Risk-Based Adaptive Security for Smart IoT in eHealth

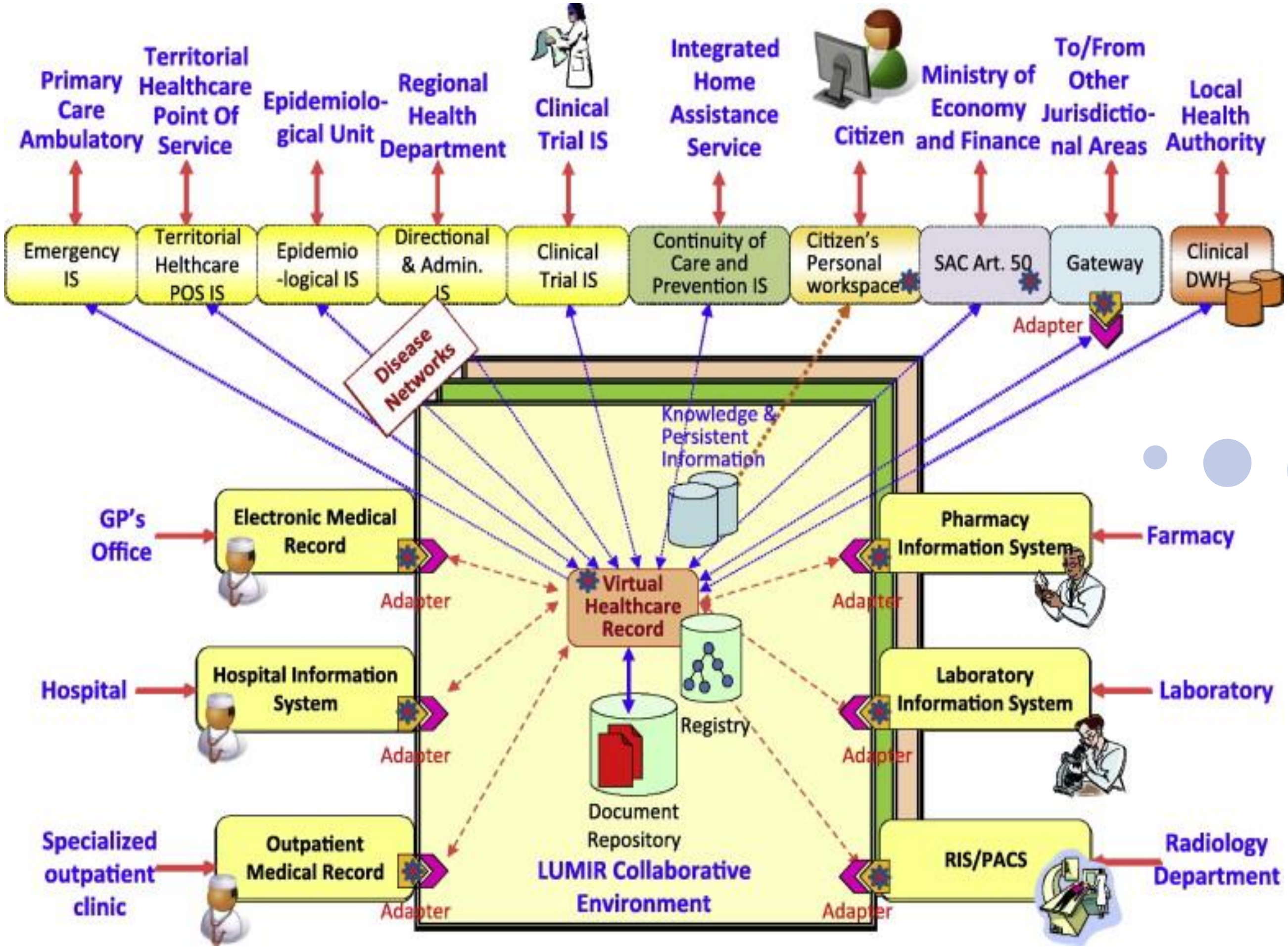
Habtamu Abie[1], Ilangko Balasingham[2]
[1]Norwegian Computing Center
[2]The Intervention Center, Oslo University Hospital

SeTTIT Workshop
Oslo 26/09-2012

Risk-Based Adaptive Security for Smart Internet of Things (IoT) in eHealth

- Digital Health Ecosystems and IOT
- IoTs simplify everyday life and improve quality of lives, are also vulnerable to attacks
- Adaptive risk management can change the future
- Game theory allows modeling conflict and cooperation between players
- Proposed Risk-based Adaptive Security Framework
- Case Study: Patient Monitoring
- Conclusions and Future Work

Digital Health Ecosystems create digital environments for networked health organizations



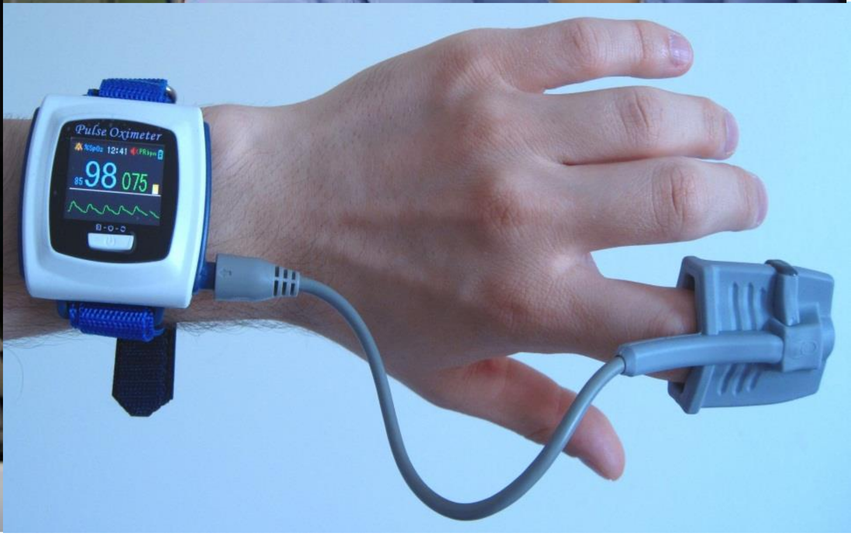
Primary Care Ambulatory
Territorial Healthcare Point Of Service
Epidemiological Unit
Regional Health Department
Clinical Trial IS
Integrated Home Assistance Service
Citizen
Ministry of Economy and Finance
To/From Other Jurisdictional Areas
Local Health Authority
Emergency IS
Territorial Helthcare POS IS
Epidemio-logical IS
Directional & Admin. IS
Clinical Trial IS
Continuity of Care and Prevention IS
Citizen's Personal workspace
SAC Art. 50
Gateway
Clinical DWH
Adapter
Disease Networks
Knowledge & Persistent Information
GP's Office
Electronic Medical Record
Adapter
Virtual Healthcare Record
Pharmacy Information System
Farmacy
Adapter
Hospital
Hospital Information System
Adapter
Registry
Laboratory Information System
Laboratory
Adapter
Document Repository
Specialized outpatient clinic
Outpatient Medical Record
Adapter
LUMIR Collaborative Environment
RIS/PACS
Radiology Department
Adapter

Source: L. D. Serbanati et al., Steps towards a digital health ecosystem, Journal of Biomedical Informatics, 44(4), August 2011, 621–636

IoT is one of the building block of the digital health ecosystem

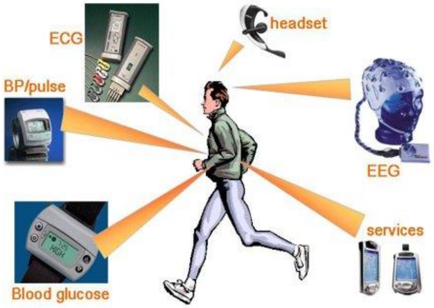
IoT connects a large number of things to simplify everyday life

Sensewear



IoTs improve quality of lives

- ► IoTs improve the quality of our lives at home, while travelling, when sick, at work, when jogging, and/or at the gym.
- ► IoTs in eHealth can be used to track objects and people (staff and patients), identify and authenticate people, collect and sense data automatically



Source:
Digital Medicine

IoTs are vulnerable to attacks

- communications are mostly wireless
- unattended things are usually vulnerable to physical attacks
- most IoT components are constrained by energy, communications, and computation capabilities

necessary for the implementation of complex security-supporting schemes

Current IoT security models are not flexible

- Most current security models and mechanisms are hard to change, reuse, and analyze
- Making infrastructures inflexible, lost investments, and damages resulting from mechanisms not matching the changing threats

Security and privacy

- Security and privacy
  - How do we trust the data our sensors are sending?
  - In fact how do we even know it is a sensor that is sending data at all, and not a bot or piece of malware?
  - One of the key issues is therefore data integrity that also involves authentication, access control and secure communication

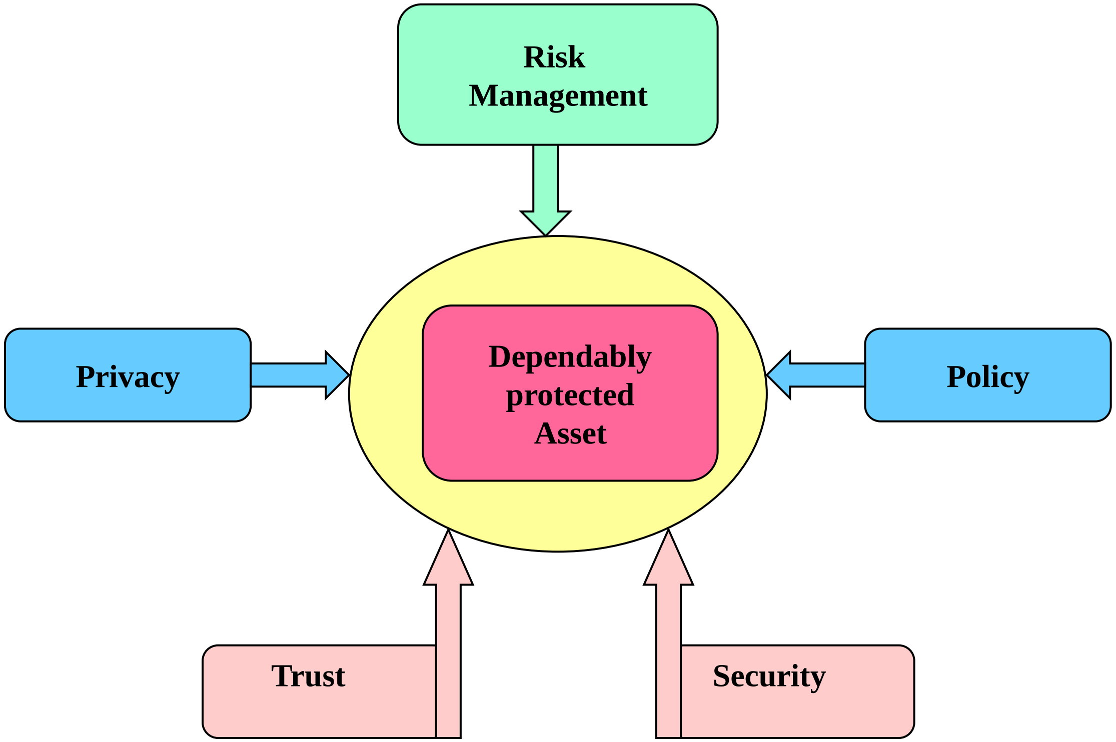
- Some types of modern IoT applications require instant adaptation their security mechanisms due to their exposure to increasing situational dynamics

Adaptive risk management can change the future and maximize the value of taking risk

- Adaptive risk management learns, adapts, prevents, identifies and responds to new or unknown threats in critical time, much like biological organisms adapt and respond to threats in their struggle for survival

- Thus, “the purpose of risk management is to change the future, not to explain the past” - Dan Borge

- The moral is to maximize the value of taking risk

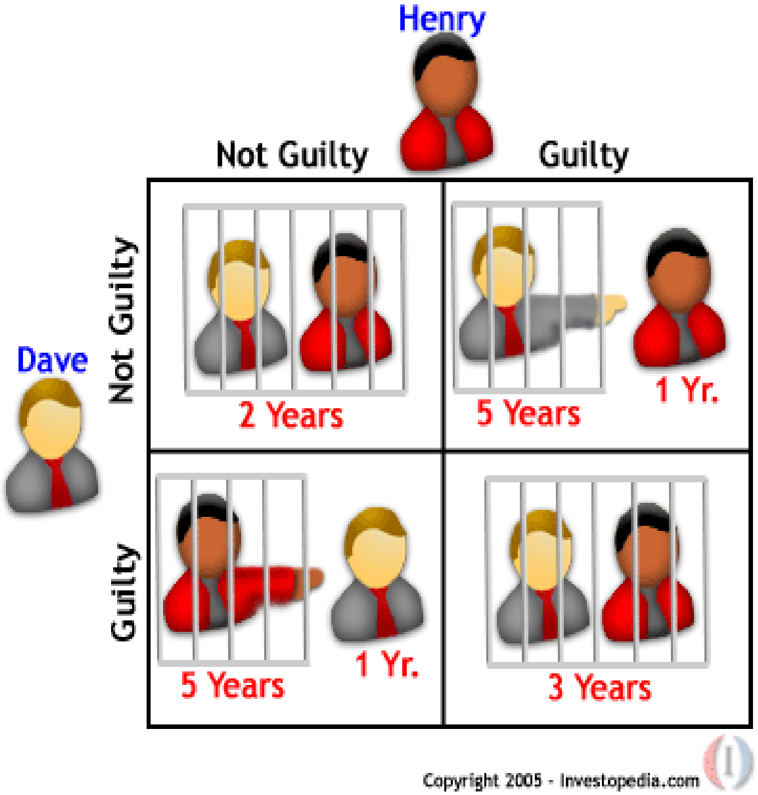


Risk management holds the key to managing security and privacy

- Risk-based adaptation
  - sensitive access could be authorized according to the measured risk
  - measurable risk to strengthen the security of IoT systems
- Risk-based adaptation implements quantified risk adaptive security solutions
  - measuring risk,
  - establishing an acceptable risk level, and
  - ensuring that the information is used, accessed and distributed all the way up to the acceptable risk level.
- Self-adaptiive risk-based protection
  - automatically adjust the settings and actions to satisfy sensitivity and protection requirements of the new operating conditions

Game theory allows modeling conflict and cooperation between two or more players

- ► Game-theoretic formulations of attack-defense conflicts can greatly improve risk analyses that attempt to model attacker decisions as random variables or uncertain attributes of targets (“threats”).
- ► Game theory can produce more sensible and effective risk management recommendations for allocating defensive resources than current risk scoring models.



Source: V. M. Bier and M. N. Azaiez, Game Theoretic Risk Analysis of Security Threats, Springer, 2008, 236 pages.

Alignment of ISMS, ISRM and ASSET

Information Security Management System (ISMS) Process	Information Security Risk Management (ISRM) Process	ASSET Adaptive Risk Management Process/Methodology
Plan	Establishing the context Risk assessment Risk treatment planning Risk acceptance	Analyze (Plan)
Do	Implementation of risk treatment plan	Adapt (Execute)
Check	Continual monitoring and reviewing of risks	Monitor
Act	Maintain and improve the Information Security Risk Management Process	Adapt (Learn)

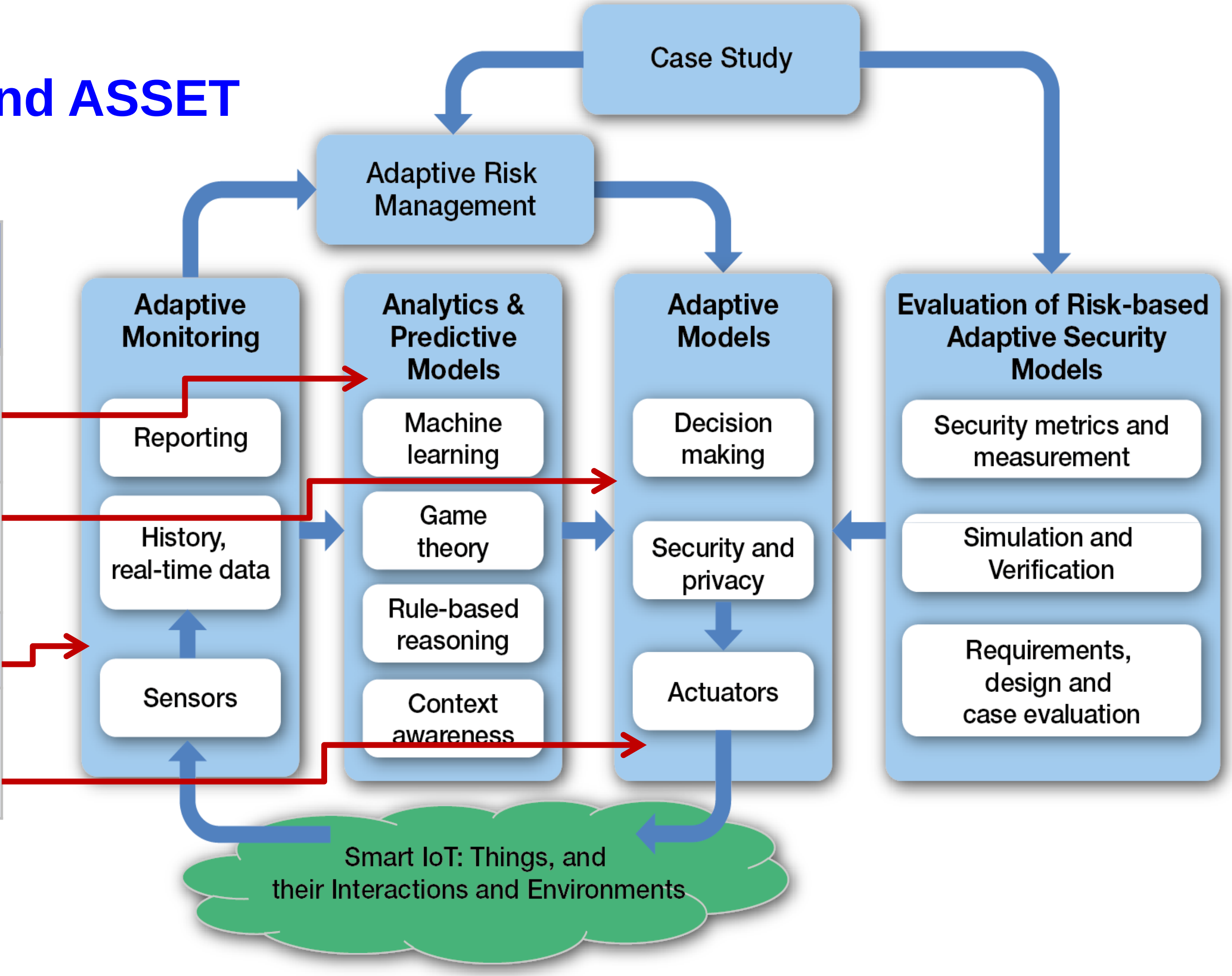
ISO/IEC 27005:2007

ASSET: Monitor-Analyze-Adapt (plan, learn, execute)

Proposed Risk-based Adaptive Security Framework

Alignment of ISMS and ASSET Processes

ISMS Process	ASSET Process
Plan	Analyze (Plan)
Do	Adapt (Execute)
Check	Monitor
Act	Adapt (Learn)


Case Study
Adaptive Risk Management
Adaptive Monitoring
Reporting
History, real-time data
Sensors
Analytics & Predictive Models
Machine learning
Game theory
Rule-based reasoning
Context awareness
Adaptive Models
Decision making
Security and privacy
Actuators
Evaluation of Risk-based Adaptive Security Models
Security metrics and measurement
Simulation and Verification
Requirements, design and case evaluation
Smart IoT: Things, and their Interactions and Environments

Adaptive Risk Management estimates and predicts risks and impacts

- Adaptive risk-based security models estimate and predict security and privacy risks and future benefits and base their decisions dynamically
  - models for accurately predicting future events and adapting accordingly
  - adaptation causing minimal deviations from normal operation
  - enabling adaptation across multiple time scales
  - where and how much risk to take
  - could risk damages be controlled

Adaptive Security Monitoring model monitors context and status of IoTs

- The ASM is utilized for obtaining automated technical evidence for the purposes of continuous operational security monitoring of IoTs.
- It is adaptive with a continuous cycle of monitoring of the information about context and status of the smart IoTs which is exploited at runtime in the adaptation process.
- It uses security measurement and metrics for quantitative measures by which IoT security solutions can be evaluated

Analytics and Predictive Models analyze and prioritize decision making activities

- use game theory and context awareness to understand and prioritize the decision making activities.
- improve the accuracy of estimation and prediction mechanisms by applying optimized machine learning and rule-based algorithms
- increase the ability to precisely predict and measure the risk of damages and future benefits and adapt security decisions upon those predictions
- improve the light-weight abilities of smart things by improving their context-awareness and self-abilities

Adaptive Security Decision-Making Models adapt to the dynamism of Things

- adapt to the dynamism of Things, their interactions, and the environment, and to the varying degrees of risk that the IoT eHealth system will be compromised

- optimize algorithms for different IoT processing capabilities to detect in real-time unknown security and privacy threats

- respond to threats, and adapt to the environment and changing degree of security and privacy breaches

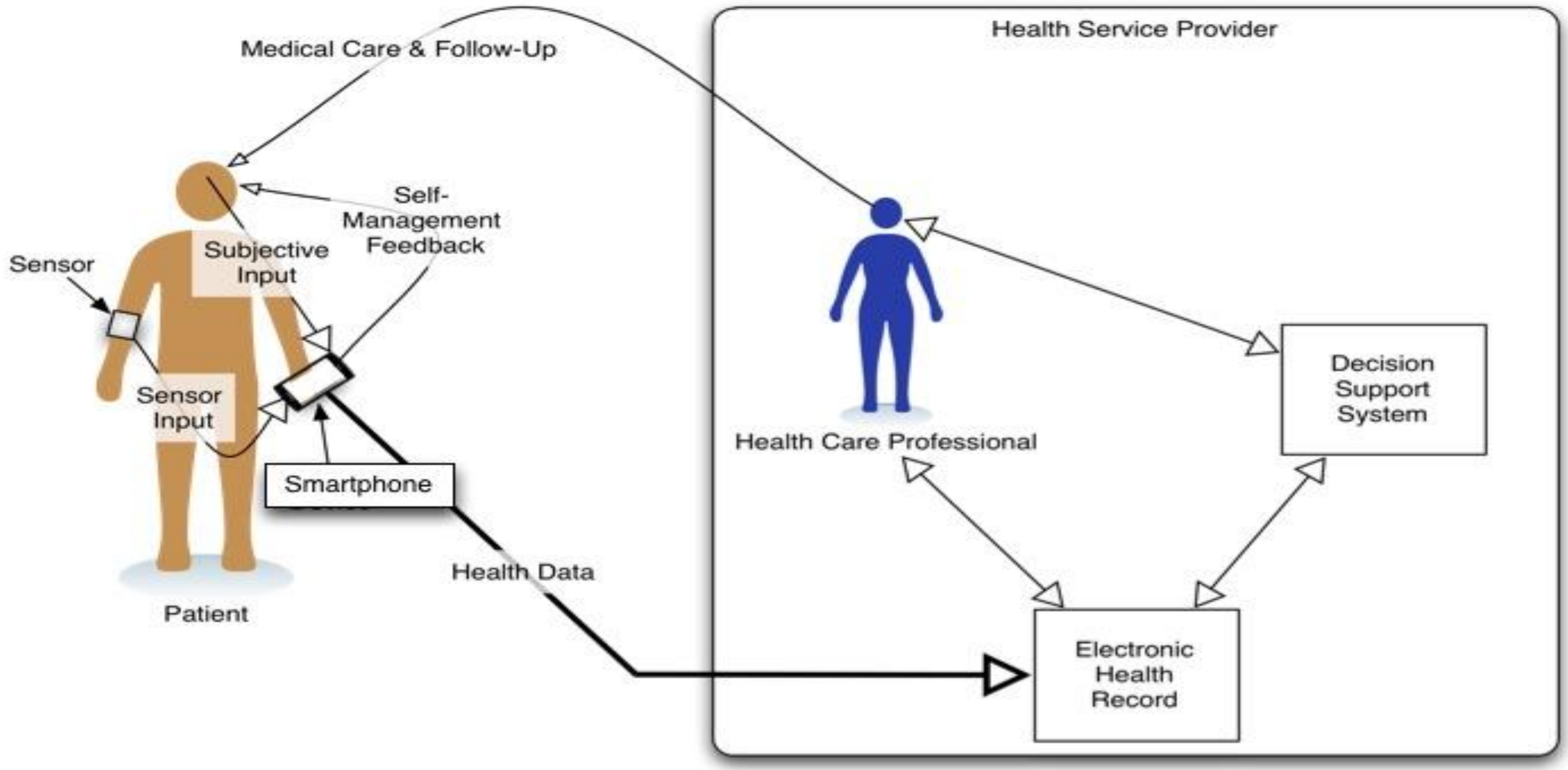
Adaptive Security Decision-Making Models learns adapt to changing IoT

- It does this by
  - combining adaptive risk-based decision model, adaptive security and privacy models, and actuators to make effective adaptive reaction, and
  - integrating different metrics for validation and verification, adaptive risk assessment, and predictive analytics models for estimation and prediction of security and privacy risks and impacts

Evaluation and Validation Models

- Security Measurement and Metrics are needed for evaluating and validating the run-time adaptivity of IoT security solutions
- Predictive simulation and verification based security metrics can help to understand trade-offs between different solutions by varying assumptions on threats and requirements
  - to select better metrics that are risk indicators of current and future IoT security risks, and to provide a variety of benefits to decision-makers

Case Study: Patient Monitoring



Things include smart phones, tablets, sensors, sensor nodes, and actuator nodes.

Case Study: Patient Monitoring

- Patient monitoring systems are a major data source in healthcare environments
- It is important these systems maintain a certain level of availability, quality of service (QoS), security and the protection of privacy of the patient
- Blood pressure, electrocardiogram (ECG) and heart rate
- Two different scenarios such as home and hospital environments, where different QoS metrics and adaptive security methods and mechanisms will be analyzed using game theory

Case Study: Overhead cost analyses

- The analysis will also include the overhead cost of processing complexity on sensor nodes due to readjustment of the predictive models and adaptive security regime
- The overhead cost of additional data transmission due to transmission on the feedback channels will also be analysed
- The study will provide the tradeoff between desired QoS and security in bandwidth limited, battery driven wireless sensor networks

Conclusions

- An innovative risk-based adaptive security framework for IoT in eHealth to estimate and predict risk damages and future benefits, and to identify unknown threats to IoT eHealth systems has been introduced.
- The framework consists of a continuous cycle of adaptive risk management, adaptive security monitoring, predictive analytics, automated adaptive decision-making, and evaluation and validation metrics.

Future work

- Further development and prototyping of the components of the framework and validating the effectiveness of the adaptation
- Improvement light-weight abilities in smart things that will allow them to detect in real-time unknown security
- Validation of the results in a simulated eHealth patient monitoring scenarios

Thanks!

Habtamu Abie[1], Ilangko Balasingham[2]
[1]Norwegian Computing Center
[2]The Intervention Center, Oslo University Hospital

ADAPTIVE SECURITY FOR SMART INTERNET OF THINGS IN EHEALTH
ASSET

The Research Council of Norway

SeTTIT Workshop
Oslo 26/09-2012

The End!