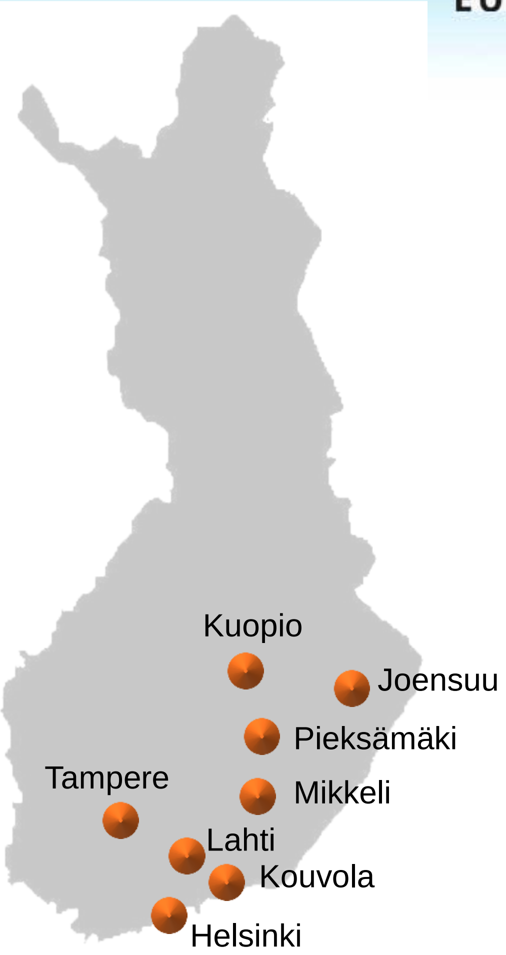
Proposers Day
7 May 2014, Oulu

Celtic-Plus Success Stories SASER-SIEGFRIED

Dr. Markus Sihvonen, Mikkelin Puhelin Oy
Markus.sihvonen@greenpeak.fi

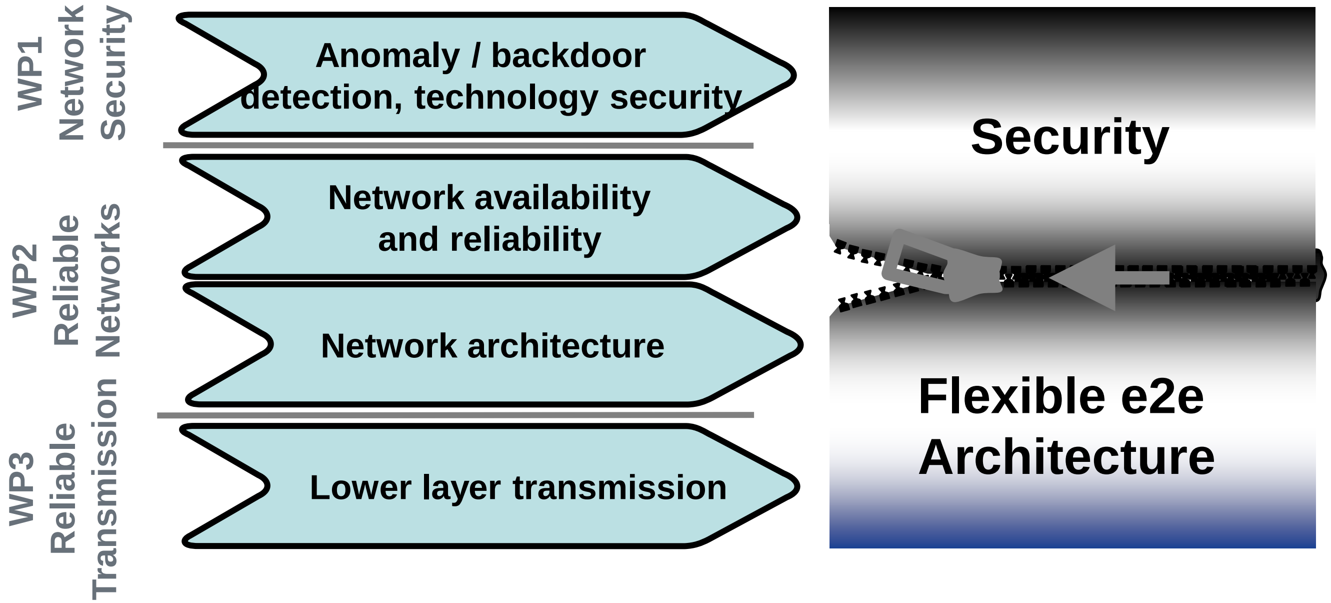
MPY in eight cities

- MPY (Mikkelin Puhelin Oy) was founded in 1888. MPY is wholly owned by Mikkelin Puhelinosuuskunta,
- We serve businesses as well as community and public sector organisations, telecommunications companies and private persons.
- Today, we operate in eight cities: we employ more than 125 professionals in Helsinki, Joensuu, Kouvola, Kuopio, Lahti, Mikkeli, Pieksämäki and Tampere.



SASER–SIEGFRIED Objectives

Define a concept for a flexible and energy-efficient network architecture that fulfils current and future security requirements



WP1 Network Security

Anomaly / backdoor detection, technology security

WP2 Reliable Networks

Network availability and reliability

Network architecture

WP3 Reliable Transmission

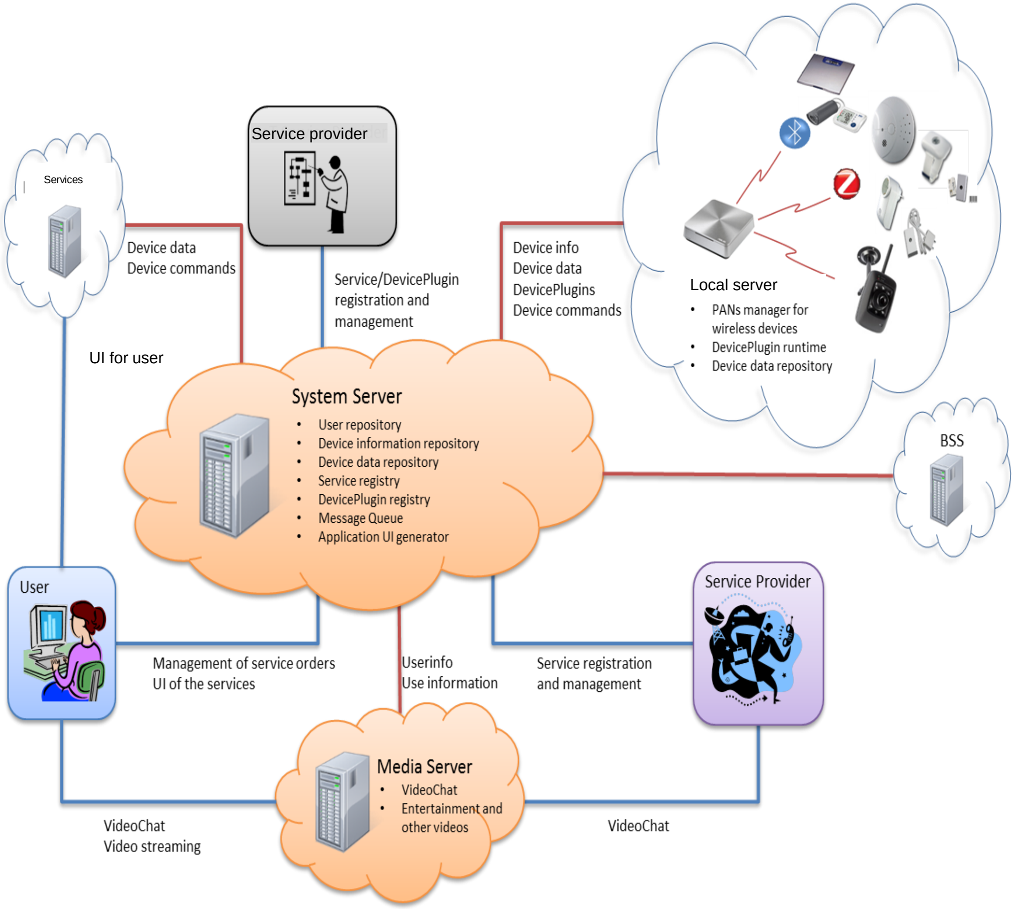
Lower layer transmission

Security

Flexible e2e Architecture

Secure Smart Home Services

- Cloud - System Server
  - Maintains repositories and registries and provides RESTful API
    for the other components in the system
  - Generates HTML5/JS based application UIs
- Cloud - Media Server
  - Mediates videochat calls
  - Provides videostreams for stored video files
  - Adminstrates repository for videofiles
  - Generates HTML5 based UI for VideoChat and Video file streaming
- Local Server
  - Coordinates PANs for WiFI, ZigBee and Bluetooth devices
  - Mediates data from devices to the System Server and device
    commands from the System Server to the devices
- User
  - Browses, orders and uses the offered services s
- Service Provider & Service provider
  - Offer services that end user can order from home and
    use at home



Services

Device data
Device commands

Service provider

Service/DevicePlugin registration and management

Device info
Device data
DevicePlugins
Device commands

Local server
- PANs manager for wireless devices
- DevicePlugin runtime
- Device data repository

UI for user

System Server
- User repository
- Device information repository
- Device data repository
- Service registry
- DevicePlugin registry
- Message Queue
- Application UI generator

BSS

User

Service Provider

Management of service orders
UI of the services

Userinfo
Use information

Service registration
and management

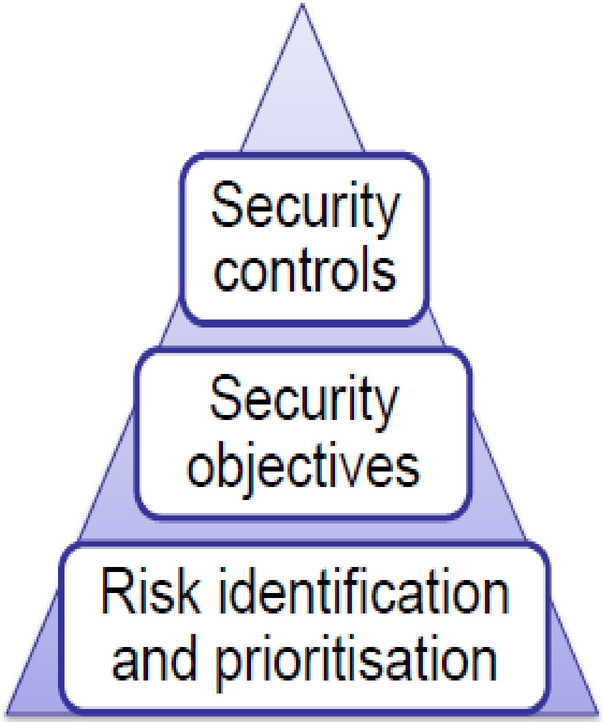
Media Server
- VideoChat
- Entertainment and other videos

VideoChat
Video streaming

VideoChat

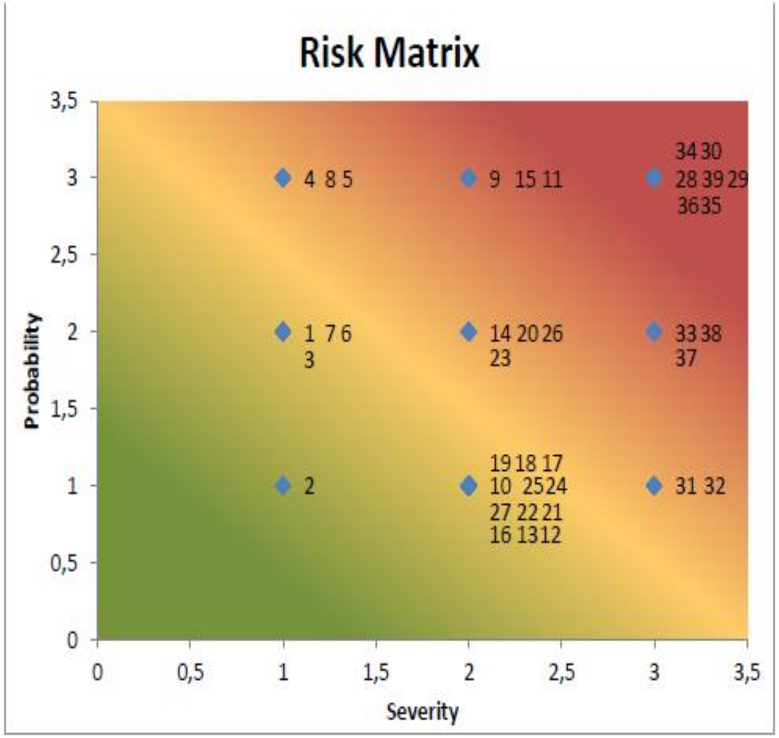
MPY use case risk analysis

- presents an abstraction how security controls are built on security objective and prioritized risks.



MPY use case risk analysis

- Risks and threats are identified from two perspectives, i.e. business and the End-User viewpoints.
- After the risk identification, severity and probability values for the risks are given
- Risk matrix in Figure sets risks to probability-severity axes in order to facilitate prioritization.



MPY use case risk analysis

- Network security must involve the authorization of access to data in a network, which is controlled by the network administrator.
- The End-Users must be as-signed an ID and password or other authenticating information that allows them access to information and programs within their authority.
- VPNs and Firewalls should be used when possible.
- All management traffic should be strictly filtered to reject non-manager End-Users.
- **All sensitive information must be encrypted when transported** across networks to fulfil the confidentiality aspect.
- Also stored/mediated **sensitive data** in a web service should be **encrypted** when possible. So the End-User can trust that all sensitive information is safeguarded.
- The **privacy** is fulfilled by the prerequisite of advanced access control and **strong authentication and password administration**.
- **Also the surveillance of the operation of the whole system affects user privacy**. The availability of the system must be ensured by providing enough redundancy so that any possible failure anywhere in the network will not affect the overall systems operation.

Security Requirements for the End-User

- The End-User is the one that uses the services the system provides. For the End-User there are several different aspects that affect his/her requirements for security.

- First of all, the End-User may wish to use several different types of services over the same infrastructure. This means that there might be entertainment, education, banking, medical, and other services that the End-User utilizes.

- Services may require different levels of interaction from the End-User and also the underlying sensor network that has been established.

- Thus, there cannot be a one security solution that can be applied for the End-User. **The security depends on the context and the services that are used.**

Security Requirements for the Service Provider

- The Service Provider provides some service(s) for the End-Users in the system.
- The **security requirements of the Service Provider are related mostly to the business of the service provider**.
- This means that **the security controls that the Service Provider needs have to be balanced between costs and benefits.**
- As many of the costs and benefits of security requirements are not easy to valuate in monetary terms, there can be a lot of variation in the chosen security methods.
- Both government and industry regulations can push for more security, when there is an economic incentive to do so.
- Also **educated customers can demand more security features for the services**

Security Requirements for the Network

- The network is the backbone of the system. **It provides connectivity between the End-Users and the different services**.

- The security **requirements of the network are related to trusted communications** so that there are no eavesdroppers or other malicious parties involved in the delivery of the messages between sender and recipient.

- Furthermore, the availability of the network is crucial in modern society. Especially when critical functions such as **medical aid are delivered partly via the network**, the availability of the network becomes very important.

Security Requirements for the Platform and Infrastructure

- In modern systems, the services are often provided in a cloud computing environment.
- This means that many servers host multiple virtual machines that run different operating systems and a multitude of different programs.
- Also the **systems can have various different configurations depending on their use and unwanted and unknown dependencies can arise**
- Furthermore, **malicious or accidental interaction between different virtual machines on the same server can cause security issues**.
- This creates challenges for the security requirements for the different platforms and the infrastructure as a whole.

Security Requirements for End-User's Digital Identity

- End-User's digital identity is widely accepted as "the digital representation of network entities by the individuals, communities, and governments having three fundamental aspects, namely; people, objects, and organizations".

- On the other hand, digital identity is defined as "a collection of personal, context-specific, group, and profiling attributes of the user of Web Service.

- **User Identity Management** can be seen as an essential solution for the service designers and the service providers.

- Furthermore, **it creates the basis for trust, reputation, and data privacy between the users and the Service Providers** (SPs) as well.

- The description of data privacy is focused on
  - (1) distributed processing of personal information of the users,
  - (2) information privacy in general, and
  - (3) guaranteeing of digital identity of the users within the WSs represented by dif-ferent SPs.

- One perspective to user's privacy should be based on:
  - access control,
  - the other one should be based on the viewpoint of the organization that is operating the WS,
  - and yet another one should be based on controlling the uncovering of personal data.

- In order to provide a high level protection for user's digital identity and to allow access to the services, it is important to address the privacy requirements

Security Requirements Derived from Laws, Acts, and Regulations

- In addition to technical challenges, **data processing in the service is facing the challenges regarding the compliance of laws, acts, and regulations originating from different sources in different countries**.

- These “external regulations” together with the needs arising from the business itself are integrated in set of business rules of the enterprise.

- The problems arising during the exploitation of the service are troublesome logical presentations of the problems.

- In general speaking, **the service designers aiming to collect and provide access to the data of the service user must consider a number of legal issues from the outset**.

- Important legislation for them to be aware is related to **public records and data protection**.

- The service designers and providers need to have a good understanding of the legal framework governing digital user’s identity and information privacy related issues and employ measures to guard against breaking the law.

- There are numerous laws, acts and other regulations to be conformed in each country.

Contact Info

Dr. Markus Sihvonen
Mikkelin Puhelin Oy
+358407564802
Mikonkatu 16, 50100 Mikkeli, Finland
www.mpy.fi