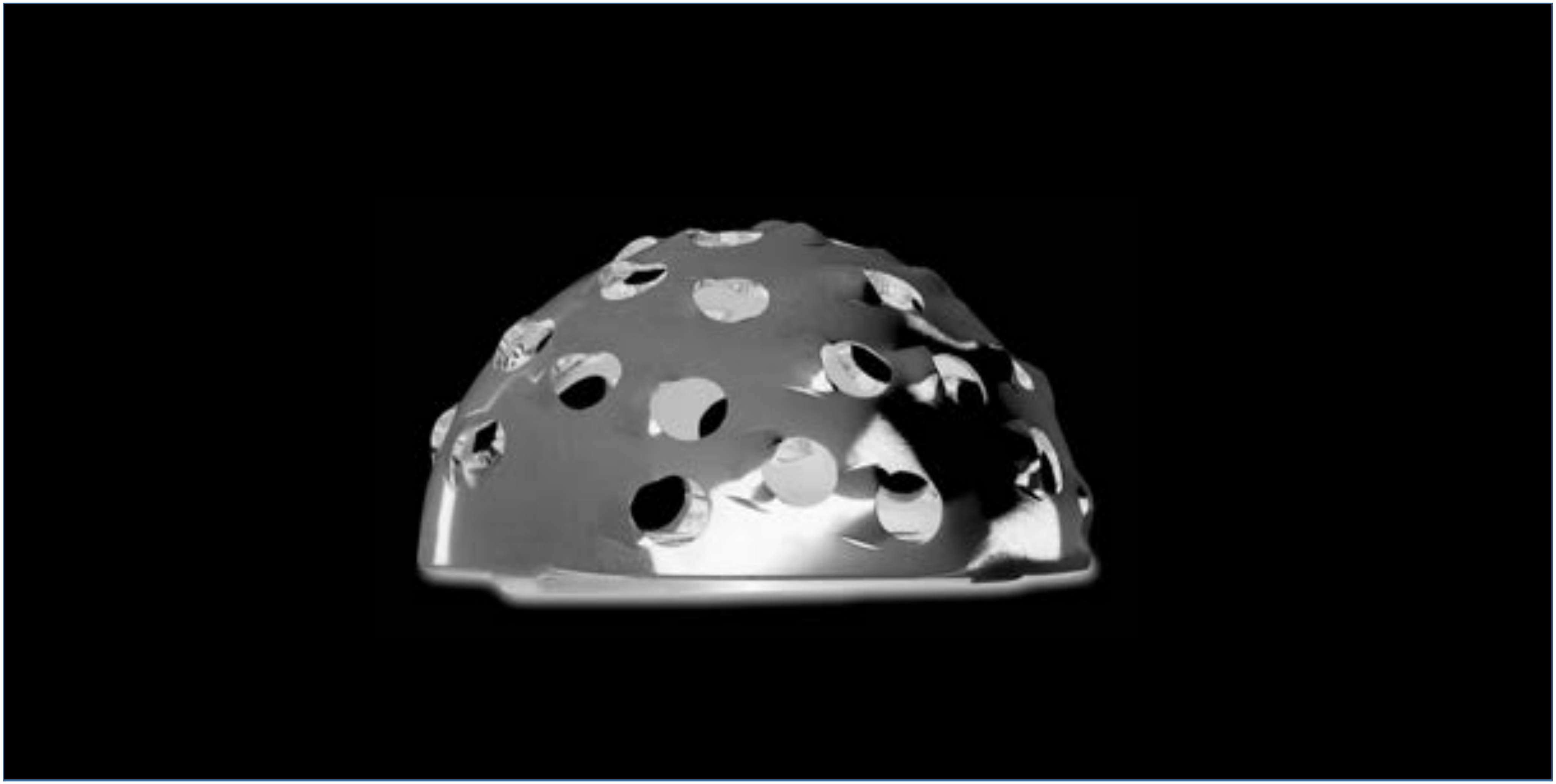
Regulations are largely looking at

”Connected Devices”

rather than the much larger picture ….

Understanding the ***VALUE PROPOSITION*** of IoT/IoMT

and potential data ***SECURITY RISKS***.



IoMT Example

Application – Total Hip Arthroplasty

- Example from:
  - IoT Inc
  - Bruce Sinclair

IoT Inc.

Internet of Things

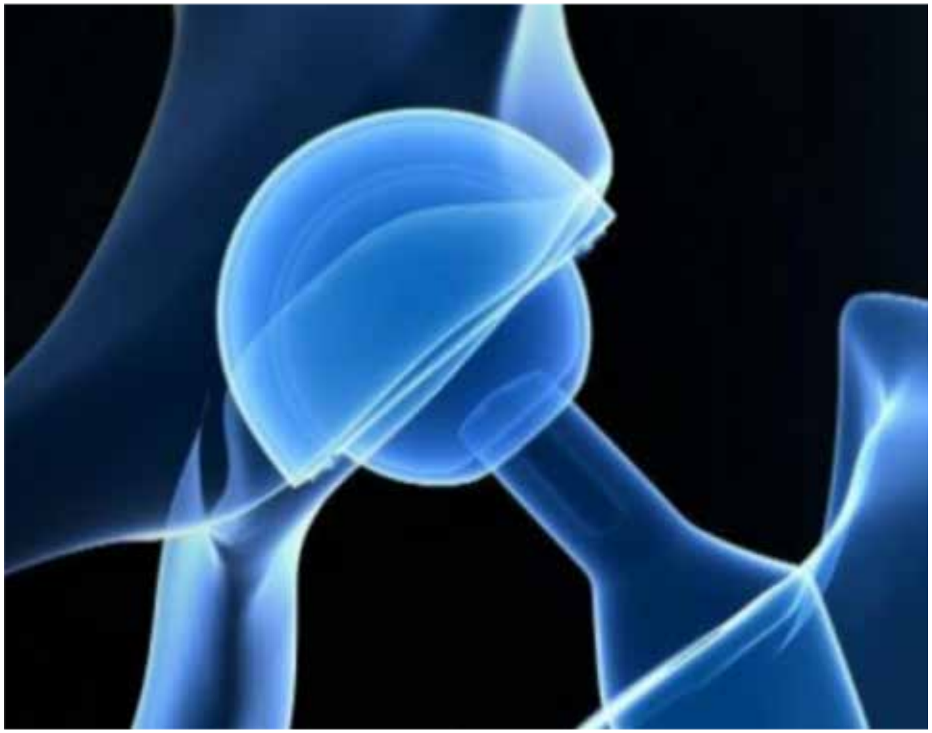
Outcome Economy

Bruce Sinclair

- 60 – 90 Minute Procedure

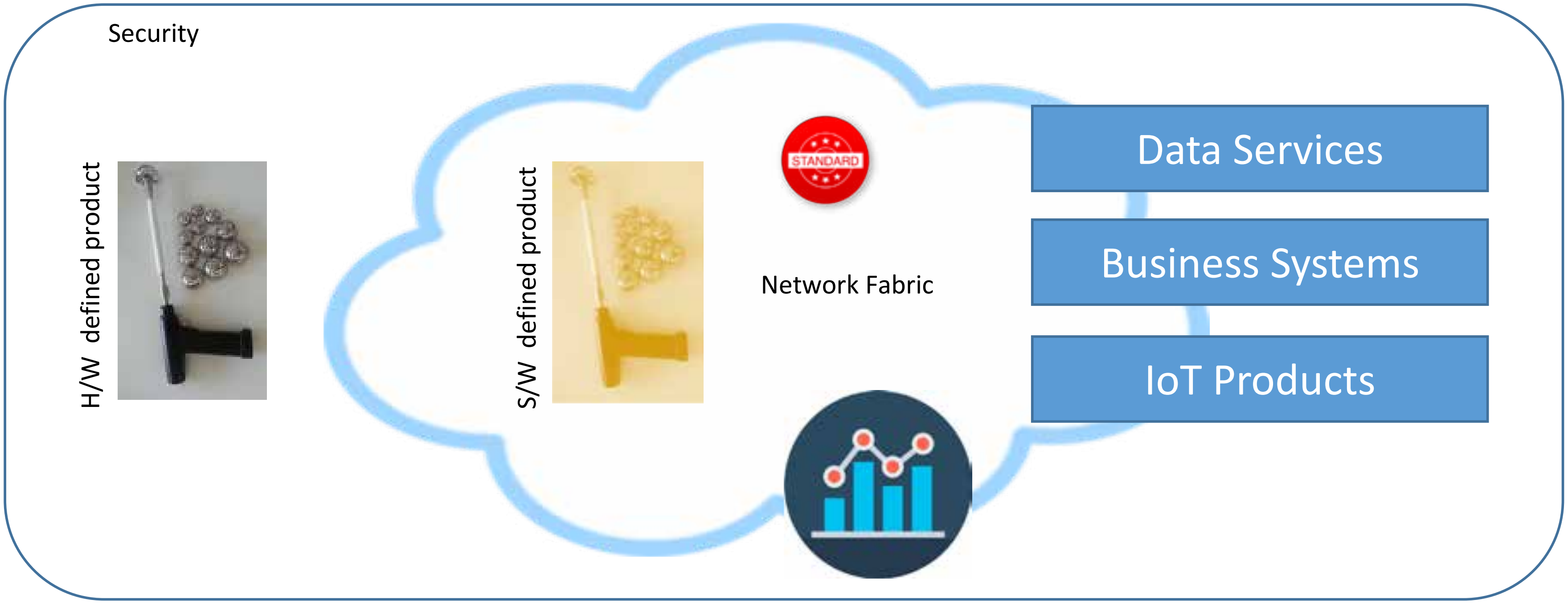
- Acetabular Reamer
  - Drill a cup in pelvis

- Challenge – Necrosis



IoMT Value Proposition

- Perform the procedure in the shortest time while maintaining patient health
  - Redress rates



Security

H/W defined product

S/W defined product

Network Fabric

Data Services

Business Systems

IoT Products

- Hardware Defined Product
- Software Defined Product
  - Digital Twin, Application
- Standardization
  - Media, Networking, Application

- Network Fabric
  Cloud, Fog
- External Systems
- Analytics & Big Data
- IoT Device Security

IoMT - Model

- Temp is a *f*(Rotational Speed, Pressure, Time)

- Sensors = Rotational Speed, Pressure, Time

Application Requirements

- Control rotational speed to limit temperature
- Rewrite equation:
- Rotational Speed = *f*(Temp, Pressure, Time)
  - Temp never above 55

Application Requirements

- Expand equation to include -

Rotational Speed = *f*(Temp, Pressure, Time, Patient Demographics, Health, Environment, etc)

Analytics can help predict results (Outcomes)

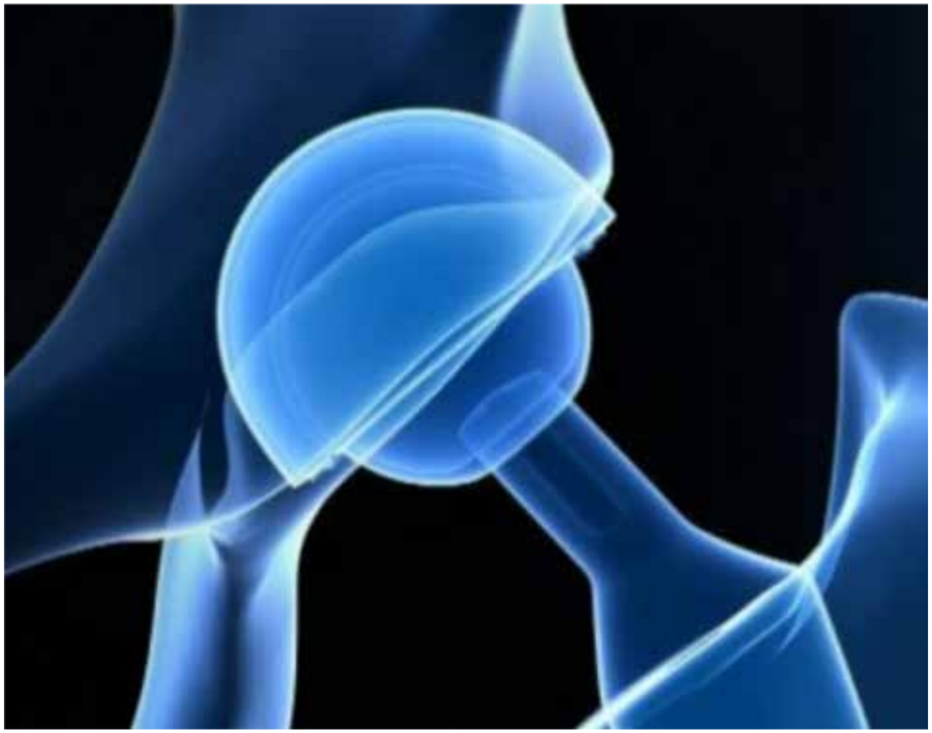
Application Requirements

Different Model to evaluate:

- Optimize Blade Design
- Operation
- Other parameters

Importance of Data

- In this Example:
  - Data is critical to creating value
    - Patient
    - Hospital
  - Influencing outcome
  - Value proposition extends well past keeping patient data safe & secure
  - Context



IoT / IoMT Axiom

- All incremental value from an IoT / IoMT product comes from transforming its data into useful information.

- Critical CIA
  - Confidentiality
  - Integrity
  - Accessibility

IoT / IoMT Challenges

- Wireless / Cordless / Convenience

- VA / DoD
  - DoD and Department of Veteran Affairs Directives require:
    - Specific Wireless Protocols
    - FIPS Validation

References

Department of Veterans Affairs Medical Device Isolation Architecture Guide V2.0, http://www.himss.org/department-veterans-affairs-medical-device-isolation-architecture-guide-v20-0

Department of Veterans Affairs VA Handbook 6500, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=793&FType=2

Department of Veterans Affairs VA Directive 6512, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=883&FType=2

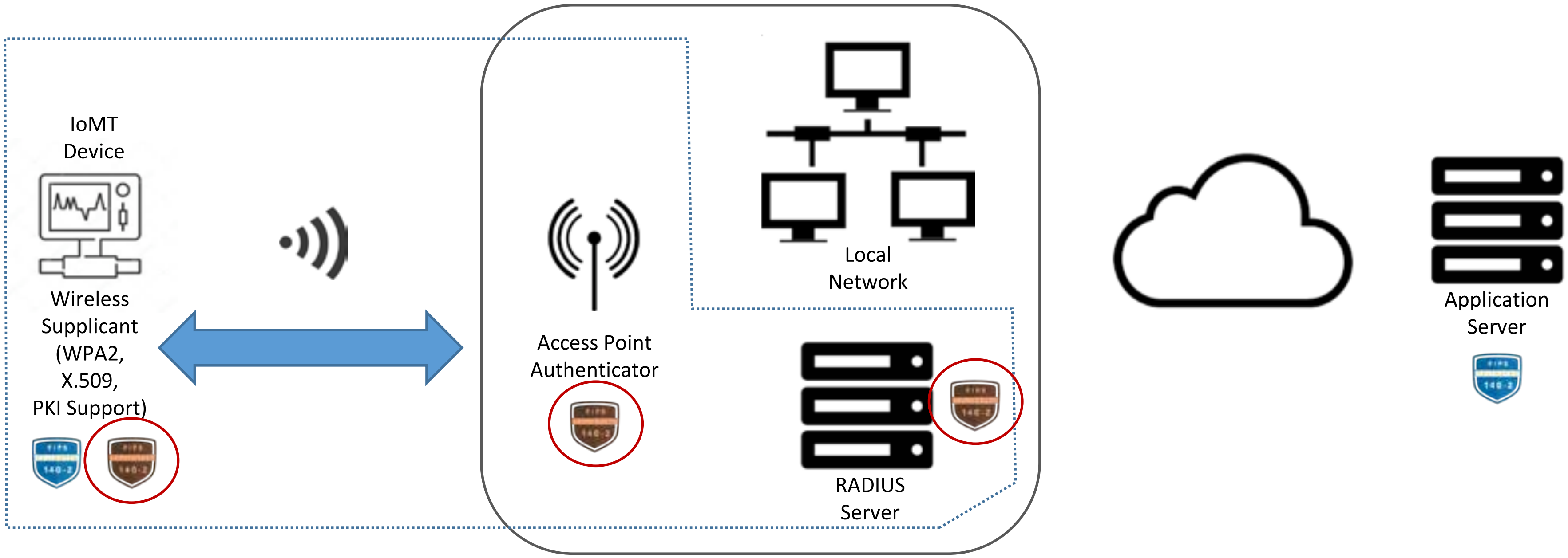
IoT / IoMT Challenges

- WiFi Alliance and WiFi Certified
  - Requires WPA2 for both Personal and Enterprise
  - Utilizes AES-CCMP
  - Integrated into the silicon
  - For FIPS Validation must provide mechanism for POST
    - Specific VECTOR and KAT

Requirements

- Wireless
  - Need to establish secure communications between a wireless device and an Access Point
  - Need to authenticate and validate that the device is authorized to use the network
  - Need the following technologies
    - 802.11i (WPA/WPA2) – WPA2 uses AES-CCMP and is FIPS Compliant
    - 802.1X (EAP/EAPOL/EAP-TLS) – Supplicant on the wireless device
    - 802.1X (Authenticator) – On the Access Point
    - RADIUS Server (Authentication Server)

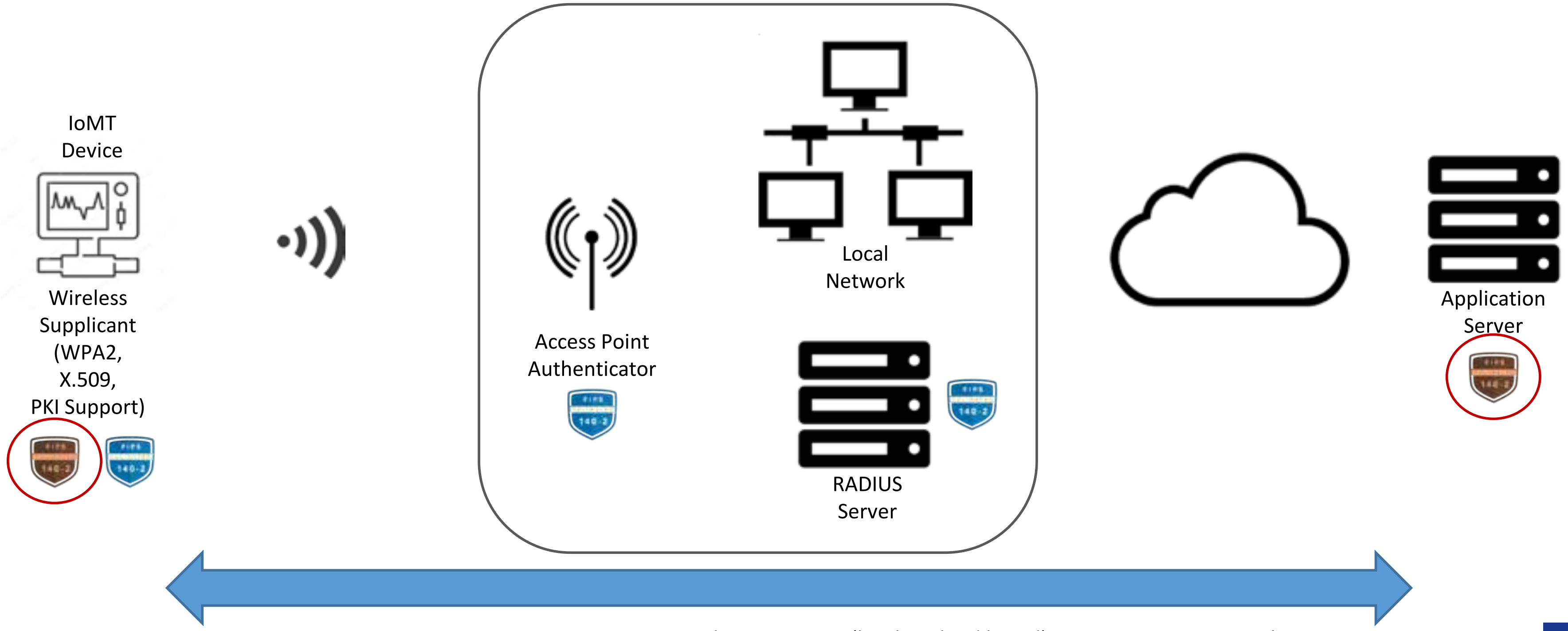
FIPS Deployment (Wireless Connectivity)



Creating a Secure Connection to the local network using 802.1X, EAP-TLS,
WPA2 - 802.11i – NOTE: Encrypts data between Device and Access Point

Allegro

FIPS Deployment (Communication to Server)



IoMT Device

Wireless Supplicant (WPA2, X.509, PKI Support)

Access Point Authenticator

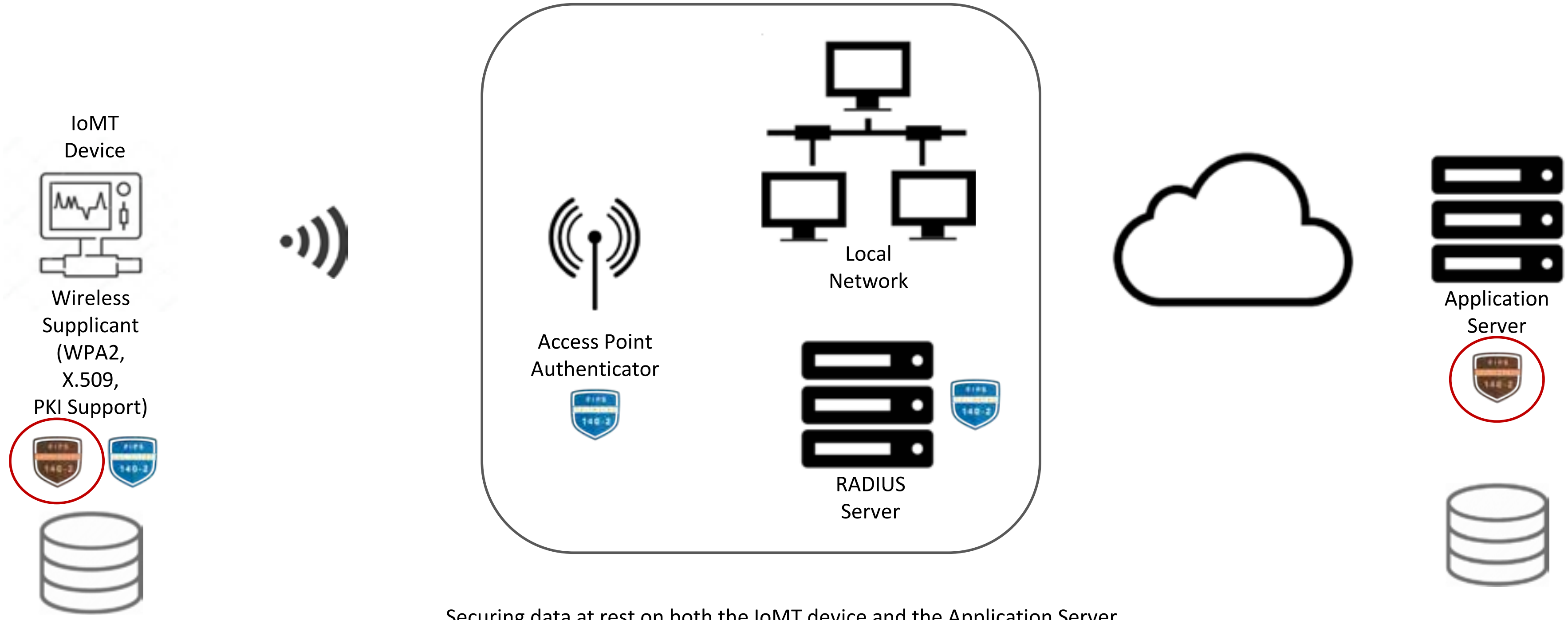
Local Network

RADIUS Server

Application Server

Creating a Secure Connection to Application Server (local or cloud based) using TLS, X509, PKI tools.
Secures PII while in data is in motion.

FIPS Deployment (Data at Rest)



Securing data at rest on both the IoMT device and the Application Server.

Holistic View

- Validated Modules
  - IoMT
    - Wireless Module
    - Application Cryptography Module
  - Access Point
    - Wireless Module
  - Application Server
    - Application Cryptography Module – optimized for server environment

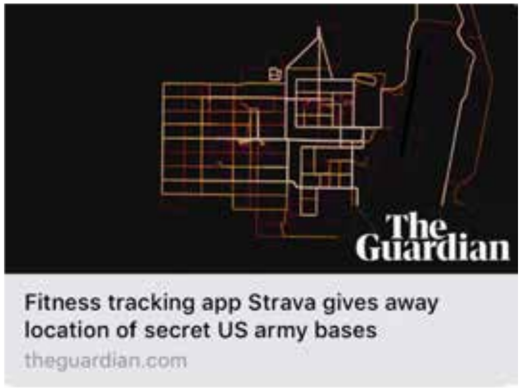
FIPS, IoT Medical Devices and VA/DoD

Data Security Can Be Complex

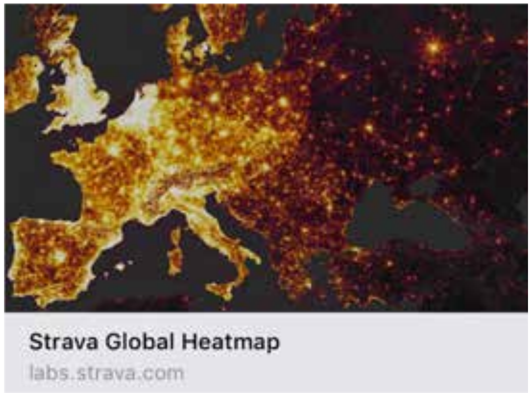
- Data triangulation
  - Use of third party data
- November 2017
  - Strava releases map of “anonymized” data of 3 trillion GPS data points
  - App used on various fitness trackers/cell phones to see popular running routes used by others
  - Gives away sensitive information about a subset of Strava users – military personnel on active duty

Knowing where to look

- Looking closer at the maps you can:
  - Identify secret underground bases in foreign countries
    - “US Bases are clearly identifiable and mappable”
    - In Syria, known coalition bases lite up at night



Fitness tracking app Strava gives away location of secret US army bases
theguardian.com



Strava Global Heatmap
labs.strava.com

- https://www.strava.com/heatmap#5.00/36.56084/29.97505/hot/all
- https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Thank You

Loren Shade

Allegro Software

loren@allegrosoft.com

+1 978-252-7355