Digital Healthcare-Associated Infection: A Case Study on the Security of a Major Multi-Campus Hospital System

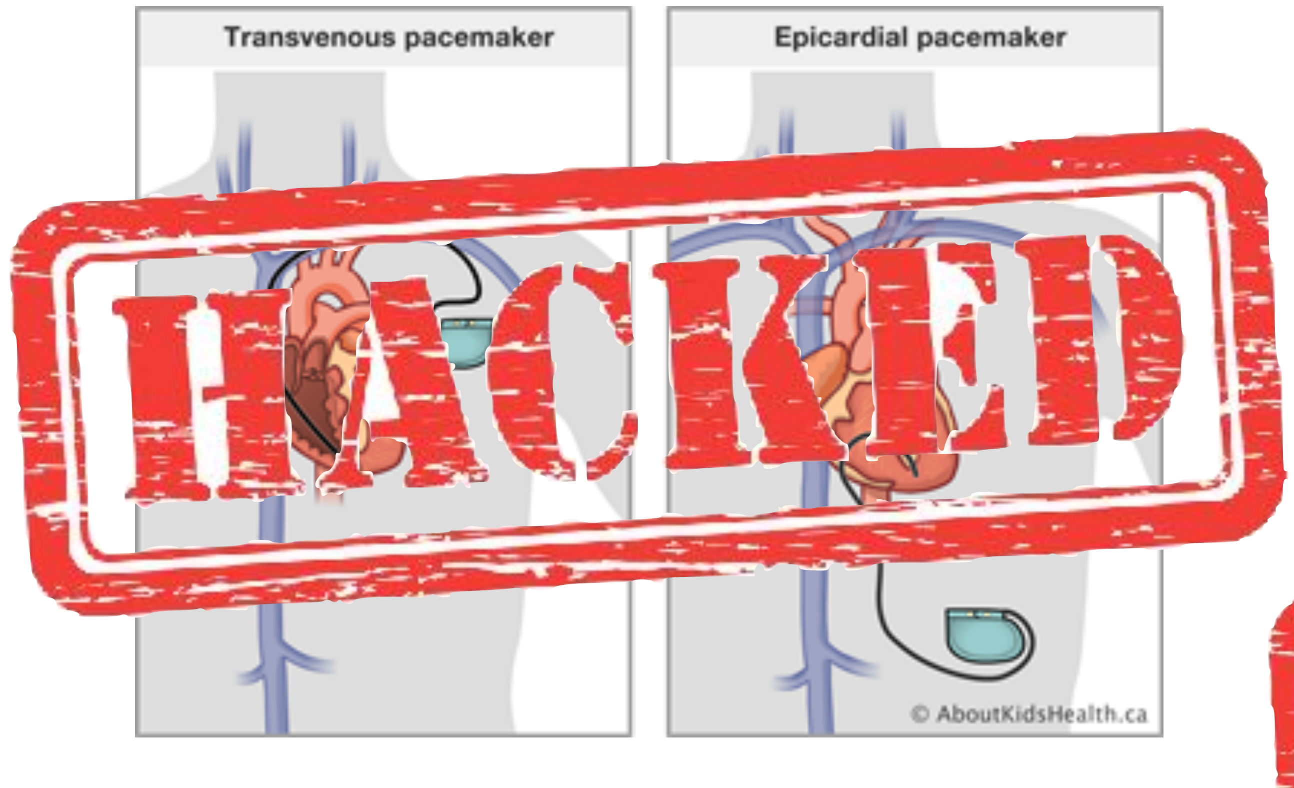
Luis Vargas, Logan Blue, Vanessa Frost, Christopher Patton, Nolen Scaife, Kevin R.B. Butler, and Patrick Traynor

26th Annual Network and Distributed System Security Symposium
San Diego, California
24 – 27 February 2019

Two worlds colliding

Medical devices

[1]



[3]

[2]

enterprise studies

[This Session]

[1] Halperin, Daniel, Thomas S. Heydt-Benjamin, Benjamin Ransford, Shane S. Clark, Benessa Defend, Will Morgan, Kevin Fu, Tadayoshi Kohno, and William H. Maisel. "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses." In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 129-142. IEEE, 2008.
[2] Li, C., Raghunathan, A., & Jha, N. K. (2011, June). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on* (pp. 150-156). IEEE.
[3] Bonaci, T., Herron, J., Yusuf, T., Yan, J., Kohno, T., & Chizeck, H. J. (2015). To make a robot secure: An experimental analysis of cyber security threats against teleoperated surgical robots. *arXiv preprint arXiv: 1504.04339*.

Operational environment?

Let's look at the network!

While network studies have been useful in many enterprises, performing such a study on a hospital requires special care… **as they contain unique data types and any unscheduled downtime to hospital devices can cause life-threatening situations.**

In this talk, we discuss…

Ethical challenges in the design process

Characterization of the hospital network

Measurement results from network traffic

Designing an ethical study

- What would an enterprise study look like?
- By design, the study should minimizes any potential for negative impacts
- **Two-year process** involving legal-IT-IRB teams of the university/hospital
- Two specification were placed:
    - Keep patients/workers information private
    - Must not disrupt daily operations

Limitations on data collection

- Private information
  - Packet payloads
  - P2P
  - HTTP
  - DHCP
- Undistributed daily operations
  - Strictly passive (no nmap or similar)
- Agreement with the hospital
  - Would *you* let a stranger look into your network?

The design process posed limitations but it is an **absolutely critical component** of ethical research

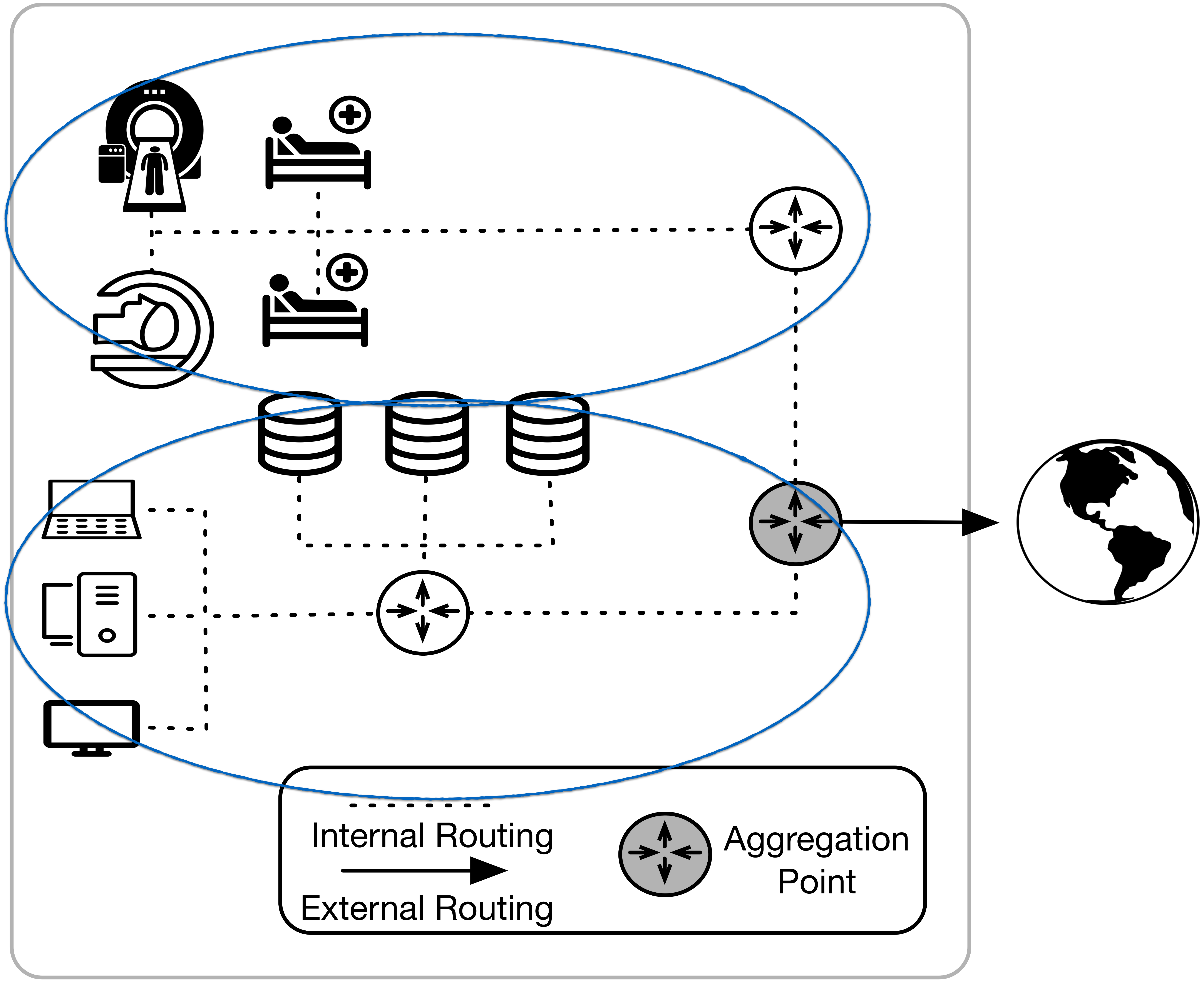
In this talk, we discuss…

Ethical challenges in the design process

Characterization of the hospital network

Measurement results from network traffic

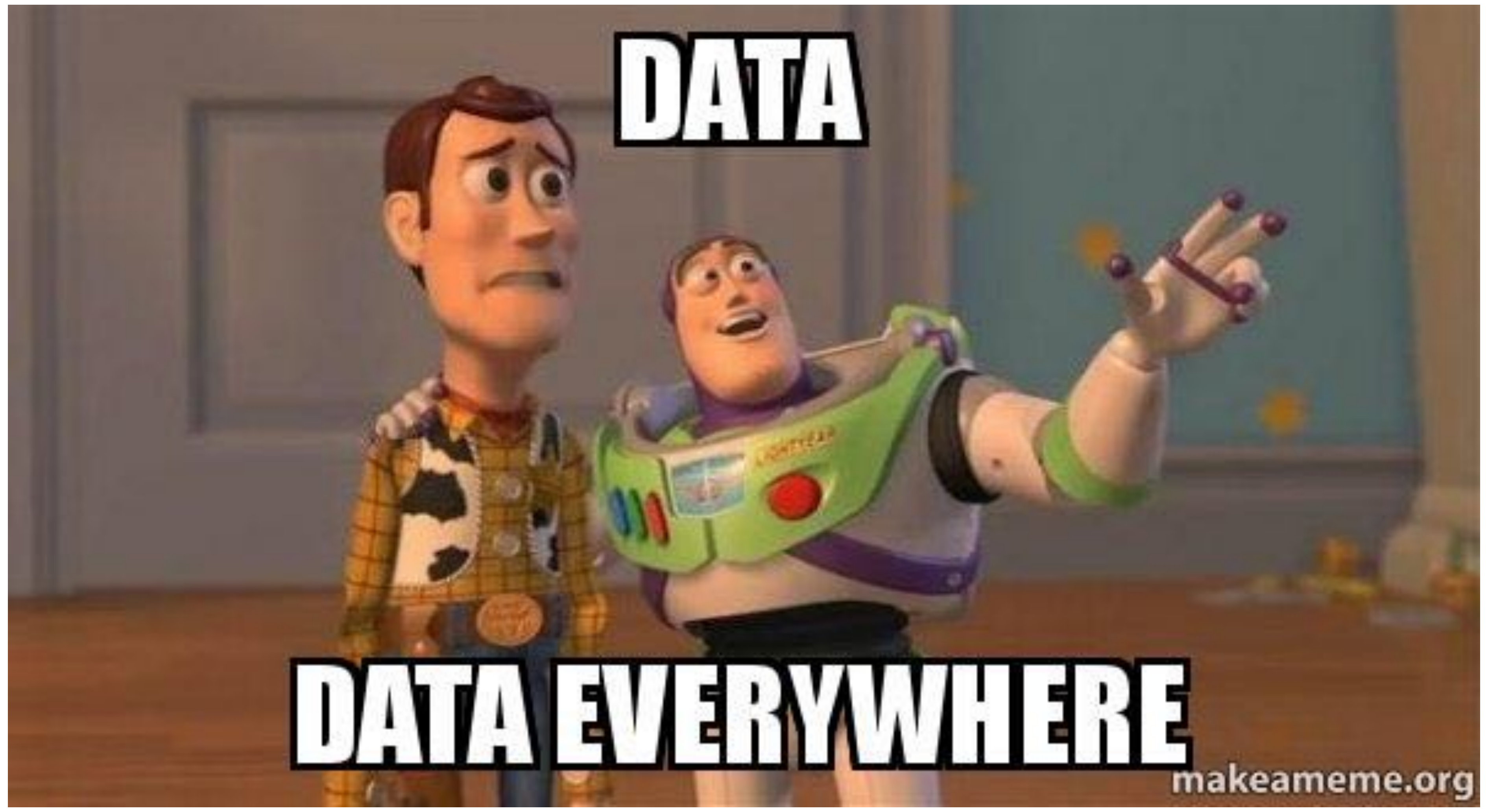
Observed hospital topology



Medical devices were *actively protected* and mostly invisible from a network perspective (both internally and externally)

Data sources

- Hospital logs (6 month - 418GB of raw logs)
  - DNS requests (725 million request)
  - Established TLS handshakes (325 million sessions)
  - Certificates
- OSINT — ground truth
  - Alexa & Umbrella top sites
  - Blacklists (5 sources)
  - Certificate Transparency (CT) logs
  - Censys



Insights of the hospital network

- Who the medical supporting devices are communicating with

- How they are establishing communications channels

In this talk, we discuss…

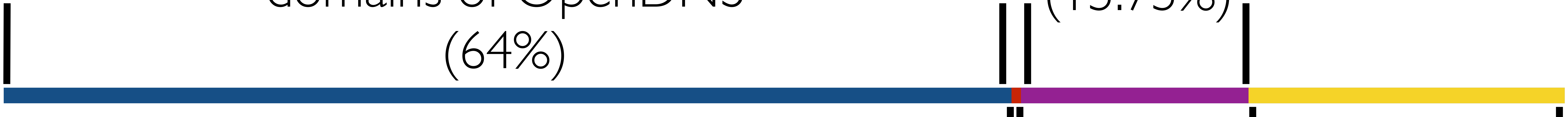
Ethical challenges in the design process

Characterization of the hospital network

Measurement results from network traffic

Categorizing DNS requests

Hospitals can benefit from having customized blacklist/whitelists techniques



whitelisted based on top 100k domains of OpenDNS (64%)

Self-association metric (15.75%)

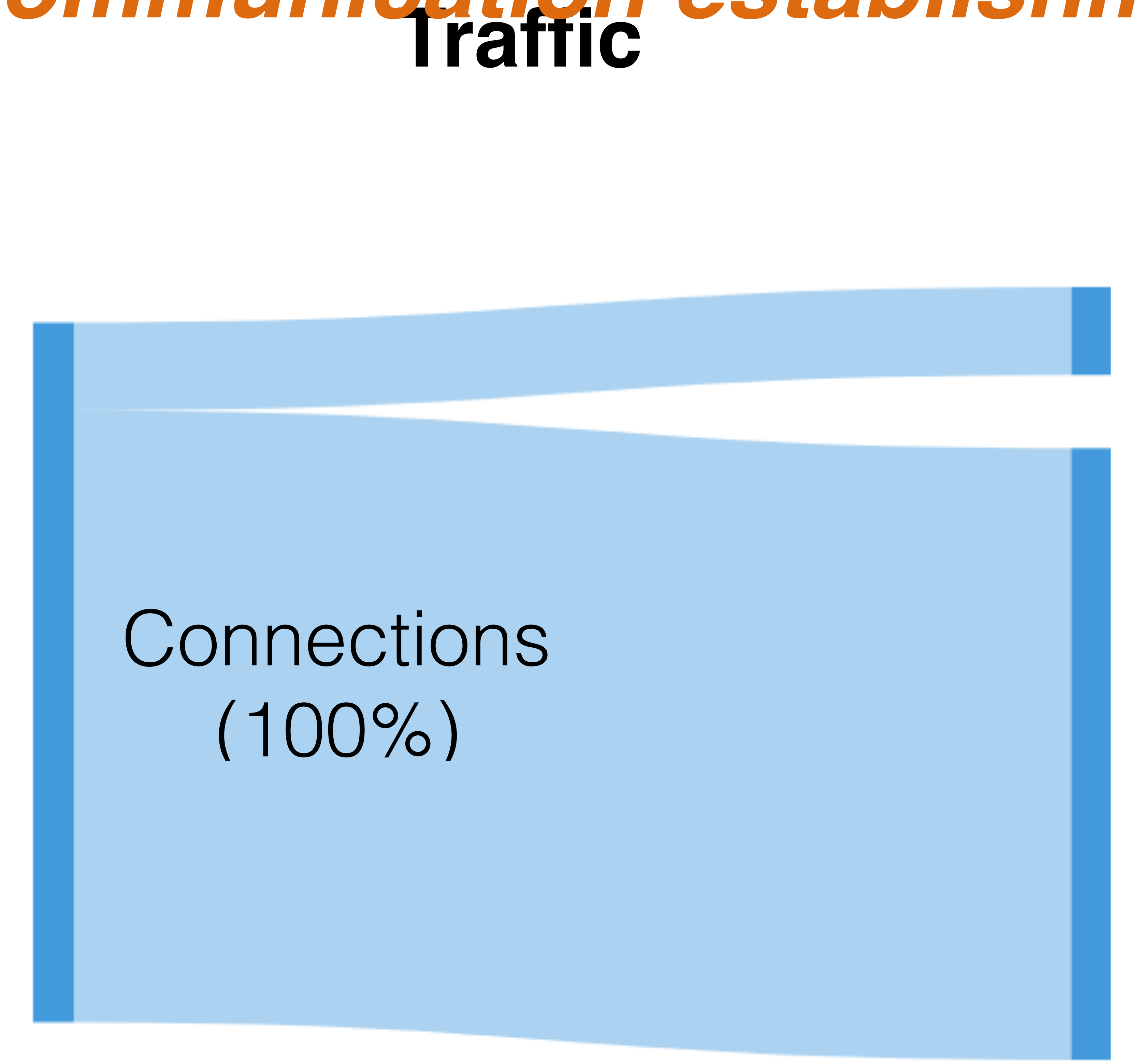
(~20%) no category

(0.01%) Blacklisted requests

Botnet related requests (Zeus & Feodo)

TLS communication breakdown

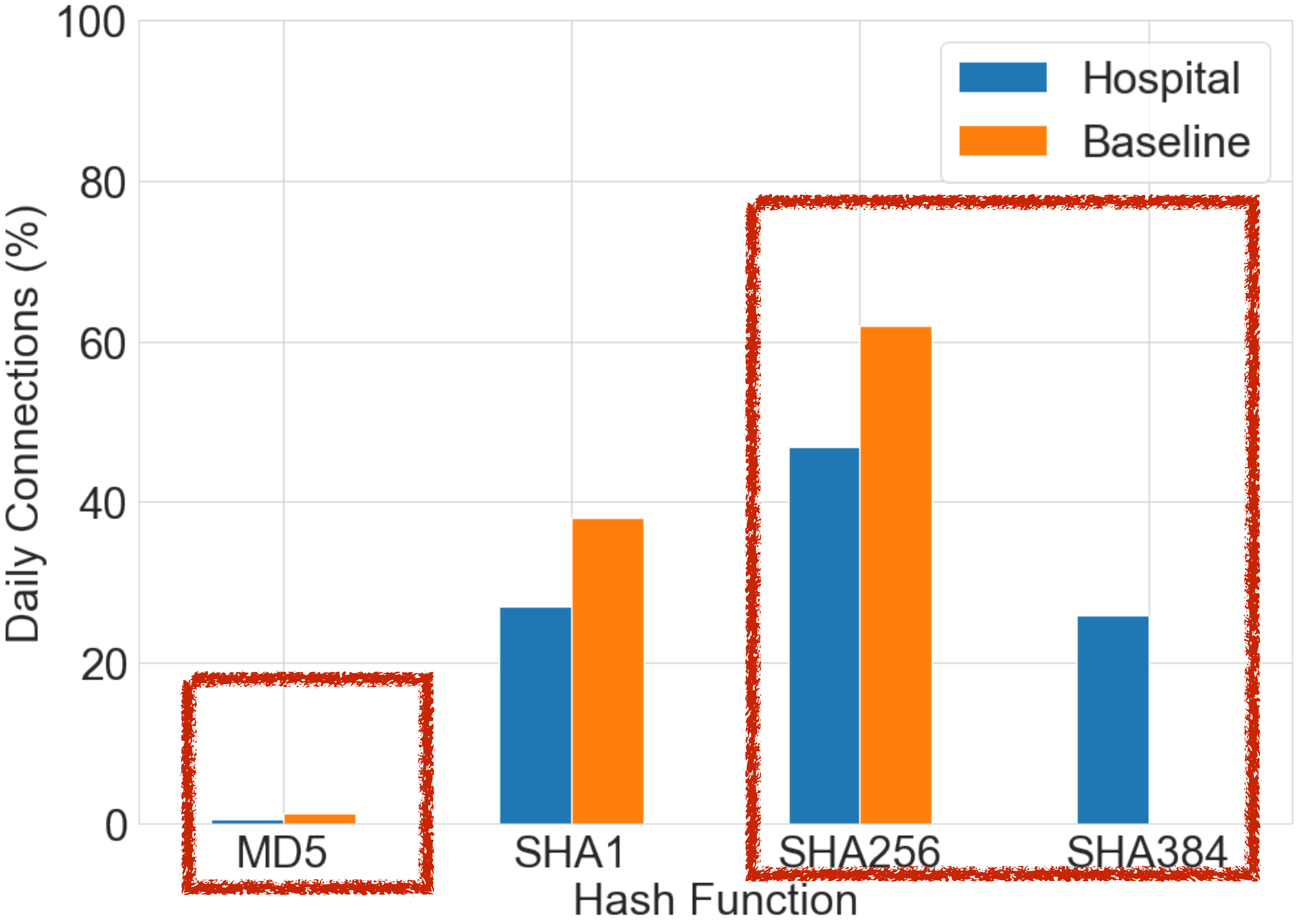
Communication establishment mostly follow good cryptographic practices



Secure	Weak	Insecure	Broken
AES-GCM ChaCha20-Poly1305 ECDSA SHA2	CBC RSA-PKCS#1v1.5	SHA1 RC4 3DES	Anonymous DH MD5 DES Export

>= TLS1.2

Hashing used in connections



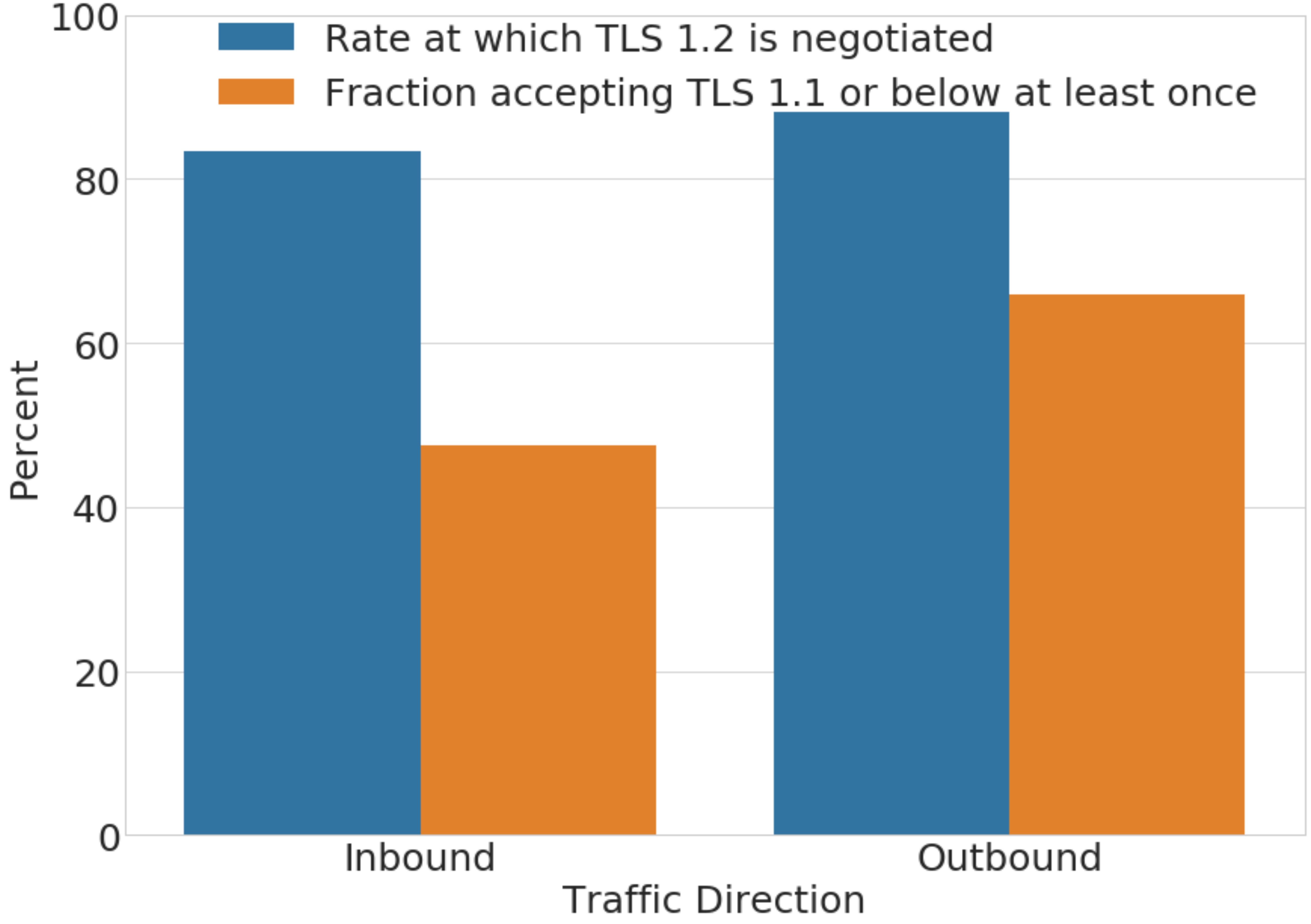
- MD5 (<1.5%)
- Secure hash
  - Hospital (72%)
  - Baseline(62%)
- SHA1 usage did not change

Secure authentication of end points is more common in the hospital than the baseline

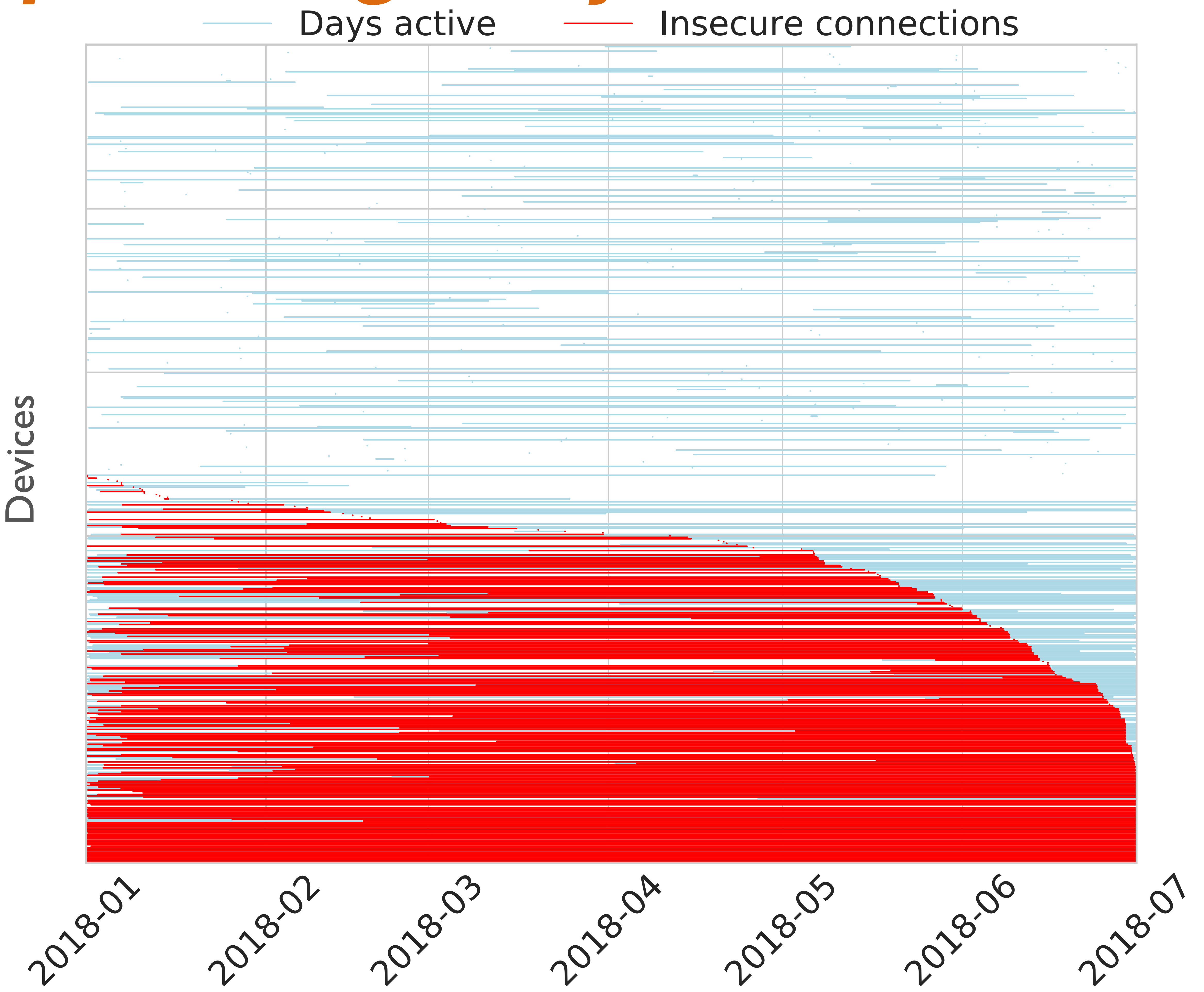
TLS configuration of devices

Long lasting medical supporting devices appear to not update regularly

Partial configurations

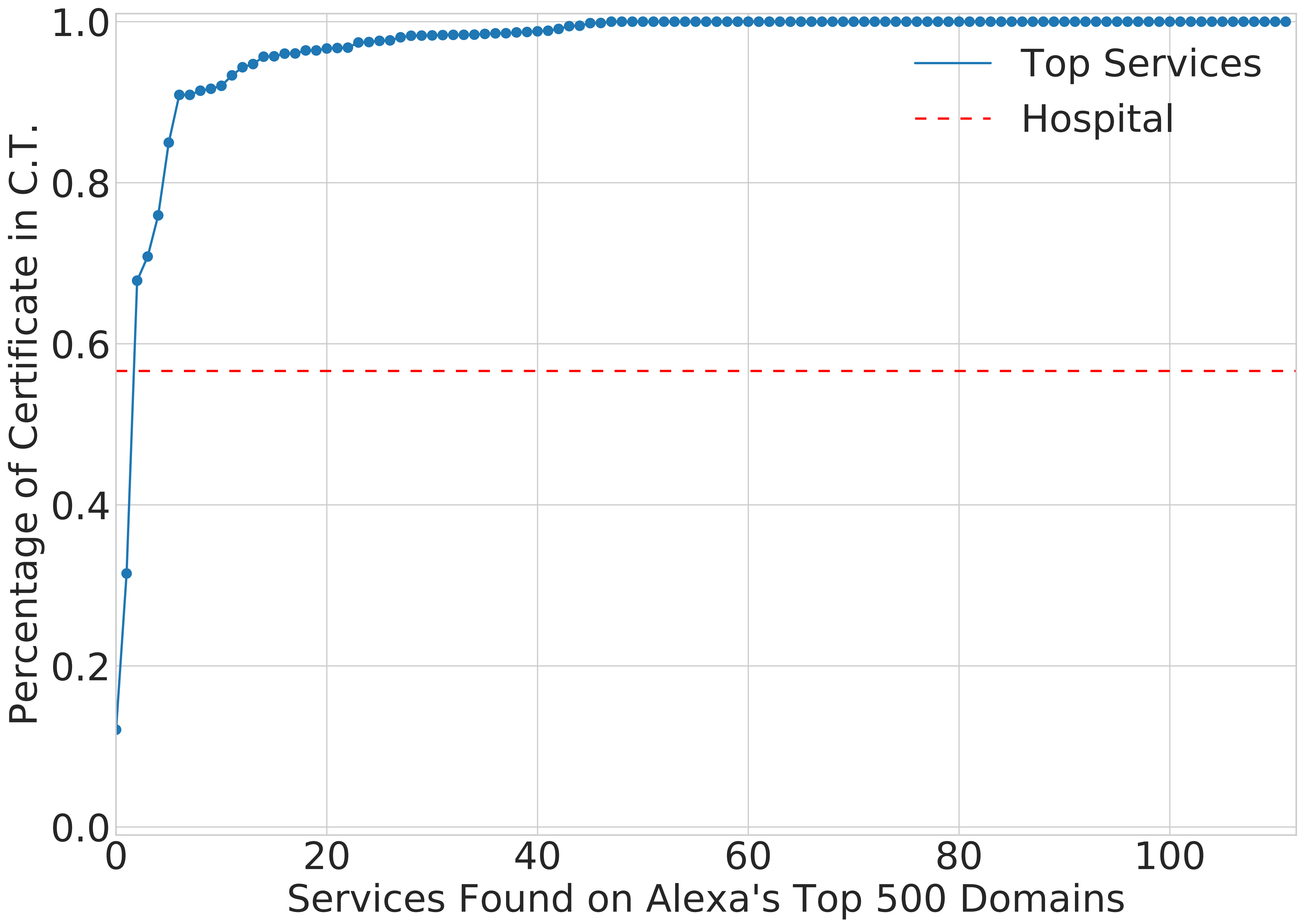


Last use of deprecated protocol



What about the certificates?

- 9% of connection reported with some issue
  - Certificates with no issuer (~11%)
  - Self-signed/expired certificates
- Certificate Transparency?
  - ~60% of hospital certificates found in CT



The hospital adoption of CT is slower than the Internet's top services.

Limitations

- Hospital security is multidimensional and requires more research aside from network egress/ingress point of view
  - Passwords get compromised
  - Misplaced end devices
  - Theft
  - Access control

Take away

- Hospital research requires careful consideration/collaboration from legal, ethical, and administrative domains
- The case study showed traffic isolation and good cryptographic practices
- This work sets a starting point for broader examinations of hospitals

@vargasL25
lfvargas14@ufl.edu
LuisVargas.me

Extras

Interesting Findings

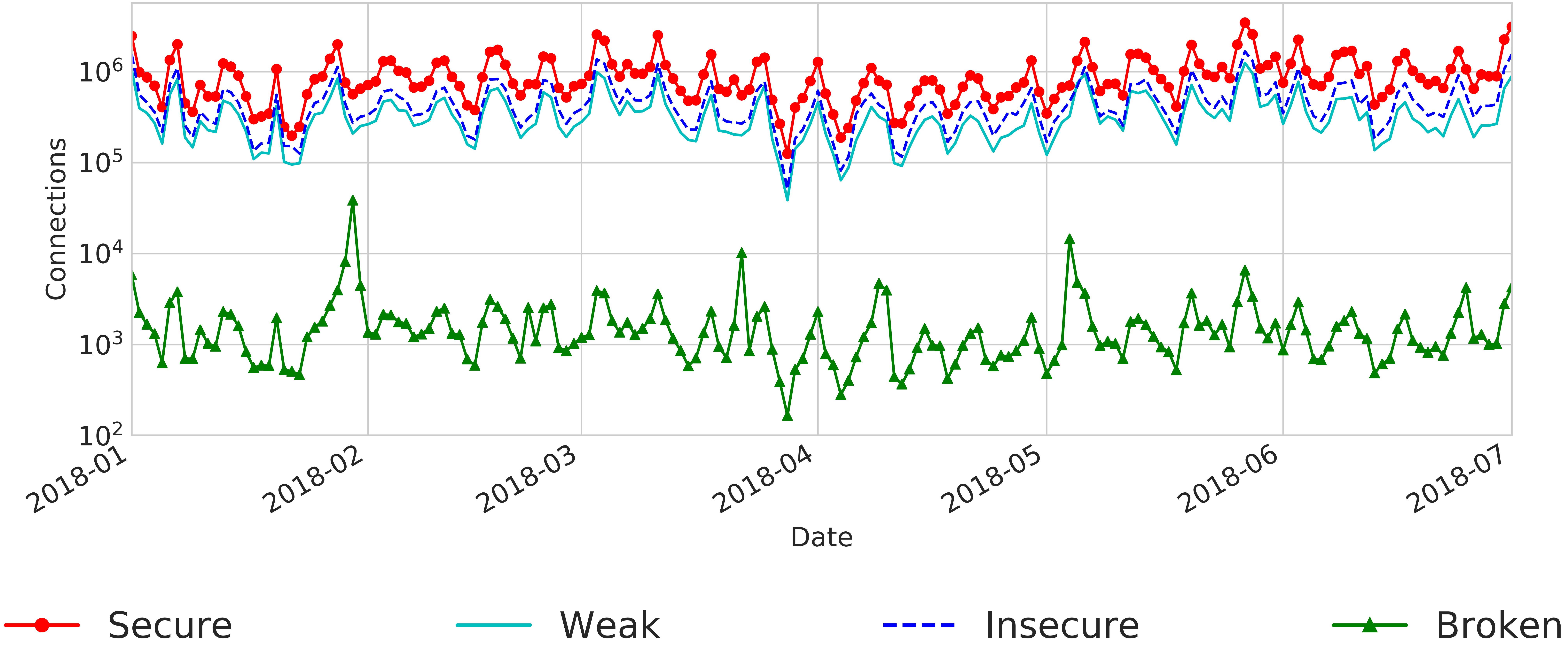
- Medical devices appear to be highly protected in the operational environment
- Standard categorization techniques do not adequately represent the hospital
- The hospital follows good cryptographic practices
- While Certificate Transparency gained a lot of traction, there is still room to grow regarding hospital work

Limitations on data collection

- Private information
  - Packet payloads
  - P2P
  - HTTP
  - DHCP
- Undistributed daily operations
  - Strictly passive (no nmap or similar)

The design process posed limitations but it is an **absolutely critical component** of ethical research

Cipher quality handshakes



AES-GCM
ChaCha2-Poly1305
ECDSA
SHA2

CBC
RSA-PKCS#1v1.5

SHA1
RC4
3DES

Anonymous DH
MD5
DES
Export

Open areas of research

- Generalizing Hospital Ecosystems
  - Are other hospitals configured the same way?
  - Size of hospital/funding available security team
- Network study solely based on the medical devices
- Understanding non-technical issues face by hospitals