Trust Management and its application to the Internet of Things (IoT)

9th of December , 2020

George Hadjichristofi

European University Cyprus

Motivation

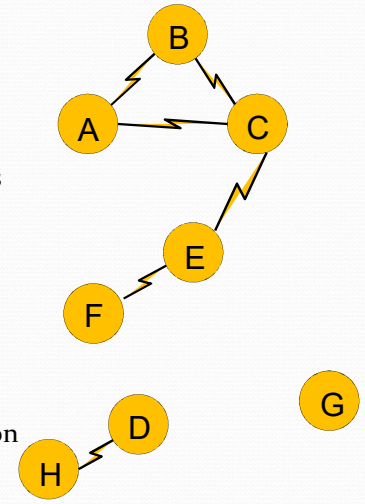
- A vast number of entities (i.e., devices, people, processes etc.) will require to connect to the Internet
  - The Internet of Everything is becoming a possibility
- The development of numerous lightweight communication protocols have enabled connectivity of devices with the outside world
  - real-time monitoring and treatment of patients
- These entities will support critical infrastructures, such as health care

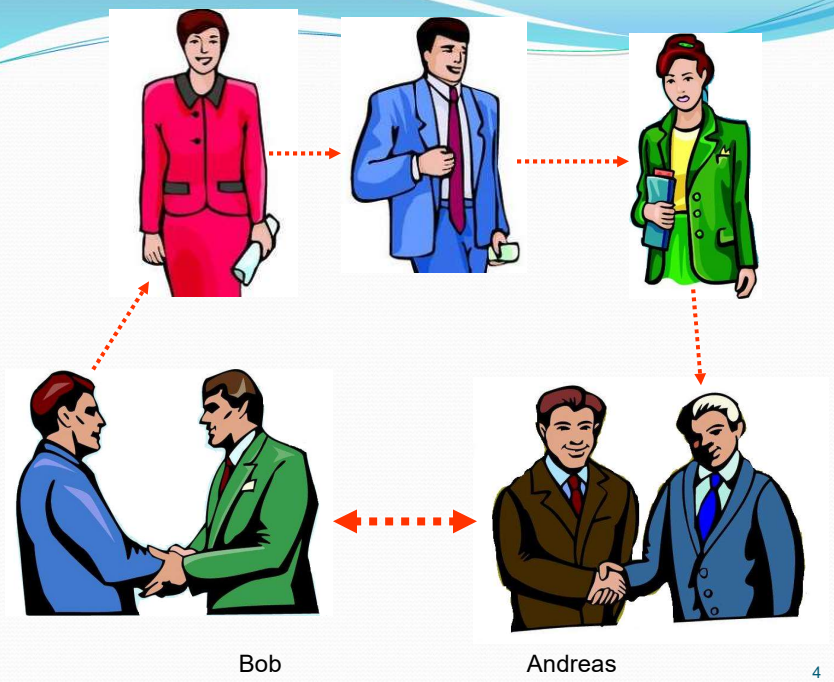
Devices suffer from both technical and environmental constraints

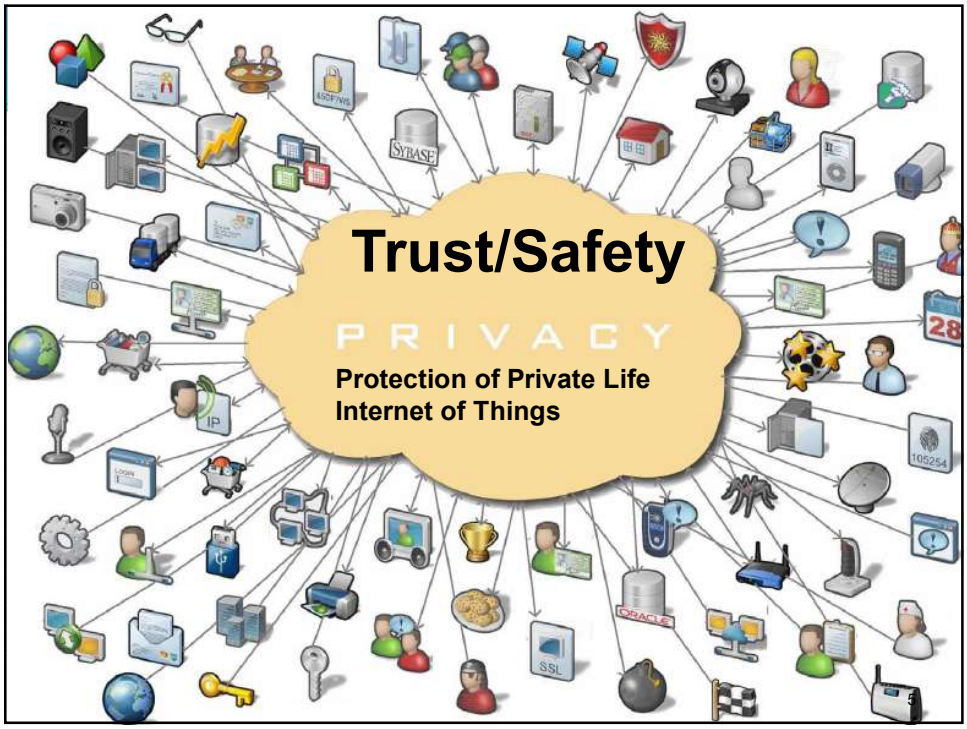
Power limitations
Processing limitations
Bandwidth limitations

Number of attacks through malicious entities has increased exponentially

Need to provide:
Confidentiality, Authentication,
Integrity, Availability, Non-repudiation
Trustworthiness







Authentication vs. Behavior Grading

- Authentication implies some level of trust to exchange secret information
- Need further criteria to assess and visualize TRUST

Motivation

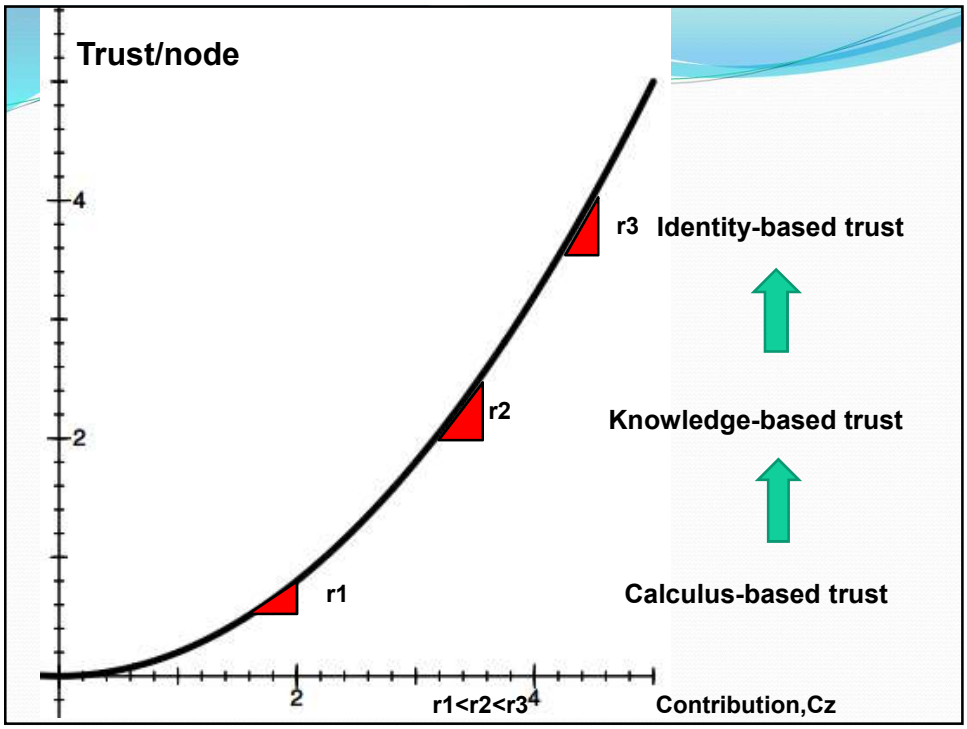
- **Trust should be there for any communication to exist**
- We need to come up with automatic and visual ways of capturing trust
- Trust is linked to behavior which is measured through contribution or Experience
  - A lot of literature on measuring contribution

What is TRUST?

- J.B. Rotter defined interpersonal trust as a generalized expectancy held by an individual that the word, promise, oral or written statement can be relied on
- Hoffman, Lawson-Jenkins, and Blum support that a thorough understanding of both the psychological and engineering aspects of trust is necessary to develop an appropriate trust model
- Activity on the network is linked to human psychology and thus it is a complex aspect
- **To better capture trust we integrate aspects of human psychology and nature in our trust evaluations**

Non linear trust response to contribution

- Lewicki and Stevenson studied trust in social networks
- "Trust does not only increase in magnitude, but also changes in character and becomes more resilient and stronger"
- Trust is developed in three successive stages
  1. namely calculus-based trust – parties are cautious
  2. knowledge-based trust – predictability in behavior
  3. identity-based trust – deeper understanding
- Trust grows in quantity and quality



Typical Evaluations of Trust

- Basic trust grading methods aggregate behavior info by
  - Number of reported events
  - Taking into account the trustworthiness of reporting entities
  - Focusing on imperfect measurements for grading and using game theory
  - Detecting anomalies in network traffic
- For this presentation, the focus is not on the validity of reported events, or the trustworthiness of reporting entities or approximations of valid input

IoT Scenario

- In this work we investigate the scenario of IoT deployment in hospitals to monitor and assist in-hospital patient care
- We introduce the notion of trust grading of Things to assess the trustworthiness of entities for patients progress.
- Trust grading is done at
  - the individual and
  - group level

Medical Devices based IoT

- Medical Devices have been defined in the classification procedure of the Code of Federal Regulations, (21 CFR 860) and Council Directive 93/42/EEC on Medical Devices
- Categories (classes) of devices have been established, defining the regulatory controls required to ensure safety and effectiveness

Healthcare Networks

- Such networks can introduce threats, and vulnerabilities on device / network functionality and end users/patients
- The integration and operation of such wireless medical devices in a hospital environment dictates that
  - threats and vulnerabilities must be identified
  - risk levels must be determined and
  - suitable mitigation strategies must be introduced
- It is becoming increasing important to evaluate the trustworthiness of entities on a patient

Contribution

- Based on our proposed methodology, a GUI is implemented
  - allows for the visualization of malicious or irregular IoT behavior and
  - the dynamic calculation of trustworthiness.
- Weights are assigned to different sensing nodes

Key Aspect

- The focus is on the methodology of presenting and processing information and not on **validating malicious activity** to assess trust
- This methodology complements work of other researchers by
  - providing a visual means to assess trust
  - introducing a human-like perception of trustworthiness of entities

Assumptions

- We assume that our **data represent misbehaviour based on deviations from the expected behaviour regardless of whether**
  - **it is intentional/malicious or**
  - **affected by some sort of failure (functional)**
- Based on the fact that misbehavior decrease the trustworthiness of an individual then trust is expressed as a **negative value**
- If positive contribution/behavior exists then it is expected that the trust value could switch to a positive value.

Terminology

- Entity :

Any item in the future Internet will be composed of devices or Things, people, or processes, i.e., the Internet of Everything

Scenario Development Hospital Environment 1/2

- We assume that monitors are installed on patients that would use wireless communication
  - facilitate aspects of patient mobility, or
  - daily care of the patient.
- A hospital room typically has 1-4 patients
- A series of (wireless) sensors on patients
  - the blood pressure monitor, the pulse oximeter, an end tidal CO_2, Capnogram, brain activity sensors (EEG), eye movements sensors (EOG), muscle activity or skeletal muscle activation (EMG) sensors, and heart rhythm (ECG) sensors.

Scenario Development Hospital Environment 2/2

- Sensors will send information to a centralized server that will assess the patient's health and assist the nurse/doctor in taking care of the patient.
- Devices could periodically fail due to functionality aspects of the device or due to malicious activity.
  - **Functionality:** hardware malfunctions of the device, low battery issues, or interferences in the communication channel
  - **Malicious activity:** alter the data or disrupt the transfer of data, such as during jamming attack.

Assessing the behaviour

- Unable to differentiate between a malfunction or a malicious event
- Consideration:
  - The lack of reception of periodic input from a device could indicate that the device is malfunctioning or that there is a jamming attack.
- Both pose a risk on a patient's health due to unreliable operation
- Both are taken into account in our trust calculations.

Use Generic and Device Specific metrics

- Generic metrics capture aspects such as lack of reports or non-timely reports
  - can be an aggregation of the number of events not reported within a pre-specified period
- Device specific metrics compare the data that the device measures to the **normal data** set, or to the **expected** data set
  - **Expected data** depends on the type of patient illness involved.
  - **For example**, a person who smokes has 10% lower oxygen content in his blood as opposed to a non-smoking person.

Aggregating the abnormal behavior of a device (Eq.1)

- Weight, W_1 for generic and (1 – W1) device specific abnormal activity over a period of time.
- Weights account for the fact that certain device specific events were more critical (e.g. extremely unrealistic measurements) as opposed to generic events (e.g. lack of reports for a short period of time).

$$\text{Abnormal}_{\text{Activity(t)}} = W_1 \times \sum_{1}^{n} Gen._{events} + (1 - W_1) \times \sum_{1}^{n} DS_{events} \quad (1)$$

Recidivism and Forgiveness

- Recidivism is the tendency of a hacker to engage again in hacking activity
- Recidivism may imply some form of addiction
- Convicted hackers may undergo some form of treatment that may make them stop any malicious activity

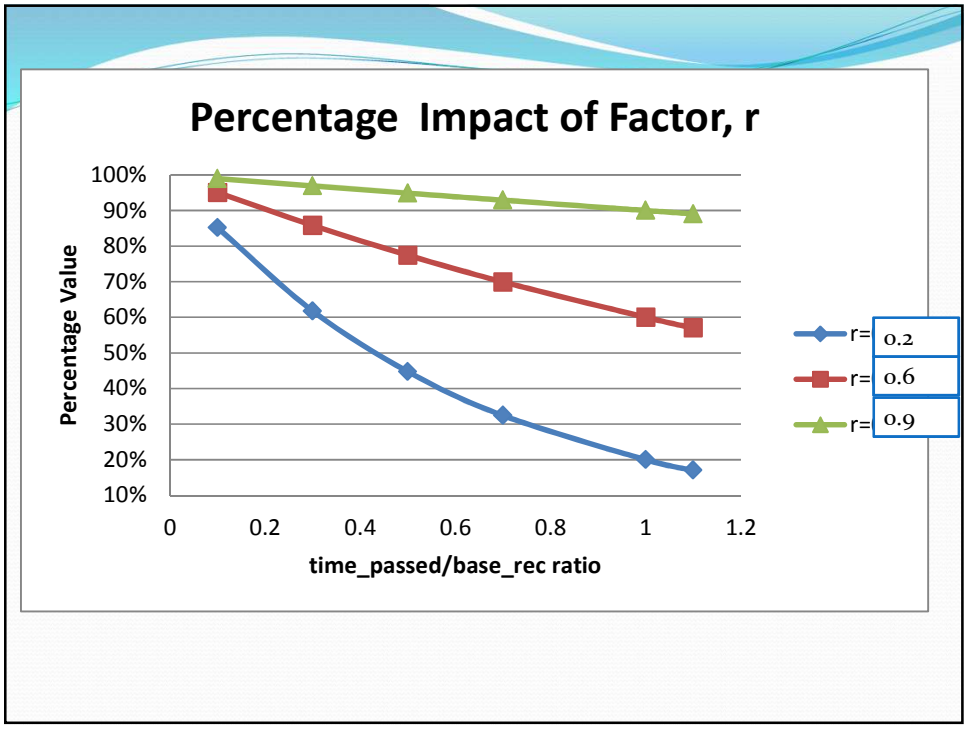
Properties of Forgiveness

- Forgiveness is the notion of improving an entity's trust if that entity has not been misbehaving for a period of time
- Humans may not repeat an offence, or as they may have found other interests

Adapting Property of Forgiveness in this work

$$\text{Trust}(t) = r^{\frac{time\_passed}{base\_rec}} * \text{Trust(t−1)}$$

- r controls the rate of forgiveness,
- *base_rec*, the time it takes to improve trust by reducing a negative trust value to r % (e.g., 1 week or 1 month)
- *time_passed* the time passed since the previous record of an abnormal activity



Existing Trustworthiness Matters

The underlying intention of an entity to harm or cause damage varies based on its existing trustworthiness

Incorporating Existing Trustworthiness of nodes

- **Punishment in real life should be linked with the type of person someone is in terms of trustworthiness**
- An individual who keeps attacking entities and already has a low level of trust should be punished more if he attacks again.
- An individual who has only deployed one attack and is relatively more trustworthy should be penalized much less when he deploys another attack
- **Harsher punishment for attackers with a very bad attack record and vice versa**

Adapting Property of Existing Trusting in this work

- We **utilize abnormal activity** to adjust trust
- Uses *log* as a means of adjusting the punishment based on the existing trust of an entity.
- Log_2 was used to enforce a harsher punishment

$$\Delta Trust = Log_2^{Trust\_Discount(t)} \times Abnormal\_Activity(\mathrm{t}) \quad (3)$$

$$\mathrm{Trust(t)} = Trust(t-1) - \Delta Trust \quad (4)$$

Group Trust

- Typical approaches focus on individual trust
- A number of devices can be installed on a patient
- We introduce the idea of group trust

- Assess the trustworthiness of a set of devices that represent a specific patient

- Indirectly, group trust reflects the associate risk in properly assessing a patient's health in the presence of misbehaviour

Introducing weights to calculate Group Trust

- To properly calculate group trust we introduce the idea of device specific weighted trust based on the sickness treated.
  - Input from one device may be more critical as opposed to another (e.g., oxygen sensor vs. temperature sensor).
  - To calculate trust activity of all sensors on a patient the value of a device is multiplied by a specific weight, such that $w1+w2+w3+...w_n=1$.
- **Trust_activity** af all sensors per patient is calculated

History of Activity for Group Trust

- Use weighted moving average methodology with weights *a*, *b*, and ***c*** being adjusted to give more emphasis to recent activity
- Trust_activity is the aggregated activity of all sensors on a patient

$$Group\_Trust = (a \times Trust\_Activity_n) + (b \times Trust\_Activity_{n-1}) + (c \times Trust\_Activity_{n-2}) \quad (5)$$

- The weighted trust values of all the devices can then be plotted on a graph

System Implementation - **Two pieces** of software were created

- A data generator that generates random abnormal activity for devices
  - random periods of time based on random lower and upper limits for the time between events.
- The type of activity is either generic or device specific
- The quantity for each activity is controlled based on preassigned weights per sensor per patient

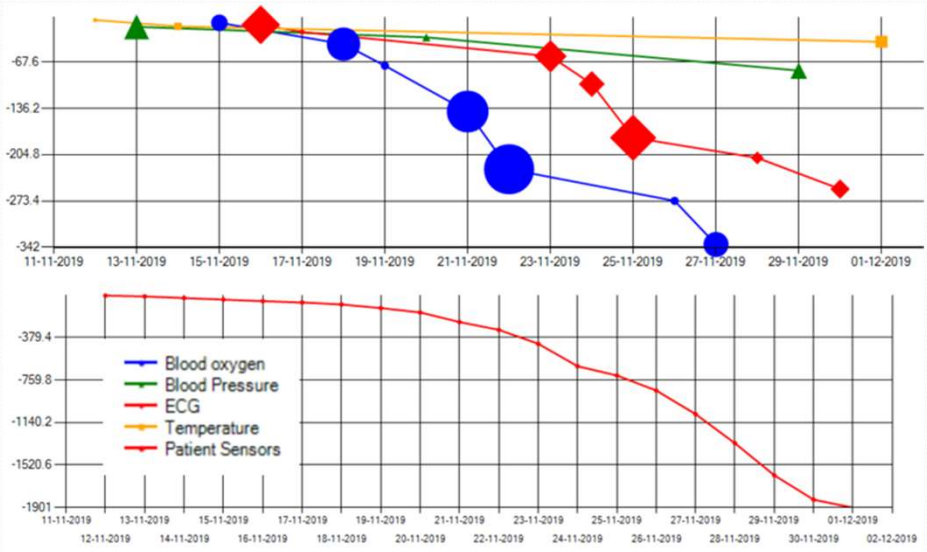
Second Software: A GUI

- Built using C#, Windows Forms, and the Chart Class to generate graphs
- Accepts as input the data generated from our data generator
- In the future it is envisioned that data could be introduced dynamically from Things as they are aggregated.
- The trust GUI presents information in 2 different graphs

Second: A GUI – Top Graph

- The top graph presents the activities occurring per device over time (x-axis)
- The y-axis presents the associated trust value of the devices as it dynamically changes and is calculated using (4).
- Different shape markers are used per device.
- The size of the markers reflects the volume of the abnormal activity.
- The user can select whether the forgiveness rate is "Conservative", "Normal", or "Relaxed".
  - achieved by varying the variable *r* in (2)

Trust and abnormal activity per device and respective group trust



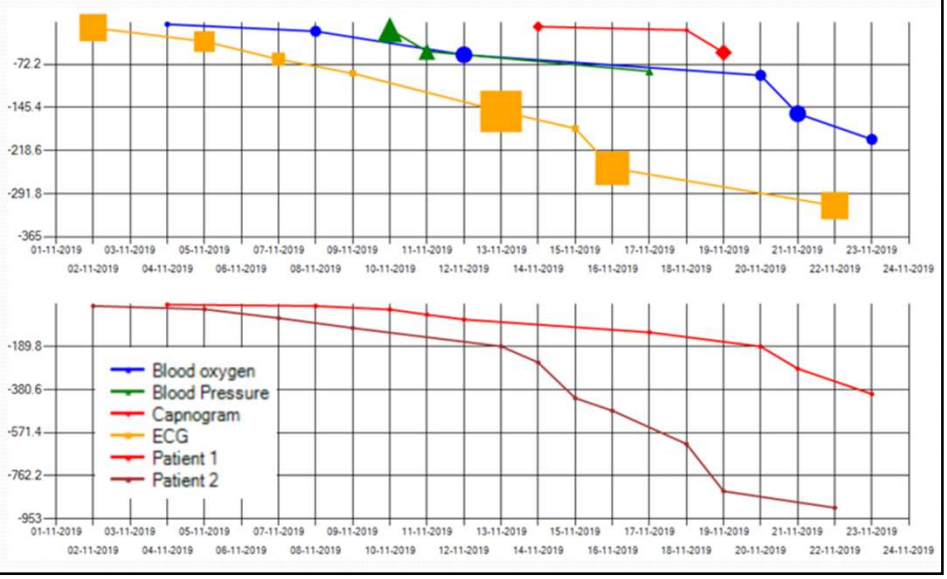
Second: A GUI – Bottom Graph

- We capture the trust fluctuations of all devices for the all data series
  - Indicates the change on the trust level of a group of devices over time.
- This graph takes into account the weighted trust values of each device based on their criticality
  - For this example we used a weighted moving average of a=0.6, b=0.3, and c=0.1

Discussion

- A low number of abnormal activity is shown by a line that is almost horizontal indicating more trustworthy devices.
- More abnormal activity makes the line move downwards to a more negative value of Trust making them less trustworthy
- For the **group trust graph**, the trust values taken have been weighted with
  - **ECG 0.5**, Blood oxygen sensor 0.3, rest 0.2 weight value
  - it can be observed that the graph resembles more the behavior of the ECG sensor with the higher weight

Graphs for 2 patients



Plotting for 2 patients

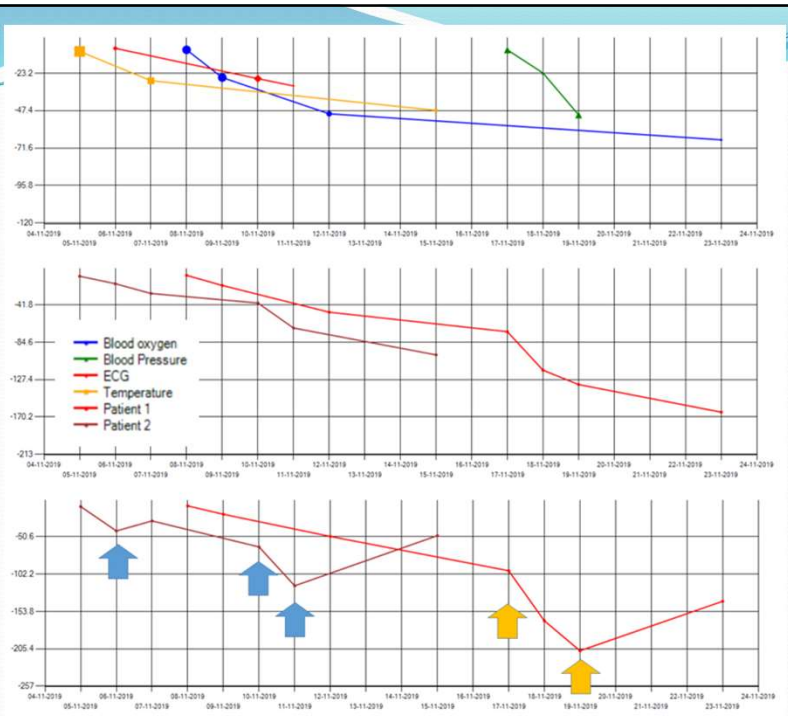
- Patient 1 has a blood oxygen device and a blood pressure device
- Patient 2 has the Capnogram and an ECG device.
- Devices on Patient 1 are more trustworthy than Patient 2 devices
- It raises questions with regards to the **risk imposed** on the Patient 2 due to his untrustworthy devices

Weights on specific devices impact the trust graph 1/2

- The top graph shows the abnormal activity of all sensors with associated trust graphs.
- The middle graph shows the group trust graphs without any weights assigned to specific devices
- The bottom graph shows the group trust graphs with weight activated
  - **Patient 1** Blood oxygen device (green line) and a Blood Pressure device (blue line)
  - The Blood Oxygen device trust is more heavily weighted as it is considered more critical and imposes higher risks to the patient's health

Weights on specific devices impact the trust graph 2/2

- **Patient 2** has an ECG device (red line) and a Temperature device (orange line)
- The ECG device trustworthiness is more heavily weighted as opposed to the Temperature device
- Middle graph shows group trust graphs that are smoother as opposed to the bottom one
- Bottom Graph shows sudden decreases in group trust
  - orange arrows for Patient 1 and the blue arrows for Patient 2.
  - This is due to the more heavily weighted devices



Challenges for Trustworthiness

- The analysis presented tied specific types of devices to specific patients for group trust assessment
  - Different combinations of sensors per patient could exist depending on the treatment
- Over time a device could be used on many patients.
  - Can the trustworthiness of a device be carried from one use to another?
  - What part of history can be maintained?

Conclusion 1/2

- Trust is a property that is difficult to quantify but very much needed
- It's application can extend to any entity (people, processes, data items, embedded devices, etc.)
- This research has been used to investigate trust for the scenario of IoT deployment in hospitals, to monitor and assist in-hospital patient care

Conclusion 2/2

- We differentiate between the different types of abnormal behaviour based on the type of the malfunction
  - Functional vs. device specific
- Integrate Forgiveness
- Integrate Existing Trustworthiness

- We create this idea of group trust that indirectly represents the risk imposed on a patient's health
  - Weight differently more critical sensors

Future Work

- We aim to investigate more complex scenarios involving different combinations of sensors

- Integrate this system into a bigger architecture that provides security and redundancy in assessments, such as through blockchains

Ευχαριστώ!
Thank you !

George Hadjichristofi
g.hadjichristofi@euc.ac.cy

European University Cyprus

49