

METRICS-DRIVEN SECURITY OBJECTIVE DECOMPOSITION FOR AN E-HEALTH APPLICATION WITH ADAPTIVE SECURITY MANAGEMENT

Reijo M. Savola¹, Habtamu Abie²

¹ VTT Technical Research Centre of Finland, Finland

² Norwegian Computing Center, Norway



Teknologiasta liiketoimintaa



ASPI 2013

Zürich, Switzerland

CONTENTS

- Introduction
- From Security Objectives to Metrics
- Proposed Decomposition Strategies
- Use of Security Metrics to Adaptive Security Management
- Conclusions and Future Work



"An activity cannot be managed well if it cannot be measured."

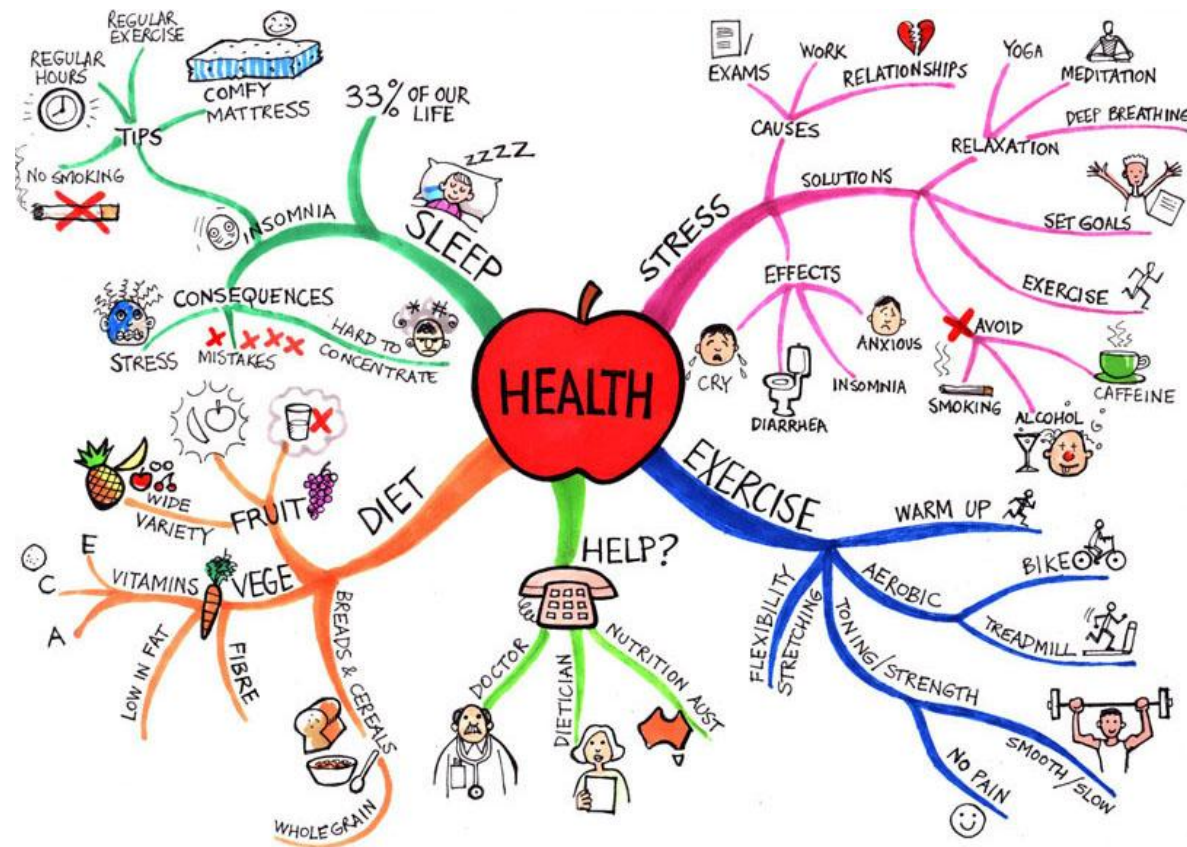
INTRODUCTION

Number of people with chronic diseases on the rise

- Diabetes: rising from 171 million (2000) > 366 million (2030) according to WHO
- COPD: (Chronic Obstructive Pulmonary Disease), rising, major cause of chronic morbidity and mortality worldwide
- Arthritis: rising

Immediate and effective preventive actions are needed to reverse the trend!

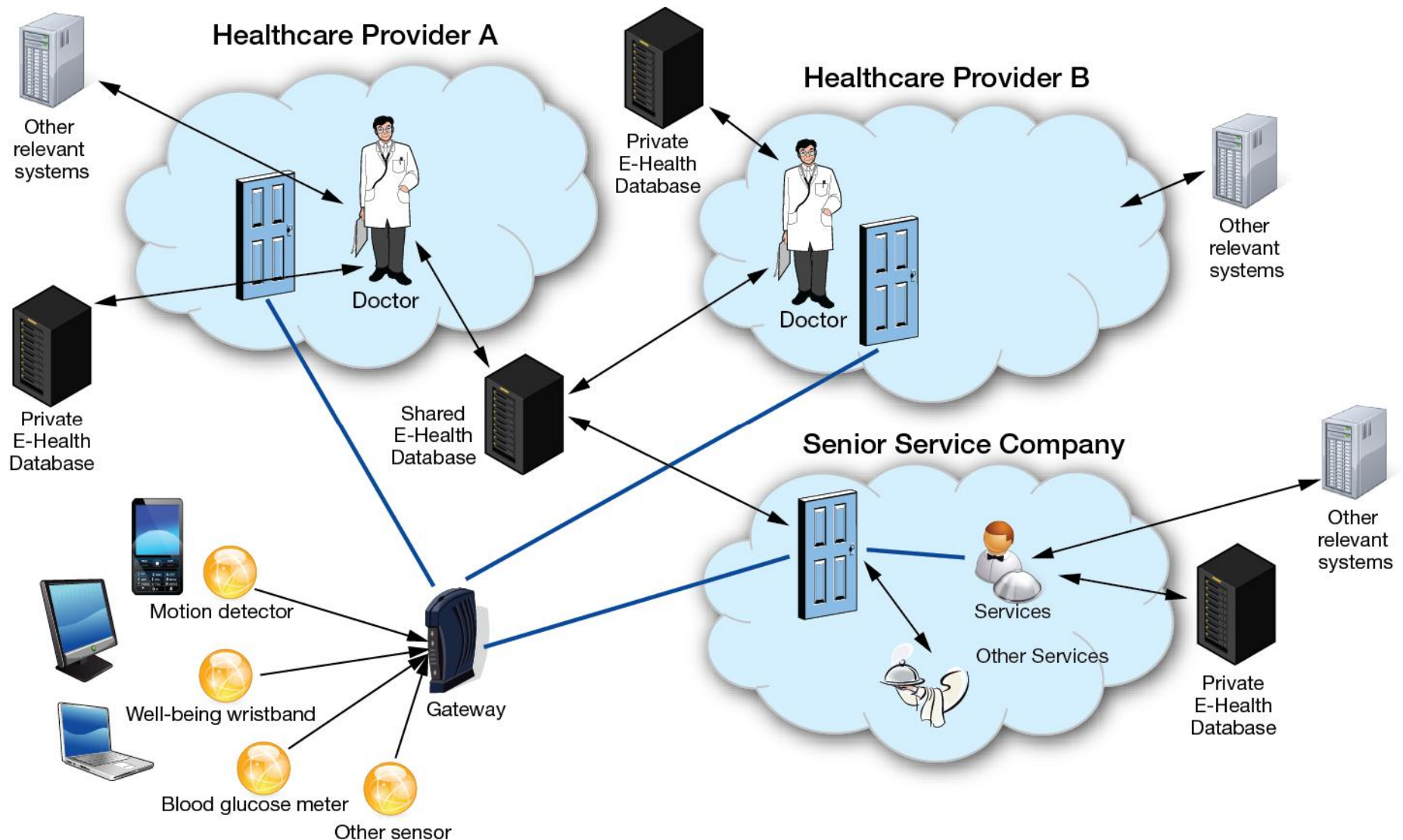
- Self-care support by technology is very promising direction!



Learningfundamentals.com.au/resources/

INTRODUCTION

Use of IoT technology in self-care



INTRODUCTION

Communication Levels / Security Domains

CLs	Description
0	Patient
I	Personal sensor network
IIa	Paramedic scenarios
IIb	Smart home scenarios
IIc	Mobility
IId	Intensive care or surgery
IIE	Pre- or postoperative sensor data management
III	Healthcare information system comprising the hospital network, computing facilities, databases and access terminals in the hospital
IVa	Communication between healthcare providers
IVb	Communication between healthcare provider and research

FROM SECURITY OBJECTIVES TO METRICS

Iterative Risk Analysis, Gaps and Biases

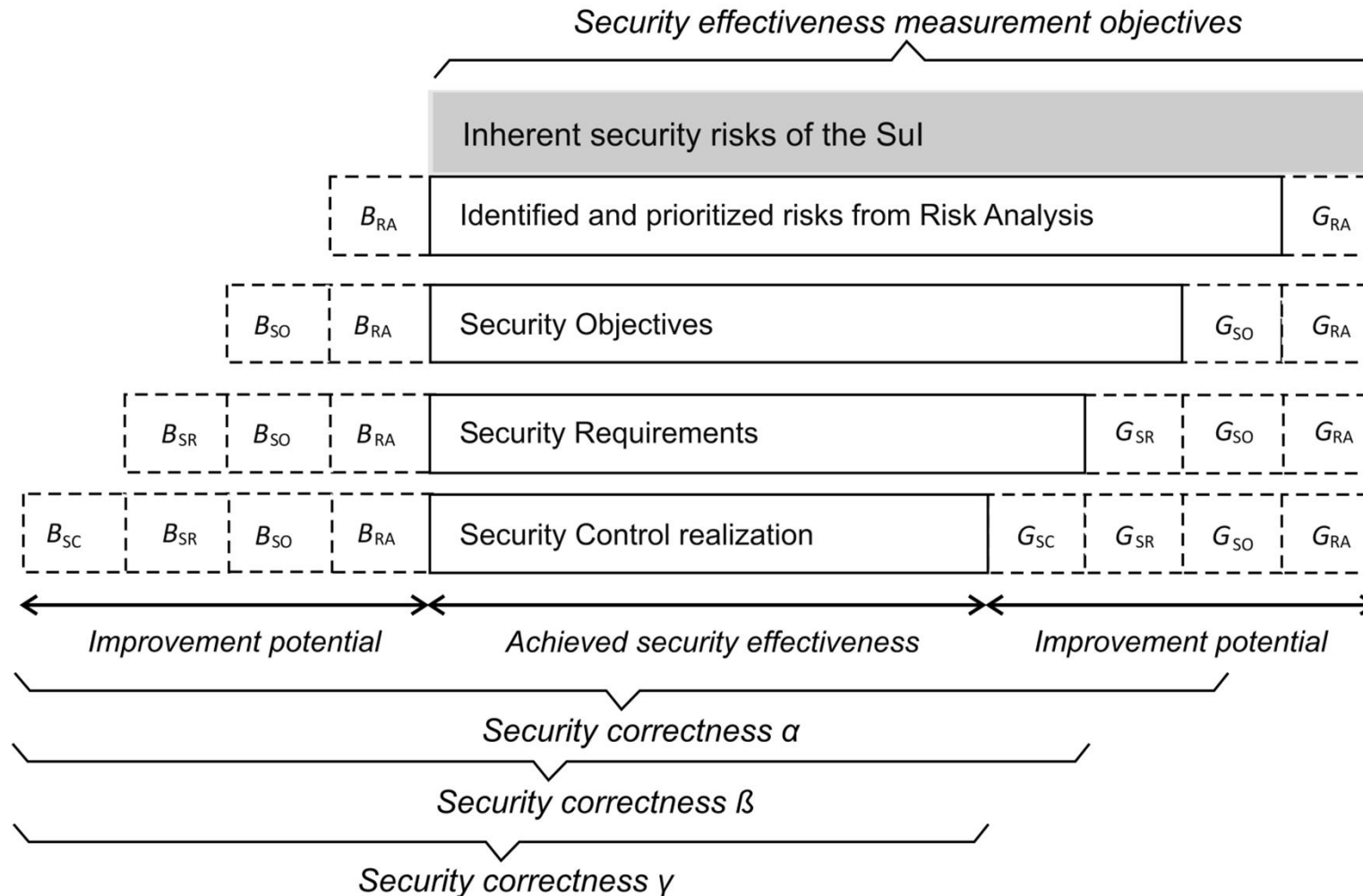
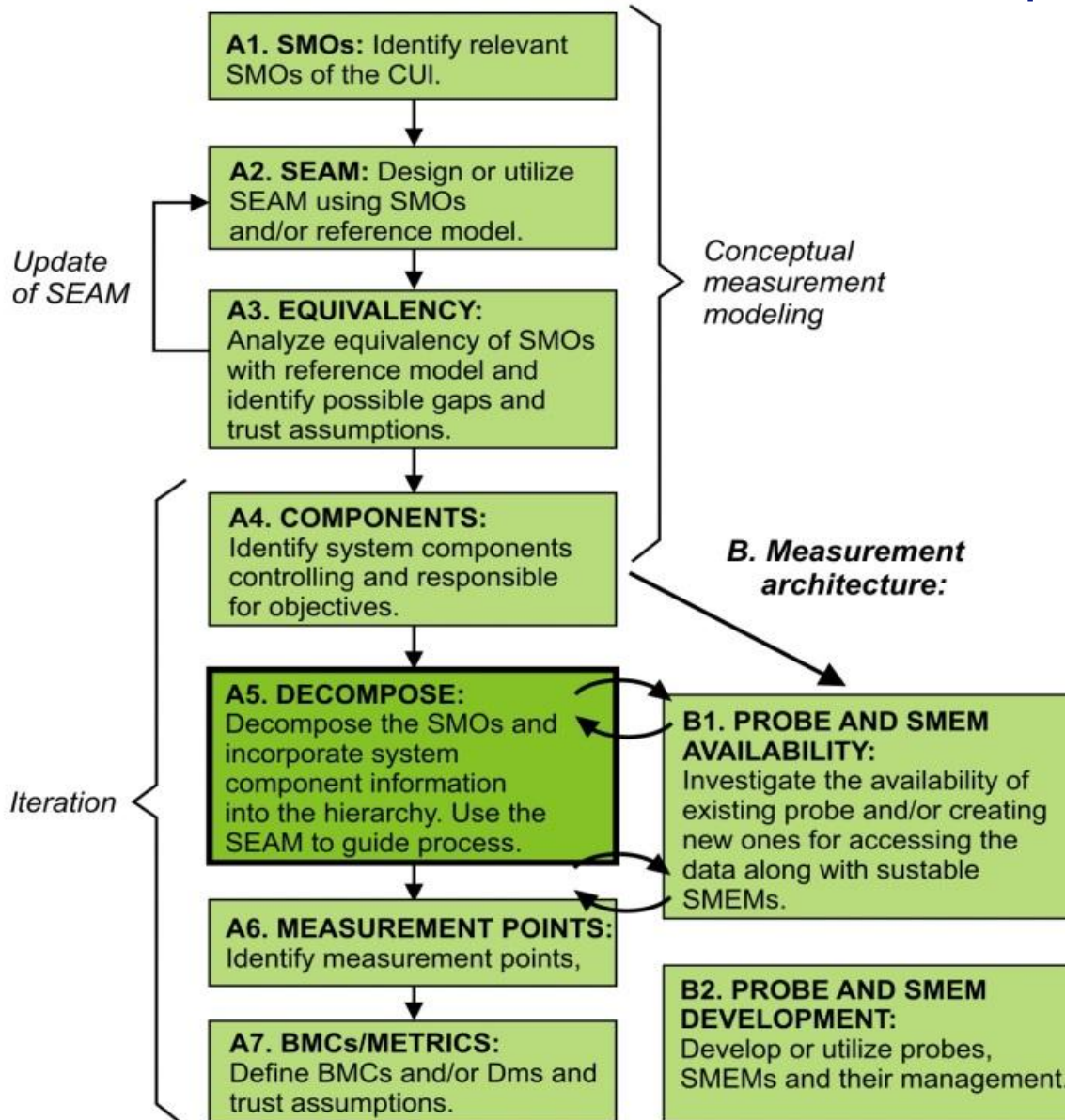


Figure: Savola, R., Frühwirth, C., Pietikäinen A., "Risk-driven security metrics in agile software development – an industrial pilot study". Accepted to Journal of Universal Computer Science, 2012.

FROM SECURITY OBJECTIVES TO METRICS

Decomposition

A. Metrics:



Metrics branch:

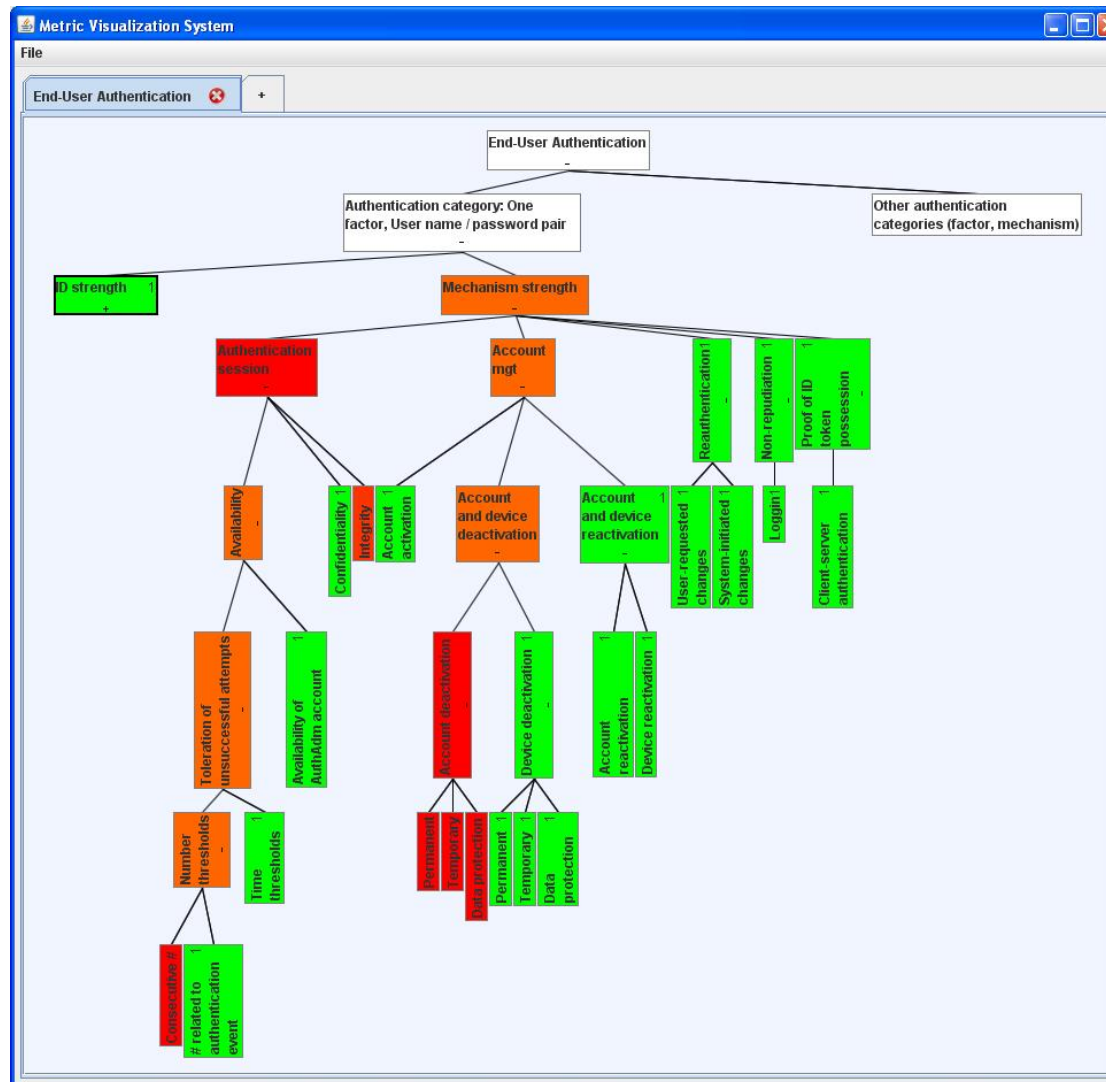
- A1. Security Measurement Objectives
- A2. SEAM (Security Effectiveness Abstract Model)
- A3. Analyze equivalency between A1 and A3
- A4. System components
- A5. The actual decomposition phase
- A6. Identify measurement points
- A7. Define metrics

Measurement architecture branch:

- B1. Probe availability
- B2. Probes and security-measurability - enhancing mechanisms

FROM SECURITY OBJECTIVES TO METRICS

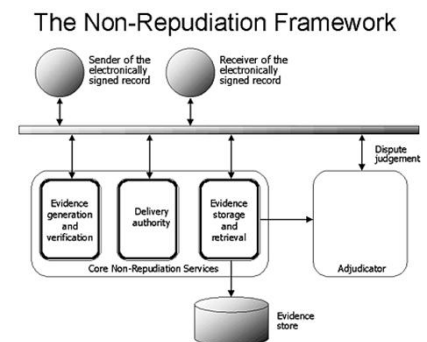
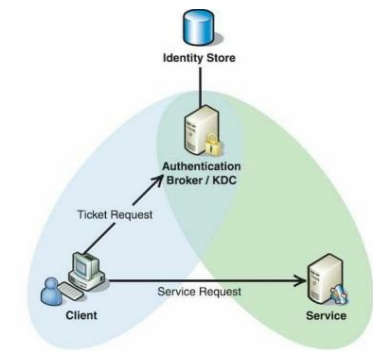
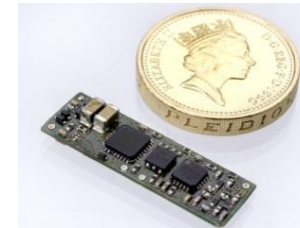
Security Metrics Model Visualization



PROPOSED DECOMPOSITION STRATEGIES

Seven Strategies

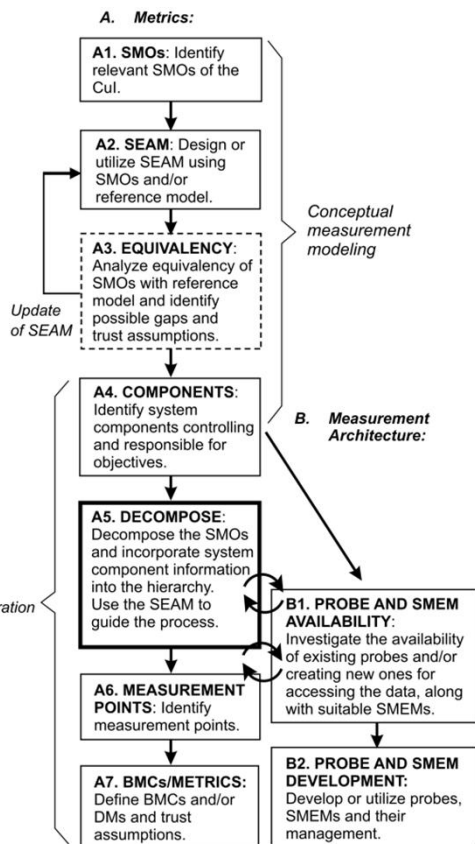
- End user authentication and authorization
- Sensor and BSN authentication
- Service provider user authentication and authorization
- Data integrity
- Privacy and data confidentiality
- Availability
- Non-repudiation

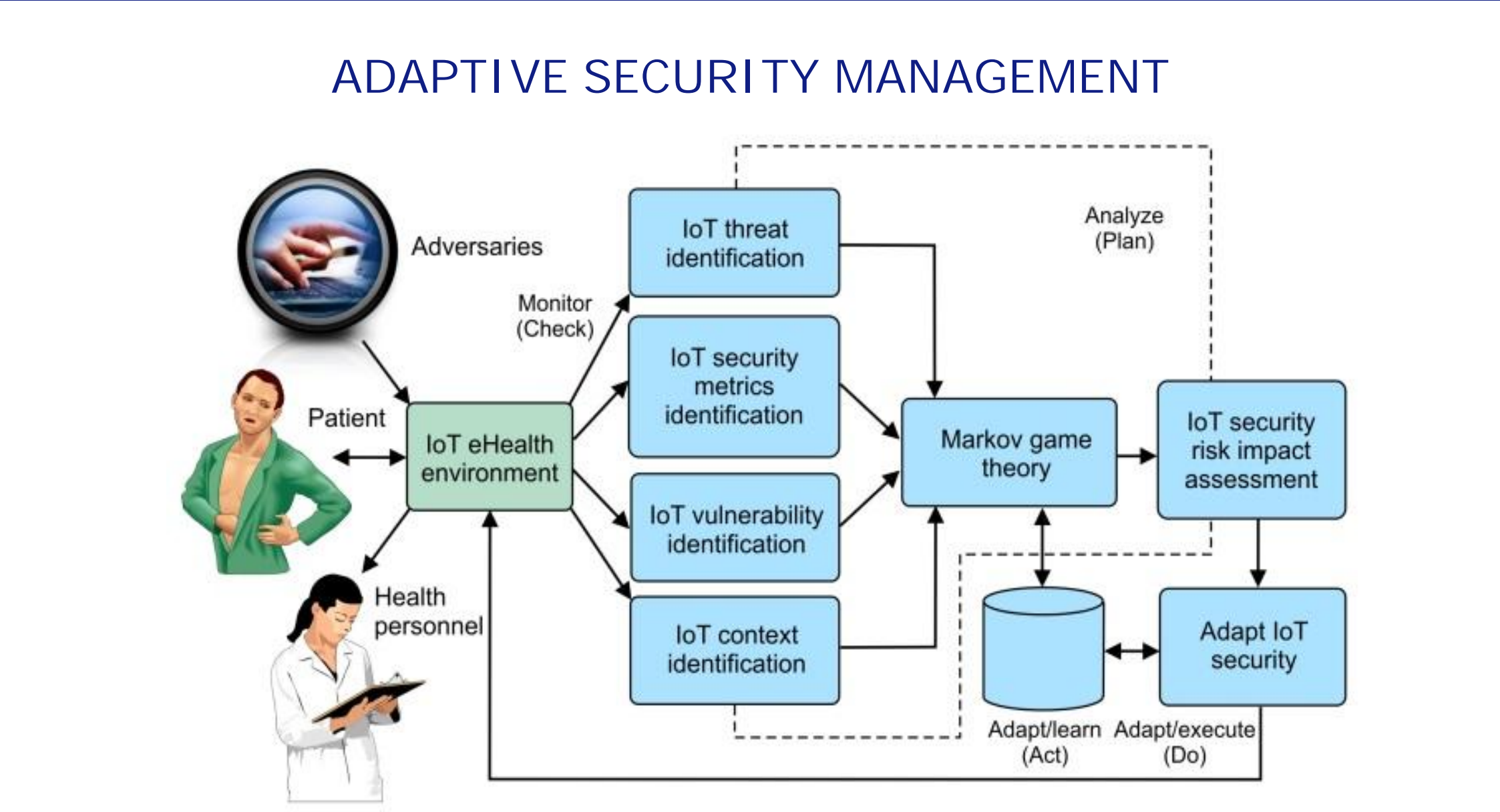



PROPOSED DECOMPOSITION STRATEGIES

Example: End-user Authentication

Stage	Description
A1	<ul style="list-style-type: none"> SO is the sufficient level of authentication and authorization to ensure in particular that the right person receives the right treatment. The following enabling strategies of [14] should be emphasized: SCC, SSQ and SET with focus on usability. DPSE is also relevant from incident management perspective.
A2–A3	<ul style="list-style-type: none"> Basis: <ul style="list-style-type: none"> Identity SE Uniqueness Structure Policy SE Mechanism SE Reliability Integrity more detailed model emphasizing SCC, SSQ, SET and DPSE. The NIST's Electronic Authentication Guideline [5] is an example of a related reference model.
A4	<ul style="list-style-type: none"> Components at CL 0, I, IIb and IIc. In particular, identity tokens and their management are important components. Focus is on client perspective, but client/server authentication protocols are important too.





- Markov game theoretic model for security metrics risk impact assessment, see details in the paper.
- 

CONCLUSIONS AND FUTURE WORK

- Informed risk-driven security engineering and management requires systematic security evidence via metrics
- We have proposed 7 security objective decomposition strategies aiming at metrics for an E-health IoT application
- A context-aware Markov game theory model for security metrics risk impact assessment was developed to enable adaptive security management.
- We plan to focus in our future work to
 - decomposing the security objectives in one model
 - Develop security metrics based on that model
 - Develop Markov game theoretic model to context awareness and unknown threat prediction



Thank you!
Questions?