Call for Papers: FTC Seeks Input on Privacy and Security Implications of the Internet of Things
Commission Staff to Conduct Workshop on Nov. 21 / iot@ftc.gov

"Project stealth – be invisible, be safe."

Mirko Ross, Personal Cyber Protection Institute

m.ross@pcp-institute.org

With the Internet of Things total privacy and security will be become a scarce resource. Users are always visible for service providers and their big data analysis in a pervasive world where wearable devices such as smart phones, watches, glasses and pens are permanently connected to the Internet. At the same time every internet device is a potential security risk due to hacking or malware. Total security and absolute privacy will not longer exist in the Internet of Things.

Can we create life areas and habitats where the Internet of Things is deliberately excluded?
A refugium where security and privacy can be created on demand and controlled by the user.

By project "Stealth" the Personal Cyber Protection Institute is developing smart solutions for user controlled privacy and trusted security zones.

About project "Stealth"

The starting point of project "Stealth" are electrically conductive textiles for intelligent clothing. The idea behind is quite simple: what if our everyday clothing could act as a "smart clothing shield" ?

Coats, pants or pockets can shield and control the transmission of digital radio frequencies. Such smart clothing allows the wearer to protects and hide devices in Internet of Things. The clothing acts as a faraday cage: if a devices is wrapped into the faraday pockets of smart clothing, the user is "invisible" for service providers: no more GPS tracking, wifi, mobile services or NFC (near field communication). Shielded users does not leave any traces of data. At the same time the devices are also invisible to potential attackers. Project Stealth smart clothing will provide privacy and security on demand.

Applications

Privacy control during meetings

A shutdown at lot of devices - eg iPhone or Google Glass - is only managed via the software interface. With many devices, the battery can not be removed and therefore the trusted shutdown cannot controlled by the user. The device may seem apparently off, but web connection, microphones and camera can be still activated by malware or trojan. Conversations may be recorded and monitored via remote intruders. With project "Stealth" shielded devices are reliably separated from mobile and internet connection. They can not receive commands and transmit confidential data. Since the shield is based on "textile hardware", this barrier is not overcome by usual methods of digital hacking.

Security shieldings for medical implants

Medical implants are increasingly being equipped with remote interfaces. For example, insulin pumps and defibrillators can be monitored and controlled by wifi or NFC. This results great opportunities in telemedicine and diagnostics. But patients must have confidence in the safety of the device and its interfaces. External attacking, for example by ransomware is a true nightmare: patients could be blackmailed to pay protection money, otherwise the attacker will change the functions of the implant. For this cases smart faraday clothing could provide security. The clothing will shield the implant from external requests. In the case of diagnosis, the carrier may neuralize the protective function by simply strip.

Protection against tracking

With the use of mobile services and location-based services adaptors leaving a data trail. Data transmission and processing into motion profiles increasingly bypass users control: for example by mobile location-based services or near-field communication via RFID. Collecting and processing data without approval is an incision into the informal self-determination. For that reason project “Stealth” is creating user controlled privacy habitats. Mobile devices or RFID communication can be specifically controlled. Wearing intelligent clothing users are temporarily invisible in the Internet of Things. They do not leave any location-based data tracks.

About the author

Mirko Ross is cofounder of the Personal Cyber Protection Institute. He is also CEO of echolot digital worx, an online Agency and software developing Company.

Since 1998, he is an open source evangelist, working on several tasks groups for the improvement and development of open source standards and open source based business model.

Already during his studies he founded 1998, together with Sven Rahlfs, his first company in the technology sector.

He is teaching Web Engineering at Heilbronn University and Mirko is involved on several research activities for open standards and business models in the Internet of Things. Mirko is also a member of the internet of things council, a worldwide IoT think tank. At the Personal Cyber Protection Institute, Mirko is managing the Project Stealth.

Contact

Mirko Ross

m.ross@pcp-institute.org

Twitter:

Personal Cyber Protection Institute

c/o echolot digital worx GmbH

Schulze-Delitzsch-Straße 16

70565 Stuttgart

Germany