HealthManagement
Promoting Management and Leadership

Designing Smart Homes for Care: Challenges and Questions

Dr. Edewede Oriwoh, MSc, PhD
******@***yahoo.com

Independent Cyber-physical
Security Researcher

As some of us get older, we start to contemplate the care and support that we will require in our advanced years and how these might be provided to us at an acceptable quality, a manageable cost and with as little disruption to us and the people around us as possible.

Smart homes (SH) are enabled by software and hardware solutions (and a combination of both) to provide support and care services to the aging, the elderly and those who require (long-term) healthcare, on an increasingly autonomous basis. These solutions include AI-based carers, cooks, transport systems, heart and motion monitors, smart kettles, phones, and fridges. SH enable a degree of independence and aging in familiar surroundings whilst giving relatives some degree of assurance about their relatives' care. There are, however, concerns, challenges and questions which need to be addressed by SH solutions developers, vendors, end users, governments, regulators and healthcare suppliers, these challenges and questions which may affect the adoption and use of SH and SH products.

- **Security and Cyber threats** to SH devices, homes and home occupants. These include Distributed Denial of Service (DDoS) attacks; ransomware; unpatched and vulnerable systems; firmware malware; rootkits and backdoors; theft/loss of data, information and hardware; blackmail and other yet unknown threats.
- **Confidentiality** of SH communications and data, whether at rest or in motion.
- **Interoperability** This concerns if, and how, existing, perhaps even legacy, technologies might work with new ones, whilst recognising that legacy systems may provide a path for malware to get onto SH networks.
- **Prejudiced Programming** Extensive, open discussions are required around equal treatment, r obo-ethics, AI ethics, robo-morals and related matters.
- **Continuous Availability** Especially for countries where power supply is intermittent or minimal, it is crucial to identify what options exist for manual backups, alternatives and even overrides of autonomous systems.
- **Privacy** of SH occupants in the face of technologies which monitor and collect data about them: w hat laws protect their data, security and privacy especially in the face of GDPR and deployments in non-GDPR-compliance countries?
- **Functionality** Considering robot "care" systems: are resets possible? How many resets per device will be allowed and by whom: by authenticated users *only*?
- **Affordability** Cost of hiring, owning, maintaining, replacing, training and insuring SH solutions.
- **Ease of use** Will (extensive) training be required before end users are able to make use of SH solutions to avoid poor configuration leading to malfunctions.
- **Universality, peculiarity and breadth of use cases** Smart technologies should understand the characteristics and cultural nuances of the different people groups of the world (languages, skin tones, etc.) whilst also addressing universal requirements.
- A **Framework** is required to guide the **secure acquisition, access, configuration, storage** and **disposal** of hardware and data.
- **Regulations** which govern the design, training, algorithms, behaviours, manufacture, sale, security, use and retirement of SH autonomous systems are required.
- **Seamless Integration** This concerns methods of maintaining normality even as a home becomes smarter so its occupants are not overwhelmed by any changes.
- **Flexibility of technologies** It is important for all SH systems to have a degree of flexibility and to be able to learn and adapt as people change their habits, without misinterpreting a change in habit as a malicious event.
- **Simplified, suitable and secure multi-factor authentication systems** A fingerprint biometric solution deployed to control access to a SH whose occupant has hand tremors may not be a suitable solution.
- **Accuracy and reliable operation** The system must be built to, as much as possible, accurately recognise trusted third parties including family, friends, carers and maintenance staff and correctly identify user error.
- **Degrees of rights and freedoms** of humans with respect to non-human elements. Consider suicides using robots, excessive care by robots and similar scenarios.

Ownership of personal devices and data (locally stored and in the cloud), and h ired and shared devices (e.g. robot carers) and ensuring shared devices can learn and accurately identify their different user's habits.

With Smart Homes, **end users should not be afraid but they must be aware** . To engender trust and comfort for end users, the following recommendations must be considered by the relevant stakeholders, as it applies to them:

(Inter)connect Smart Things only where absolutely necessary; segment and isolate networks to contain failure and avoid failure across single or multiple networks; change default authentication settings on devices and change these over time; provide cyber-awareness training and support for home occupants; use anti-malware tool(s), firewalls etc.; block unused ports/protocols; monitor **legitimate** "**backdoors"** used by vendors or service providers to monitor and communicate with SH nodes; consider taking out **insurance** against damage and loss; set up **regulations** and standard practices that smart nonhuman carers will be *designed* to adhere to and a framework that they operate within; s **ecure** all data that is fed into (machine) learning systems to prevent corruption; verify sources of data; source diverse opinions during initial design phases by using **focus groups from diverse backgrounds** ; define and implement **baselines** for managing the decisions of robots; anticipate and prepare for cyber-physical threats using **threat hunting** for SH; introduce dedicated monitoring by a trusted "relative or friend" of each nonhuman Thing (device) in the SH.

Zoom On

What is your top management tip?
LISTEN to the Junior member of staff. Let the Junior speak.

What would you single out as a career highlight?
Achieving my PhD degree and having the opportunity, for the first time, to be present at a premiere of one of my compositions on July 2nd 2017 at the London SouthBank Centre.

What are your personal interests outside of work?
Singing and Composing music.

Your favourite quote?
Anyone who thinks robots will take over from humans has not met humans. - Edewede Oriwoh

Published on : Tue, 18 Jul 2017