MULTIMEDIA AS AN EMERGING CYBER THREAT IN MODERN SOCIAL NETWORKS

Zlatogor Minchev, Vladimir Dimitrov,
Milena Tulechka, Luben Boyanov

E-mails: zlatogor@acad.bg, vgd@acad.bg,
milena_tulechka@abv.bg, lb@acad.bg

International Conference

October 2, 2014 **AUTOMATICS AND INFORMATICS'2014** Sofia, Bulgaria

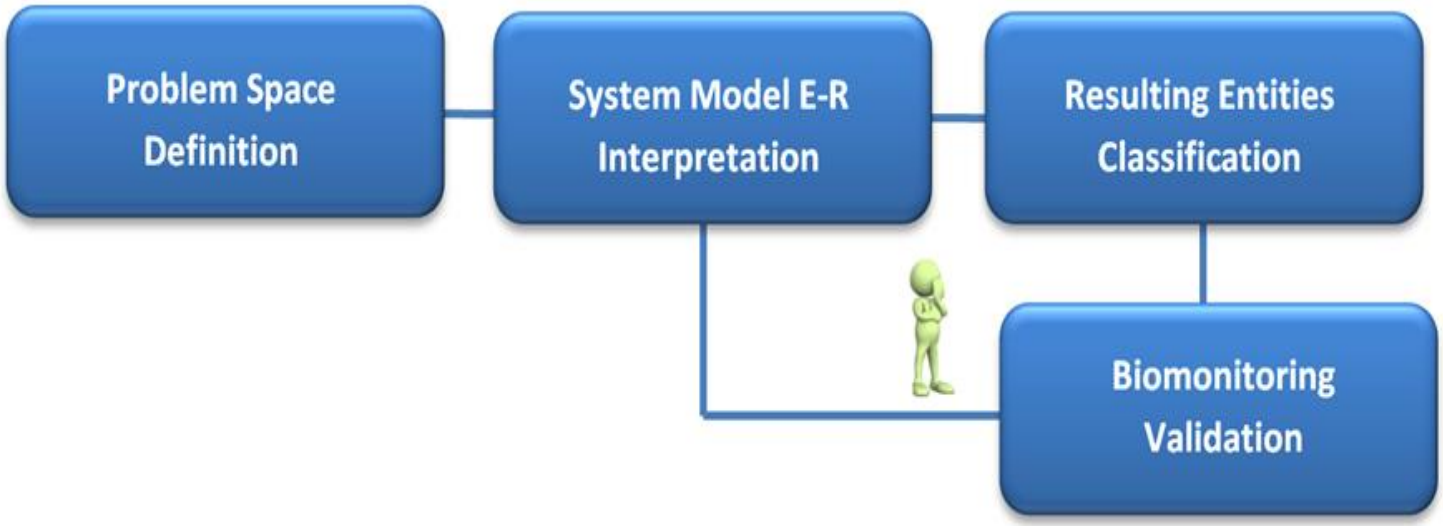
Contents

- Multimedia in our daily life
- Methodological Framework
- Problem Space Definition
- E-R Model Interpretation
- Biomonitoring Validation
- Discussion & Future Work

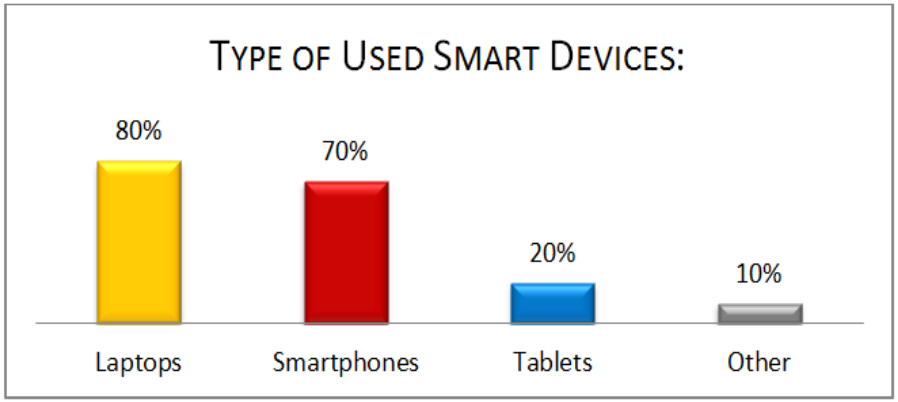
MULTIMEDIA IN OUR DAILY LIFE

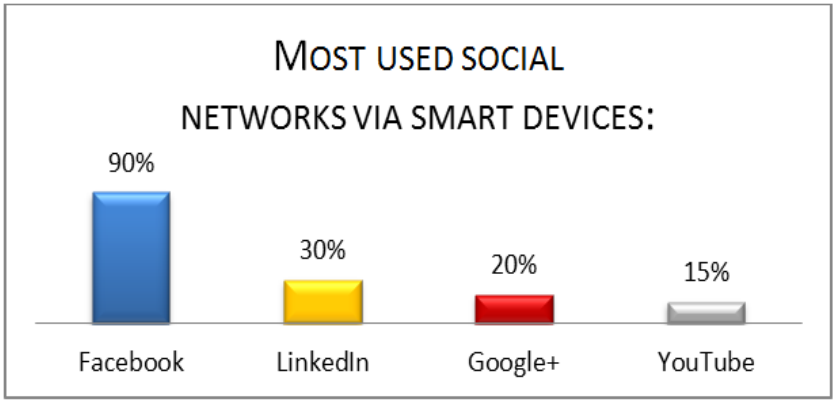
...

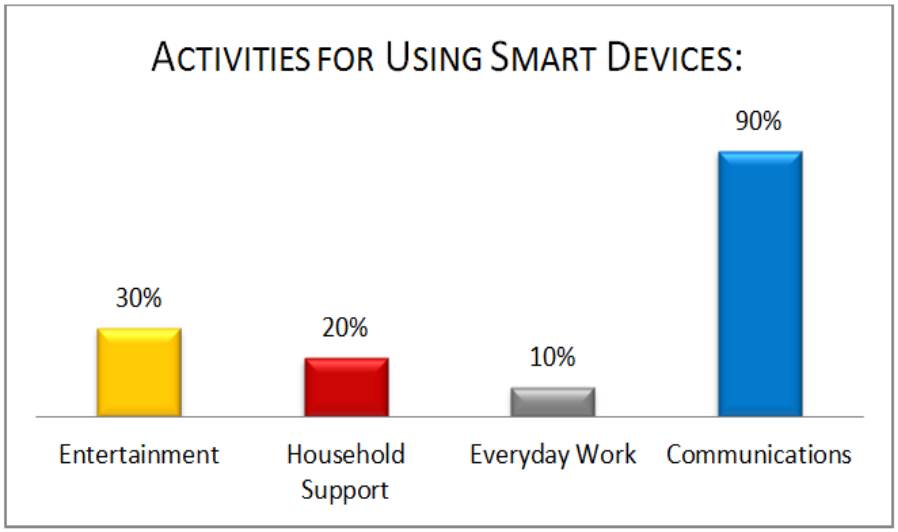
Methodological Framework

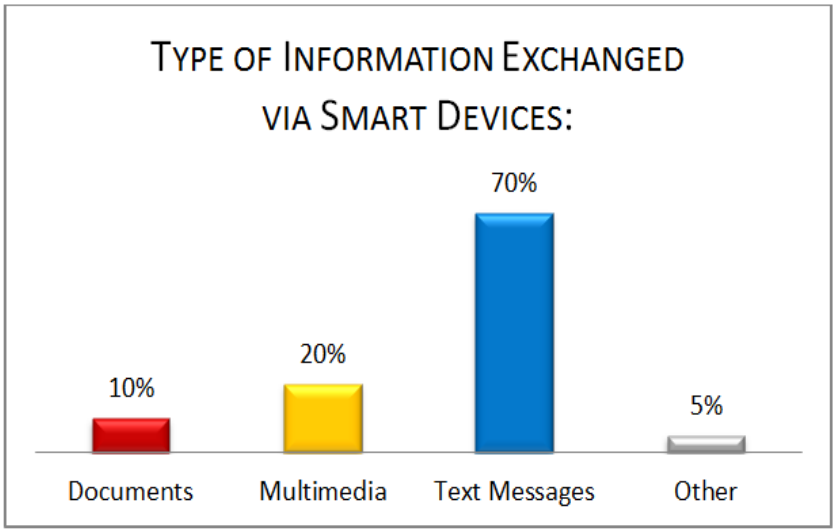


Problem Space Definition

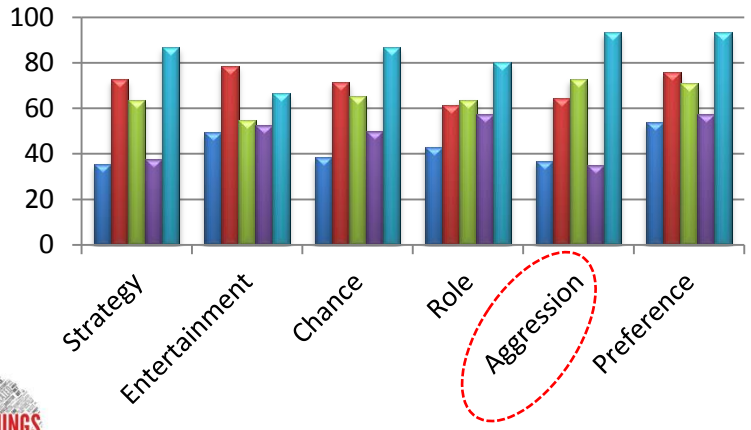








Threat/Area	Human Factor	Digital Society	Governance	Economy	New Technologies	Environment of Living
Social Engineering						
Malware						
Spam & Scam						
Multimedia Influences						
Espionage & Privacy						



THREATS

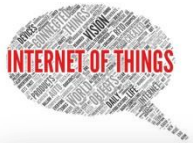
- Malware
- Targeted Attacks
- Social Engineering - Phishing

AREAS

- Mobile Devices
- Social Networks
- Critical Infrastructures

CHALLENGES

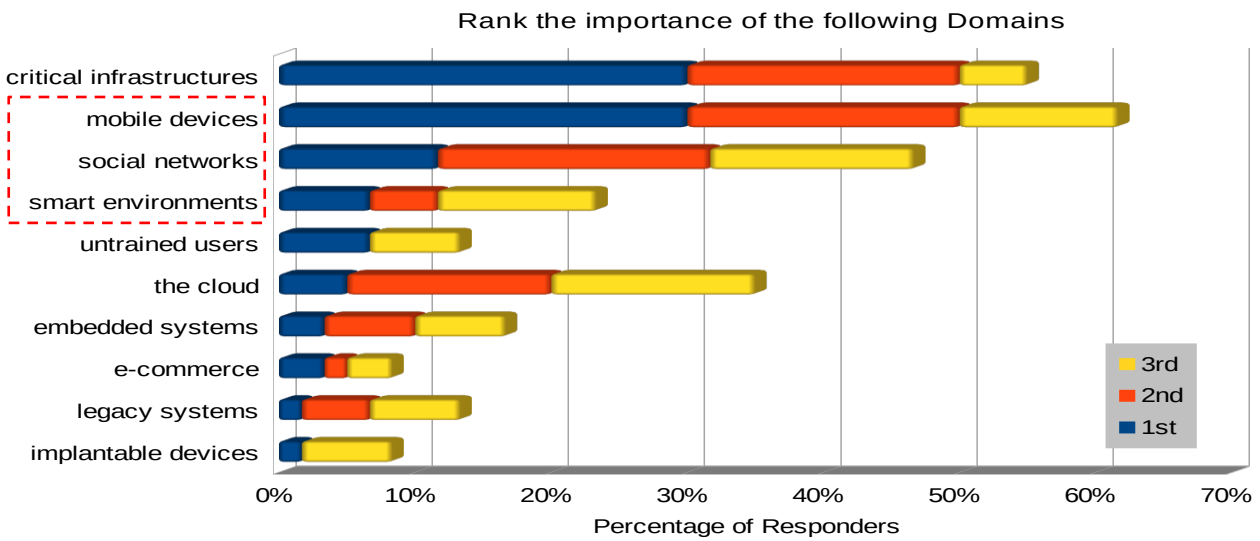
- No Device Should Be Compromisable
- Give Users Control Over Their Data
- Provide Private Moments in Public Places
- Develop Compromise-Tolerant Systems




SEVENTH FRAMEWORK PROGRAMME
Information & Communication Technologies
Trustworthy ICT
NETWORK OF EXCELLENCE
syssec
A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: *Europe for the World*
Deliverable D4.4: Final Report on Threats on the Future Internet: A Research Outlook
Abstract: This deliverable presents the final update on the emerging threats identified by the three working groups at the end of the project. The deliverable also contains the updated version of the research roadmap in the area of System Security.
Contractual Date of Delivery	August 2014
Actual Date of Delivery	September 2014
Deliverable Dissemination Level	Public
Editor	Davide Balzarotti
Contributors	All SysSec partners
Quality Assurance	Christian Platzer, Ali Rezaki

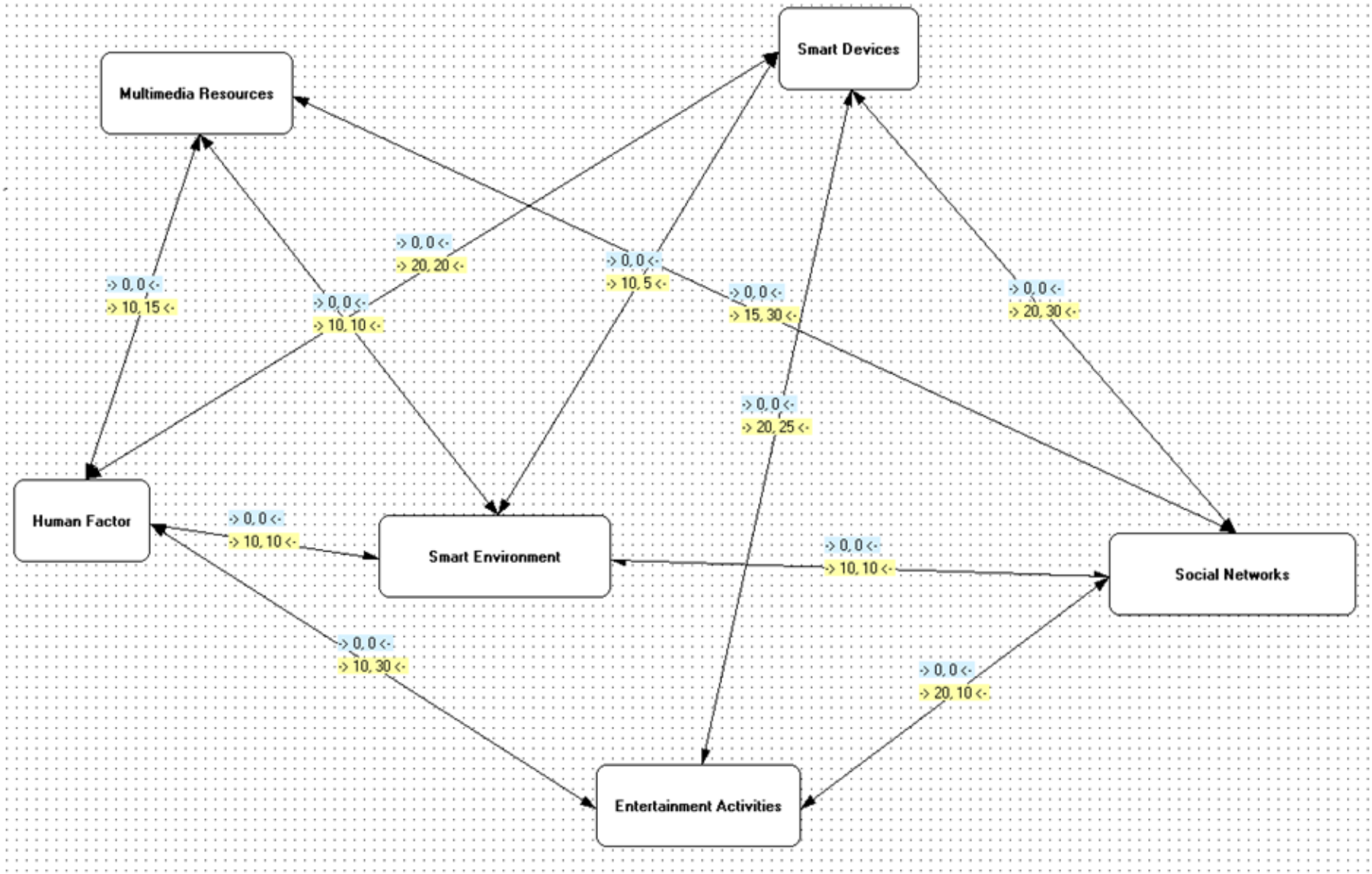
The SysSec consortium consists of:

FORTH-ICS	Coordinator	Greece
Politecnico Di Milano	Principal Contractor	Italy
VU University Amsterdam	Principal Contractor	The Netherlands
Institut Eurecom	Principal Contractor	France
ICT-BAS	Principal Contractor	Bulgaria
Technical University of Vienna	Principal Contractor	Austria
Chalmers University	Principal Contractor	Sweden
TUBITAK-BILGEM	Principal Contractor	Turkey

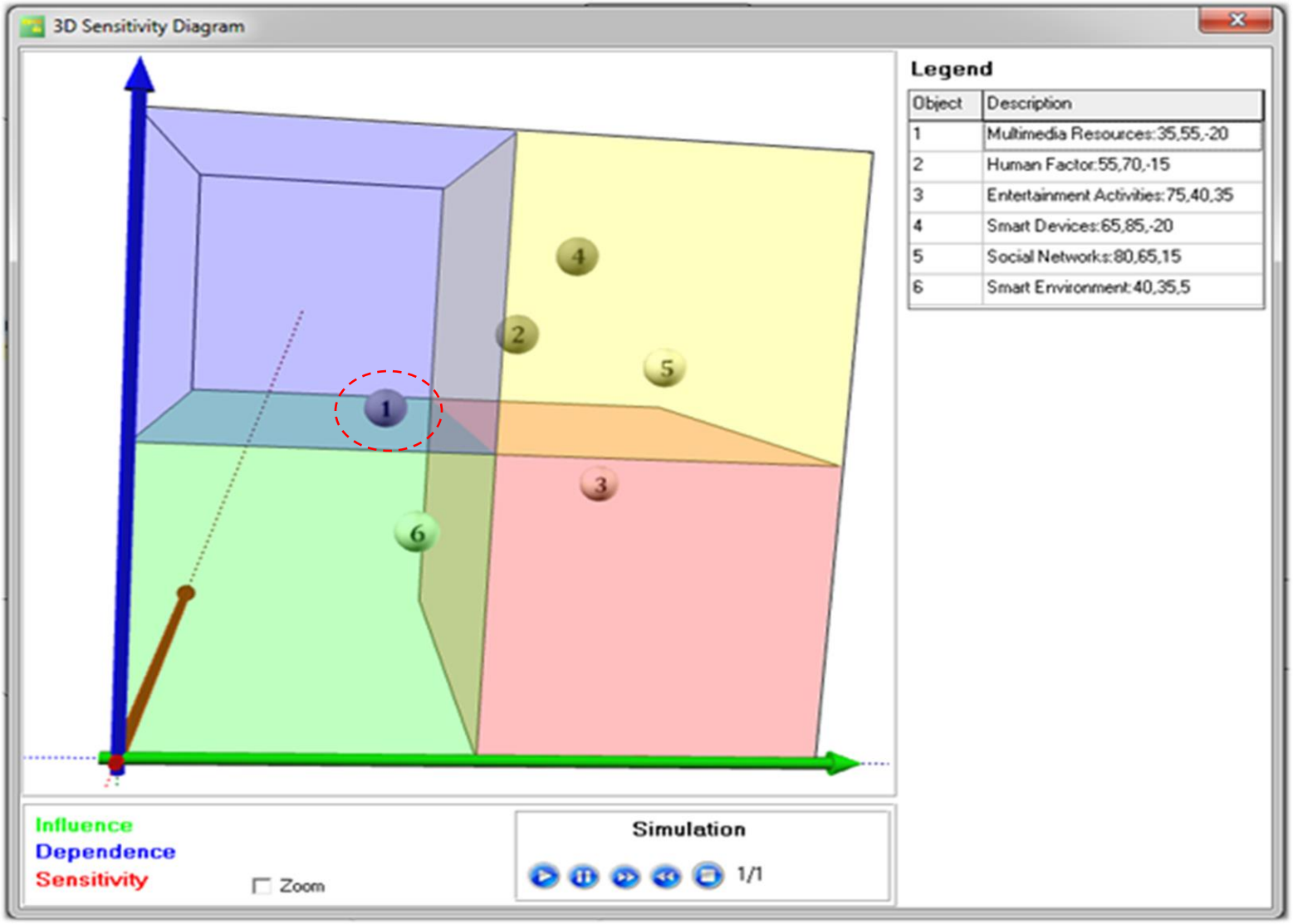


E-R Model Interpretation

I-SCIP©

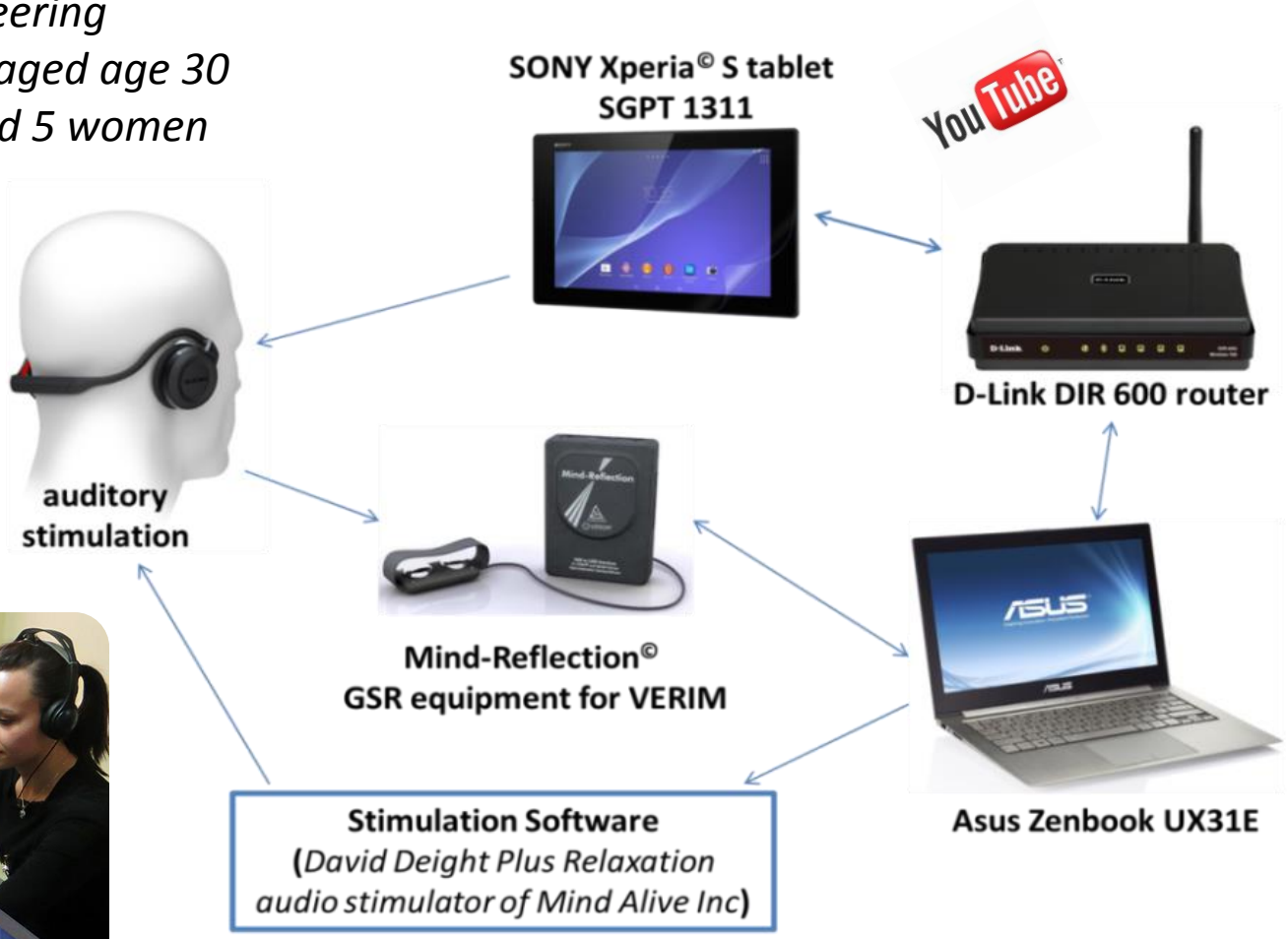


Resulting Classification



BIOMONITORING VALIDATION

15 healthy volunteering participants (averaged age 30 years - 10 men and 5 women

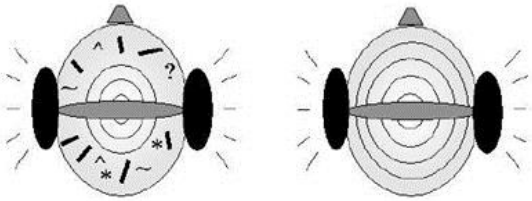


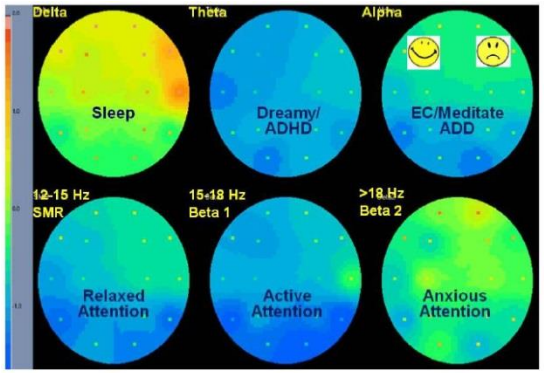
Audio Entrainment Idea

Left 14-10 Hz

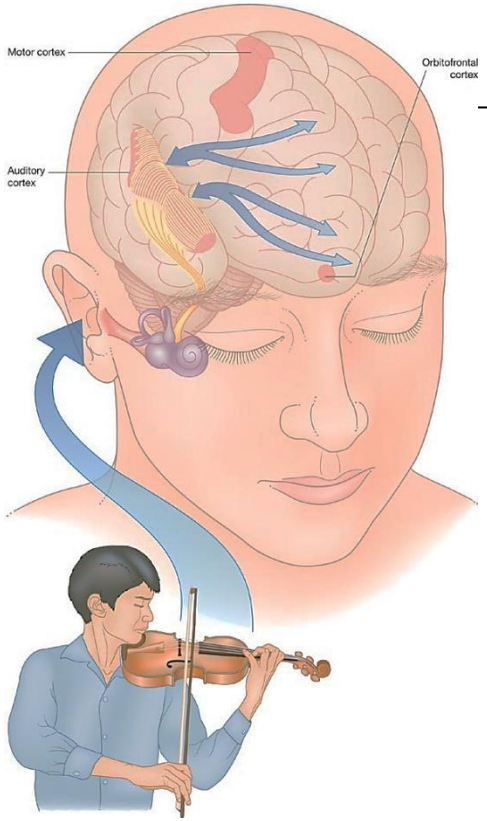
Brain Booster Session

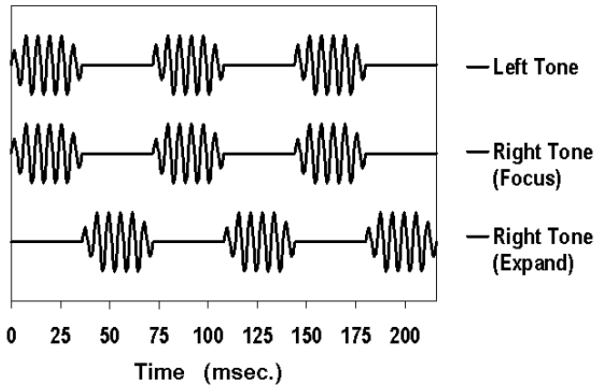
Right 19-10 Hz

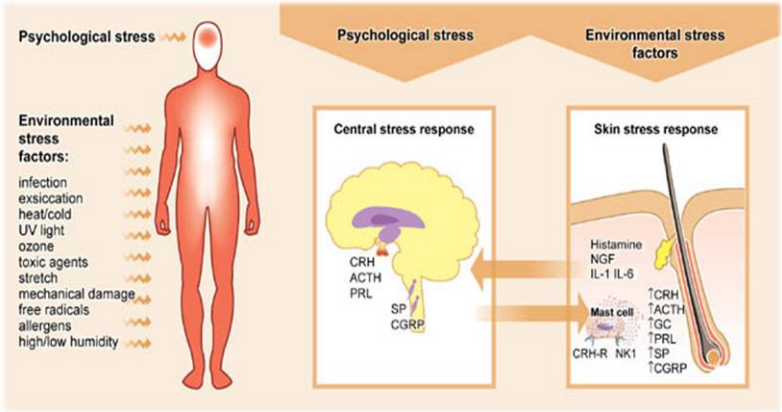




SKIL Data Base

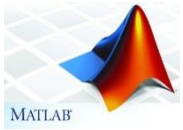




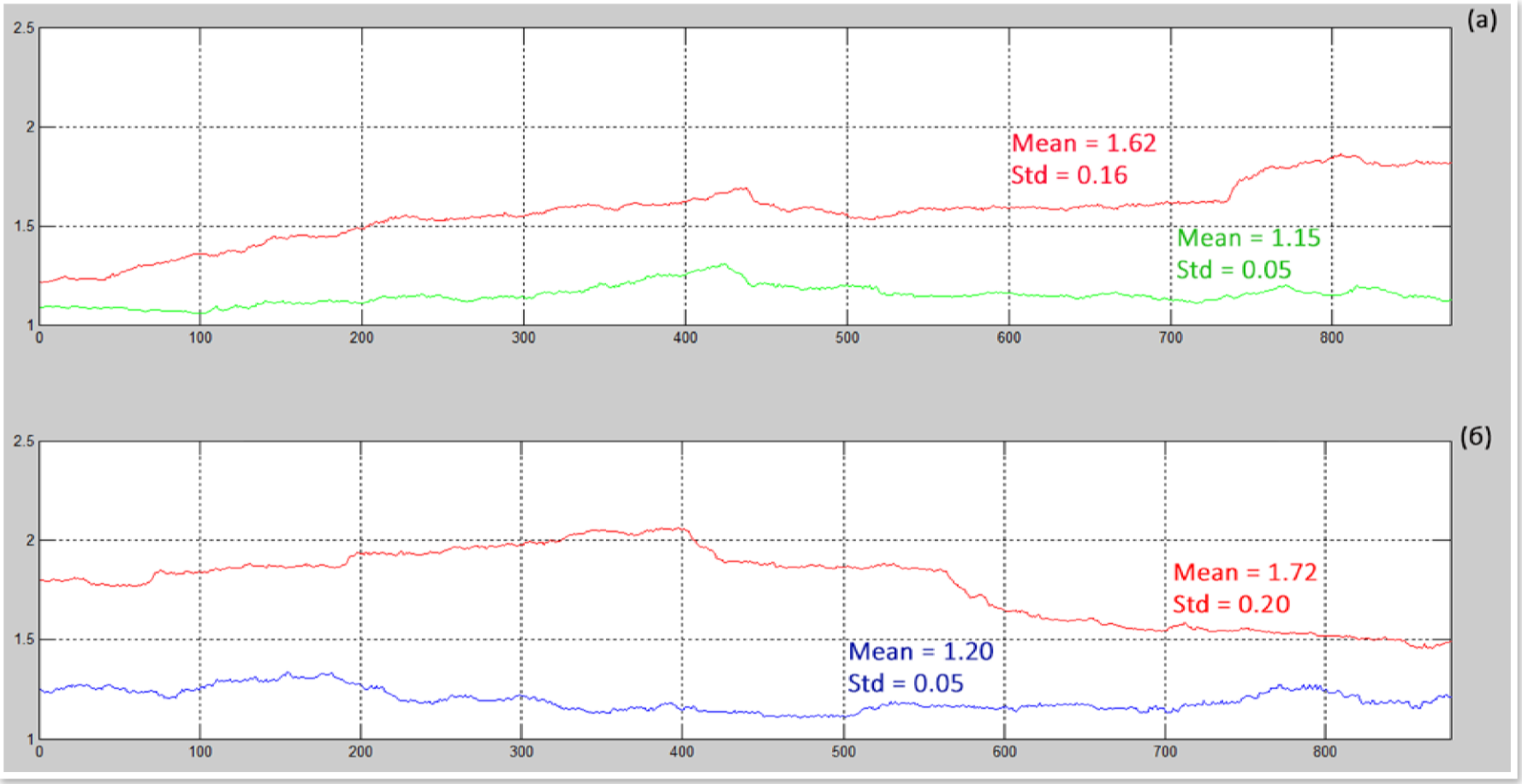


Brain-skin cross-talk

GSR Fractal Dimension Dynamics



Joy



Higuchi, 1988

Georgiev, Minchev et al, 2009

Fear

Discussion & Future Work

The obtained initial modelling and validation experimental results are giving us the possibility to make an assumption that a quantitative measurement of external multimedia auditory influence to nowadays social networks users is possible to be made up to a certain level. This, in combination with problem modelling is of vital importance for the creation of protection software service in nowadays digital world. It is important to note the necessity of implementing the proposed method in a more comprehensive multimedia sense, incorporating visual information and integrating mobile platforms. These will provide a capability for complete real-time users' behaviour and emotions biometric data monitoring and more reliable and detailed cyber threats identification.

Acknowledgements

The results in this publication are financially supported by:

 A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks, DMU03/22, NSF, Young Scientists Grant, WWW.SNFACTOR.COM

syssec EU Network of Excellence in Managing Threats & Vulnerabilities for the Future Internet – SysSec, WWW.SYSSEC-PROJECT.EU

Additional gratitude for the methodological and technical support is given to:

 A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes, DFNI-T01/4, NSF, WWW.SMARTHOMESBG.COM

THANK YOU FOR THE ATTENTION!