Towards Composable Threat Assessment for Medical IoT (MIoT)

Salaheddin Darwish, Ilia Nouretdinov, Stephen Wolthusen

School of Mathematics and Information Security

ROYAL HOLLOWAY UNIVERSITY OF LONDON

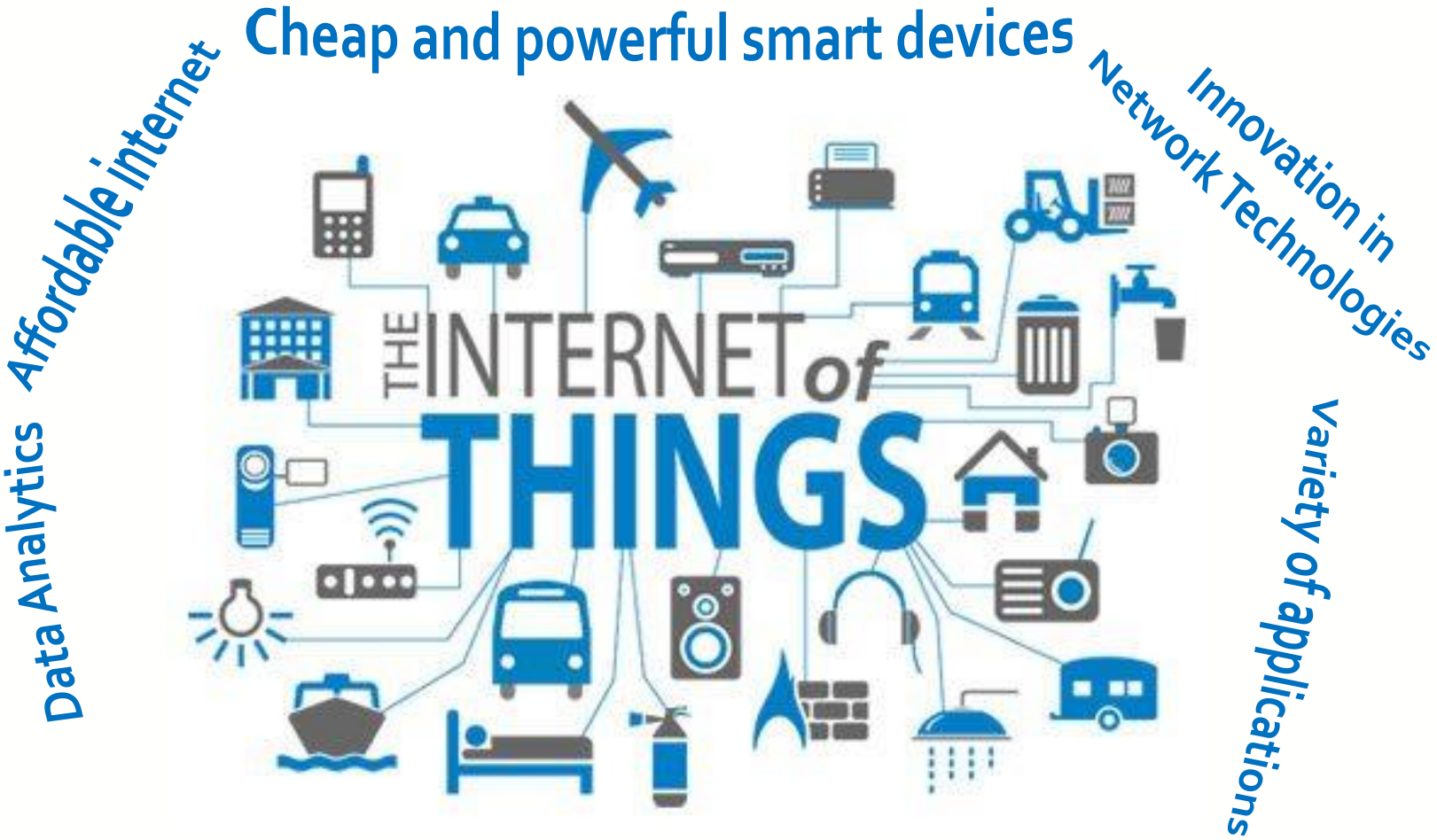
The fourth International Workshop on Privacy and Security in HealthCare 2017 (PSCare17) in Lund, Sweden

Agenda

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Introduction
- Medical IoT System
- Motivation
- Security and Privacy Medical IoT Challenges
- Threat Identification (Approach and Composability Feature)
- TIHM Threat Assessment (Case Study)

Introduction



Medical IoT Systems

- Medical IoT is another wave of IoT technologies to support public healthcare domain [1].
- The current Medical devices undergo a massive transformation [1,2].
- In our context, a MIoT system is defined as a healthcare system relying on monitoring devices to track the patient's condition so the clinicians would remotely assist the patient health and check if a medical intervention is required[3].
- This system can be exploited in domestic care environments, clinic settings or outpatient control.

* http://www.infiniteinformationtechnology.com/iot-md-transformation-and-capabilities-of-md

Motivation

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Importance of threat and risk assessment on security and privacy in MIoT: Risks and threats may lead to compromise of devices, violations of data quality and integrity, breaches of privacy expectations or policy violations as well as information governance requirements.
- However, devices and software configurations or the way data is processed by intermediate systems may change frequently, this raises the problem of continued validity of any risk and threat assessment.
- This work seeks to propose an approach for enhancing the efficiency of risk and threat assessments under updates and composition.

Security and Privacy Medical IoT Challenges

ROYAL HOLLOWAY UNIVERSITY OF LONDON

The MIoT systems have several security and privacy challenges [4] , we propose the following priority list of the most crucial ones:

1. **Device Integrity**: information has to be correctly collected and transferred by medical devices and sensors.
2. **Data Integrity**: non-existence of information flows that may have been subject to modification by entities at different levels of integrity than the originating principal (e.g. integrity of data-in-flight).
3. **Confidentiality**: a principal does not disclose information to unauthorised entities allowing the deduction of the state of the principal.
4. **Availability**: information or the means to process these must be available when they are requested/required.
5. **Privacy**: correct sharing of information also among sets where membership may vary over time.
6. **Security Usability** refers to how to make security features easy to use by users (i.e. the security mechanisms accomplish their objectives even they are not used properly).

Threats Identification (1)

- HMG IS1 Risk and Threat Assessment Standard is adopted:
  - well-structured approach.
  - Address Threat Sources and Actors in the assessment.

(1) Define Focuses of Interest (FoI) related to system architecture, i.e.- subsystems' and devices' features. for example:

- Communication infrastructure
- Device capabilities
- Storage systems
- Cloud systems
- Data (aggregation properties)

(2) Identify and evaluate Threat Sources according to FoI and the security objectives (Confidentiality, Integrity and Availability). A Threat Source is a person or organisation who would exploit a security breach for benefits. For Example:

- Hackers
- Virus and malware writers
- Commercial competitors
- Accidental misuse group

(3) Identify and evaluate Threat Actors. A Threat Actor is a person who actually launches the attack or enables an incident. HMG IS standard[1] classifies them into different families according to their common capability, motivation and opportunity As examples, there may be:

- system and service users
- direct and indirect connected non-system-or-service users,
- supply chain users

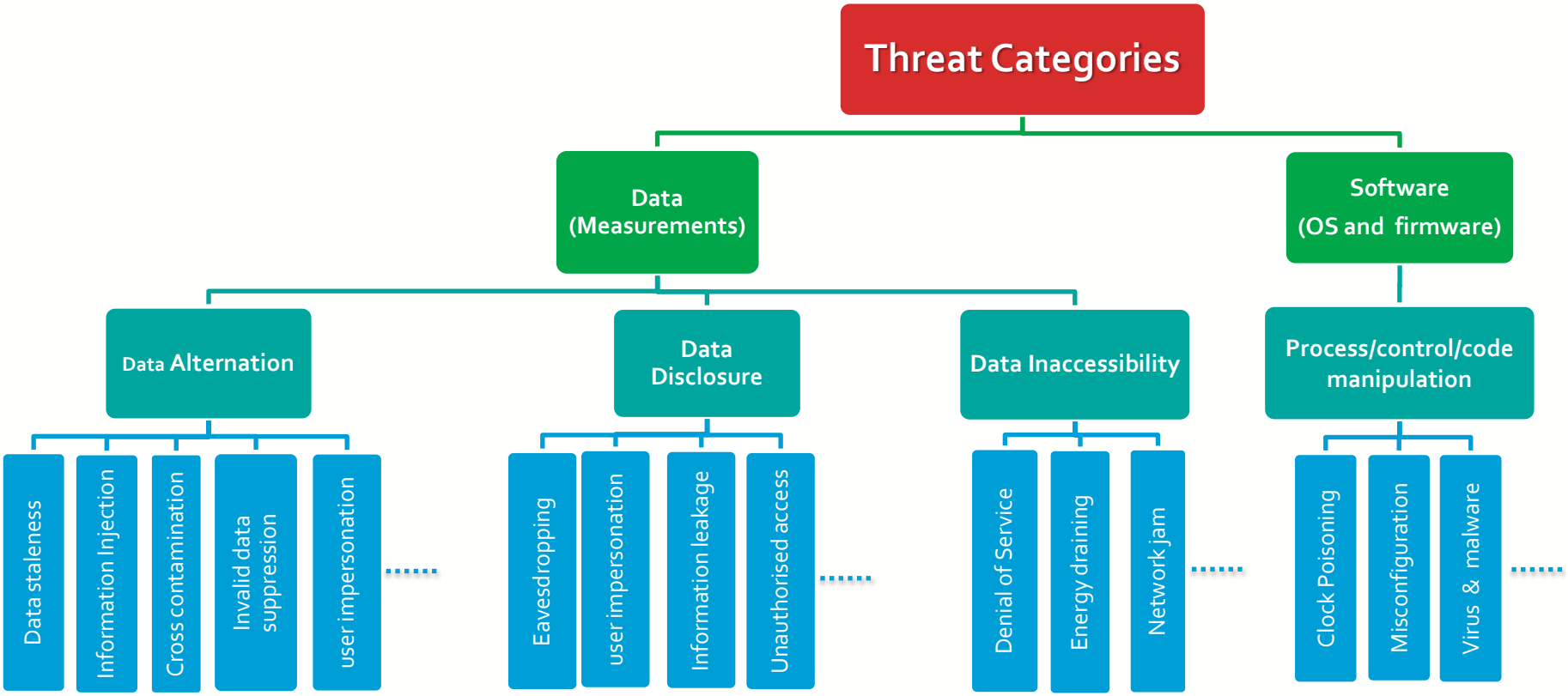
(4) Identification and evaluation of Threats and Vulnerabilities based on the defined Focuses of Interest (i.e. assets) and security goals of integrity, confidentiality, and availability, for example:

- Eavesdropping
- Impersonation
- Data leakage and contamination
- Virus and malware

The HMG IS1 method for assessing security threats [5]

Threats Identification (2)

- Threat taxonomy based on type of data targeted:

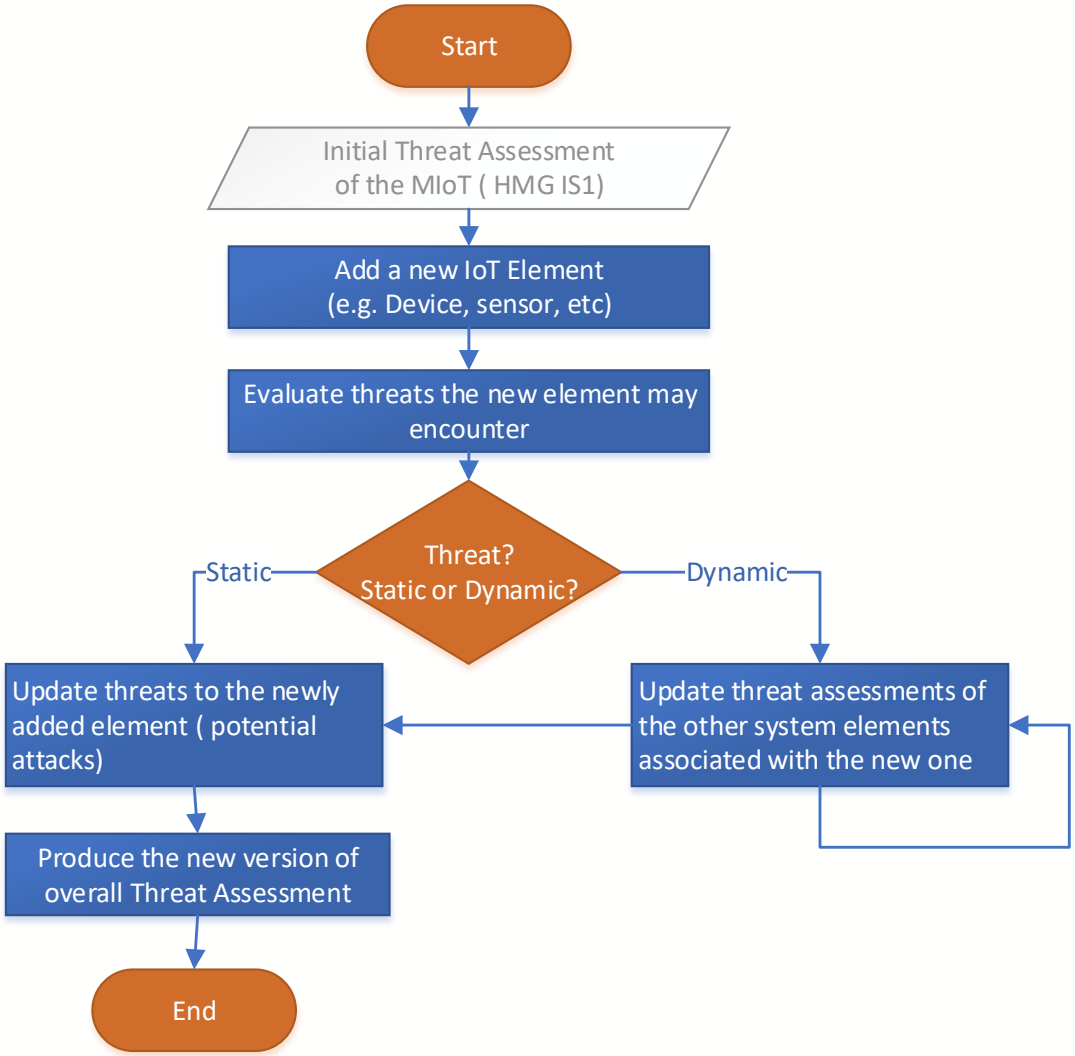


Threats Identification (3)

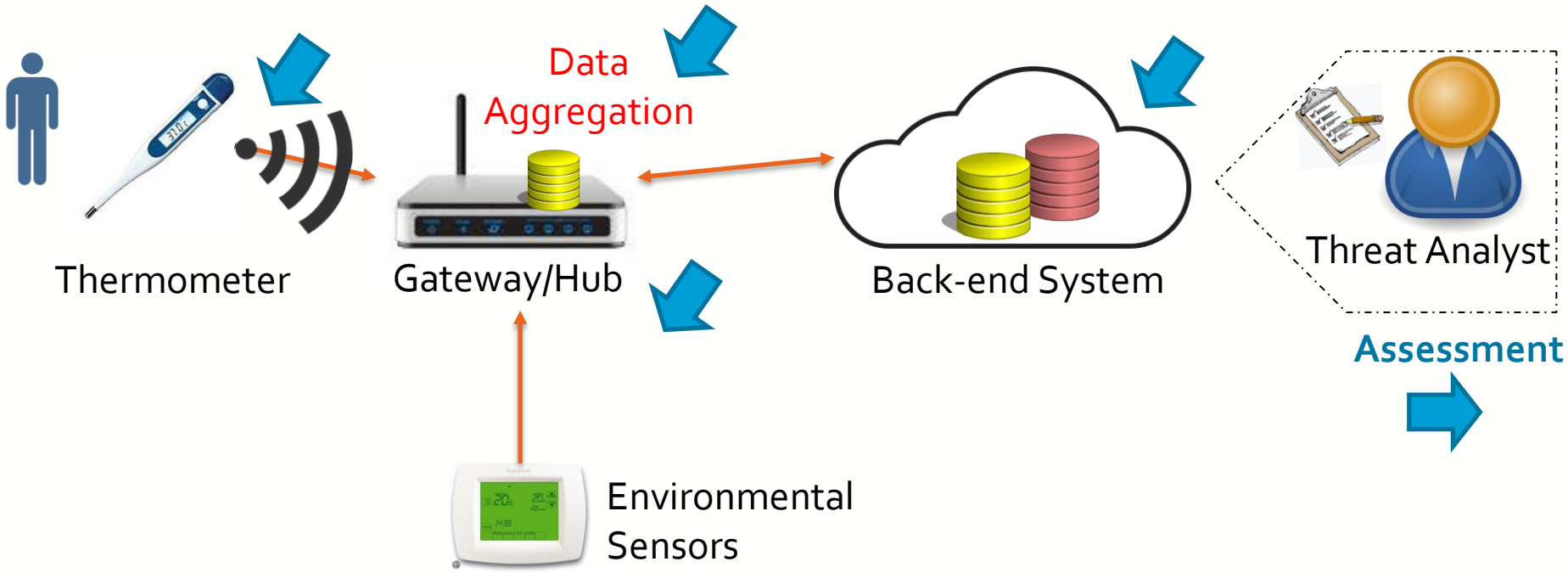
ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Composability in Threat Identification: We propose a composability property for the threats encountered by the MIoT components:
  1. **Static property** refers to threats (i.e. attacks) that need consideration only in newly added MIoT devices.
  2. **Dynamic property** (i.e. data-related) indicates that the check is demanded not just for newly fitted MIoT devices but also for all other associated devices. Indeed, these specific threats appear to be strongly related to data being handled (e.g. clock poisoning, corruption and contaminated information, privacy breaches from information leakage).

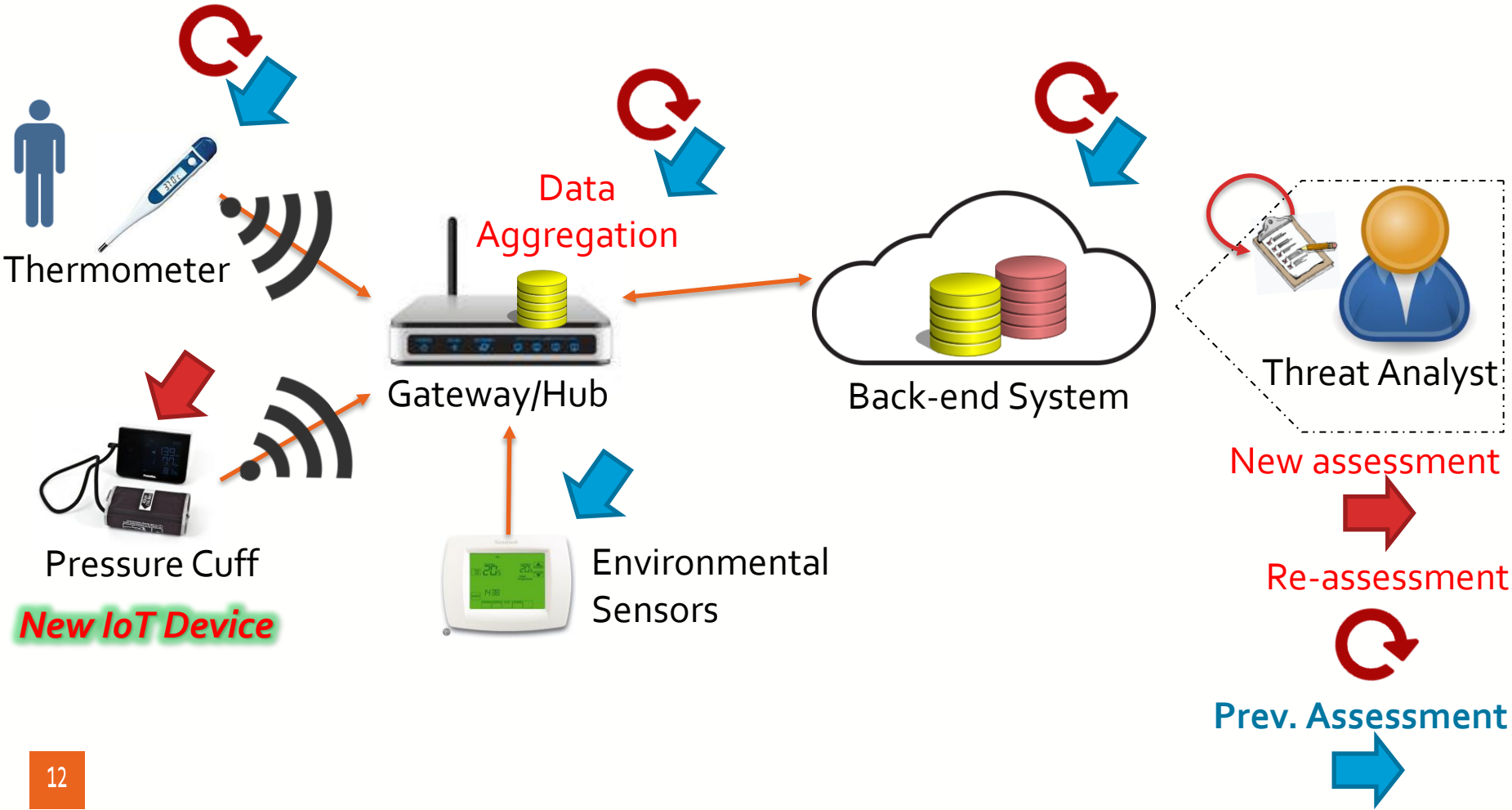
Our Proposed Approach



Our Proposed Approach (Example) (1)



Our Proposed Approach (Example) (2)



TIHM (Technology Integrated Health Management) for Dementia Project

ROYAL HOLLOWAY UNIVERSITY OF LONDON

http://www.sabp.nhs.uk/tihm

Surrey and Borders Partnership NHS
NHS Foundation Trust

SPS

Alzheimer's Society
United Against Dementia

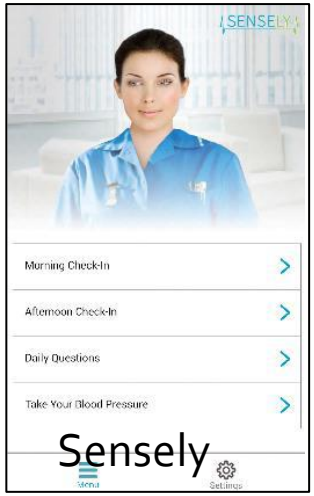
ROYAL HOLLOWAY UNIVERSITY OF LONDON

UNIVERSITY OF SURREY


Yecco

Docobo


Halliday James

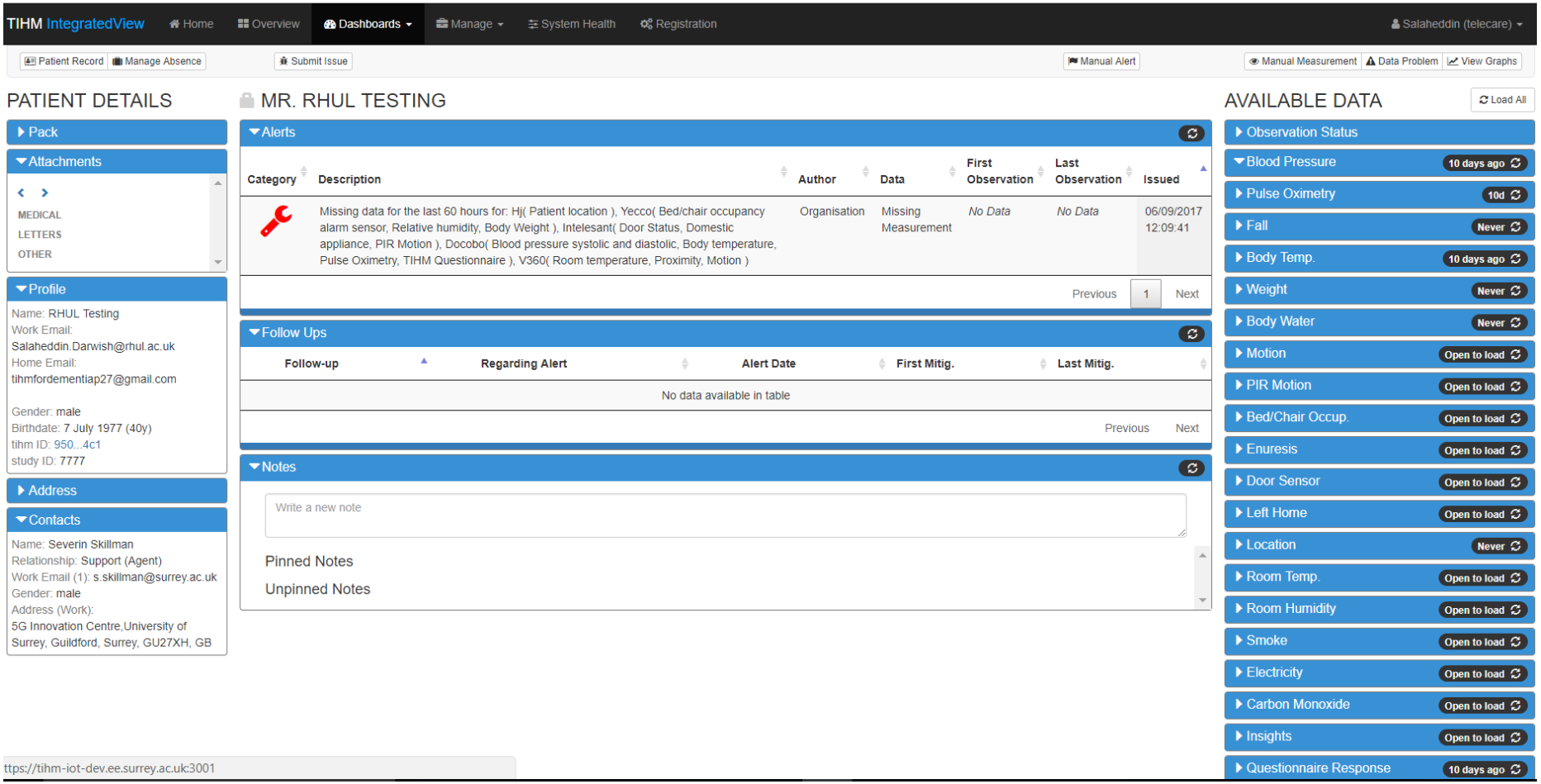


Sensely

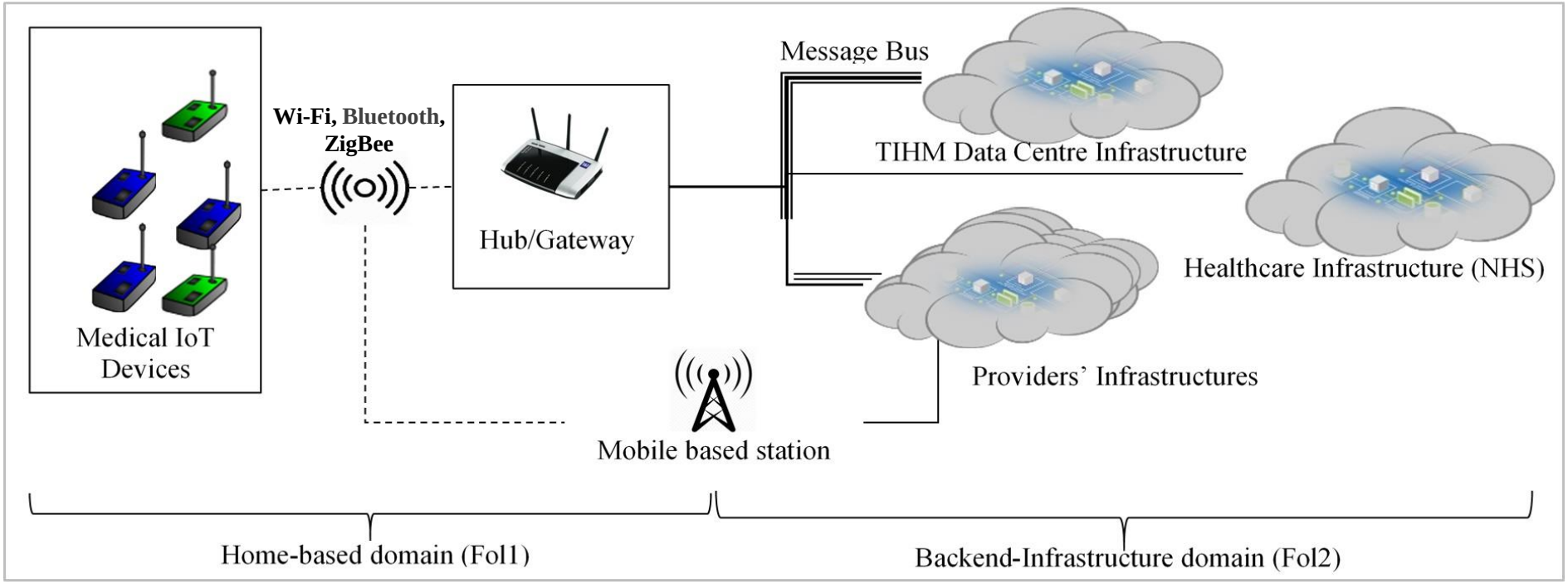

Vision360


Intelesant

TIHM (Integrated View)



TIHM Threat Assessment (Case Study)



The TIHM System Architecture

TIHM threat analysis and availability of composability properties.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Threat Analysis				Availability of Composability Properties
Vulnerability/Attack			Level	Update needed after adding a new IoT
Data Disclosure Group	FoI 1	Unauthorised access to the IoT and Hub\Gateway	Very High	Static
		Eavesdropping	Low	Static
		Home user impersonation	Medium	Static
		Information leakage or release	Low	Dynamic (patient identification by collected data)
	FoI 2	Unauthorised access to TIHM databases/storages.	Very High	Not changed by unless IoT has extra connections
		Unauthorised access to non-secure Cloud services	Very High	Static (checking whether the service is secure)
		Back-end infrastructure user impersonation.	Very High	Not changed by IoT addition
		Cross contamination (from shared resources)	High	Not changed unless a shared storage is used
		Information leakage or release	Low	Dynamic (patient identification by collected data)
Data Alternation Group	FoI 1	Home user impersonation	Medium	Static
		Information corruption or disruption	Medium	Static (for IoT misusage), with possible dynamic elements (comparing records)
		Connection interference	Medium	Dynamic
	FoI 2	Data staleness or non-Freshness	Low	Dynamic (comparing time records)
		Invalid data suppression	Very Low	Static (for IoT misuse), with possible dynamic elements (comparing records)
		Information Injection	Medium	Not changed by IoT addition
		Back-end infrastructure user impersonation	Medium	Not changed by IoT addition
		Cross contamination	Medium	Not changed by IoT addition
Data Inaccessibility Group	FoI1	Energy draining	Low	Static
		Accidental fault	Low	Static
		Network congestion	Low	Dynamic
	FoI 2	Denial of Service (DoS)	Very High	Not changed by IoT addition
		Accidental system failure	Very High	Not changed by IoT addition
Process/Code Manipulation Group	FoI 1	Virus and malware	Very High	Static (for IoT devices) Dynamic (for the network)
		Clock Poisoning	Medium	Static (for IoT misusage), with dynamic elements
		Misconfiguration	Medium	Static (for IoT devices)
	FoI 2	Virus and malware	Very High	Not changed by IoT addition

Conclusion

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Adding new equipment to MIoT may entail cascading effects.
- Considering the composability notion would save time and efforts in performing threat identification.

References

1. A. W. Atamli, A. Martin, Threat-Based Security Analysis for the Internet of Things, in: 2014 International Workshop on Secure Internet of Things, IEEE, 2014, pp. 35–43.
2. P. A. Williams, A. J. Woodward, Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem., Med. Devices (Auckl). 8 (2015) 305–16.
3. IoT Healthcare Market by Component (Medical Device, Systems & Software, Service, Connectivity Technology), Application (Telemedicine, Work Flow Management, Connected Imaging, Medication Management), End User, and Region - Global Forecast to 2022, (2017).
4. Internet of things: Vision, applications and research challenges, Ad Hoc Networks 10 (7) (2012) 1497–1516
5. HMG IA Standard No. 1 & 2 Supplement Technical Risk Assessment and Risk Treatment , issue No 1 Apr 2012, Available at pdf (2012).
6. TIHM (Technology Integrated Health Management) for dementia, Available at SABP <http://www.sabp.nhs.uk/tihm>.

Acknowledgements

This work was supported by Technology Integrated Health Management (TIHM) project2 awarded to the Department of Information Security at Royal Holloway as part of an initiative by NHS England supported by InnovateUK.

Q&A

THANKS

ROYAL HOLLOWAY UNIVERSITY OF LONDON