Making Security Available for Everyone - Towards a Community-Based Smart Home Security System

Marcus Köhler
Institute of Technology Management
University of St. Gallen, Switzerland
Email: marcus.koehler@unisg.ch

Felix Wortmann
Institute of Technology Management
University of St. Gallen, Switzerland
Email: felix.wortmann@unisg.ch

***Abstract*—The Internet of Things offers the possibility to make security available for everyone. Prior research has well-explored the technical realization of smart home security systems. However, the challenge of frequent false alarms still remains unsolved. While current research mainly focuses on sensor and algorithm improvements, this paper proposes a semi-automatic approach. It leverages the established concept of neighborhood watch communities in order to develop a community-based smart home security system. It (1) provides a market overview of existing Smart Home security systems as a technical basis for a security community and (2) shows a positive influence of community features in case of non-intrusive devices. Consequently, there is a clear opportunity to strengthen security systems by neighborhood watch communities.**

I. Introduction

In an attempt to create an overview of the current smart home security market, we clustered existing solutions. Clustering criteria were functionality and the use of indoor video technology. Functionality can be split into preventive, detective and reactive functions. Video recording gains special attention in indoor environments due to significant privacy concerns [1]. Three clusters can be identified (see Tab. I): (1) Purely preventive solutions, (2) non-obstrusive alarm systems and (3) obstrusive alarm systems.

How reliable can a security system perform its task? The base-rate fallacy [2] states that it is difficult for intrusion detection systems to be effective. Effectiveness is the ratio of relevant alarms to false alarms of the system. The absolute number of relevant alarms is low for security systems because of the low frequency of intrusions. In contrary, a high number of false alarms is provoked even by reliable systems because of the commonness of the regular status. The base-rate fallacy is particularly relevant in the case of the presented low-cost systems.

Neighborhood watch represents a completely different approach to prevent and detect crimes. During the late 1960s, the movement has emerged in the USA. It comprises three essential actions in the fields of crime prevention and detection: block watch, engraving property, and community organization [3]. The results are promising. 40% of the US citizens [4] and 29% of the UK citizens [5] live in neighborhood watch protected areas. A recent meta-analysis [4] shows that 15 of 18 studies prove the crime-reducing effect of neighborhood watch.

TABLE I. Overview of Smart Home Security Solutions

	Obtrusiveness	
	low	high
Preventive	(1) Philips Hue	n.a.
Detective	(2) Lockitron, Skybell, Scout	(3) Canary, Piper
Reactive	n.a.	

Smart Home Security Communities try to leverage the crime-reducing effect of neighborhood watch approaches by the use of technology. First studies of this combination exist. Zeki et al. [6] present a technical approach to share video camera streams between different users in order to evaluate the severity of situations. The impact of such a solution is analyzed by a qualitative study [7], which evaluates the use of shared outdoor cameras to detect suspicious activities. The study shows the potential of this solution and points out privacy concerns considering the cameras fields of view and constant use of the system.

II. Research Gap and Research Questions

The positive effect of neighborhood watch communities has been shown by various researchers [4]. Local online communities like Nextdoor facilitate such functional communities [8]. The idea to complement these communities with Internet of Things based capabilities is not new. However, in the context to privacy concerns this idea has only been evaluated for the case of street camera based communities [7]. In contrast to existing approaches, our research focuses on the liaison o2 indoor security and communities.

More specifically, we address on the following research questions. (RQ1) Do community features, i.e. the technical capability to include others into home protection increase potential users' intention to use a smart home security system? (RQ2) Do powerful yet privacy-intrusive security features, i.e. video surveillance increase or decrease potential users' intention to use a smart home security system? (RQ3) Do community and powerful yet privacy-intrusive security features have an interaction effect on users' intention to use a smart home security system?

III. Study Design

We acquired 160 participants via Amazon Mechanical Turk [9] for a small monetary compensation. The participants were randomly assigned to one of four treatment combinations.

Corresponding to the related research, we built upon two device settings. (1) Less intrusive: This setting is based on our

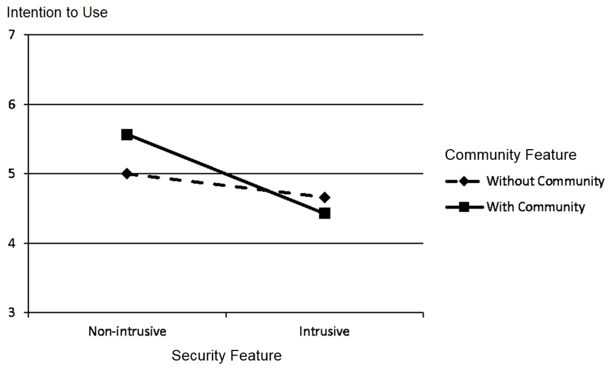

Fig. 1. Intention to use (7-point Likert scale) depending on intrusiveness and community features of the device

system ”Security Light” and its motion detection technology. (2) More intrusive: The description of the Canary system[1] is taken as an example for a video based system.

In respect to communities, we leveraged two fundamental settings. (1) Community: Community functionality was highlighted, i.e. the possibility was described to give other people like friends or neighbors the capability to access the information gathered by the security system. Also, their potential ability to act in case of an intrusion was pointed out. (2) No community: No community functionality was mentioned.

On the basis of the described settings we deployed four treatment groups (2x2 factorial design). A subsequent item-based questionnaire allowed us to measure the effects of our experiment. The metric assessing intention to use was adapted from Davis [10]. To better understand the influence of privacy as a key constraint of intention to use [1], we also measured privacy concerns on the basis of Dinev and Hart [11].

IV. Study Result

To assess the impact of community-based and privacy intrusive security features on intention to use, we conducted a two-way Anova [12]. The corresponding means are illustrated in Fig. 1. (RQ2) There was a significant main effect of privacy intrusive security features on intention to use, $F(1,160) = 7.35$, $p < .01$. Specifically, intention to use was significantly higher in case of no video settings. (RQ1) Furthermore, there was no significant main effect of community features on intention to use, $F(1,160) = .37$, $p > .05$. (RQ3) However, there was a weak interaction effect of privacy intrusive security and community features, $F(1,160) = 2.14$, $p < .10$. Community features increased intention to use in the ”no video” condition, whereas they decreased intention to use in the ”video” condition.

To better understand the role of privacy as a key driver of intention to use we additionally conducted a two-way Anova on perceived privacy concerns. There was a weak main effect of privacy intrusive security features on privacy concerns, $F(1,160) = 2.96$, $p < .10$. Specifically, privacy concerns were higher in case of video settings. Furthermore, there was no significant main effect of community features on security concerns, $F(1,160) = .00$, $p > .96$. However, there was a significant interaction effect of privacy intrusive security and community features, $F(1,160) = 4.42$, $p < .05$. Community features increased privacy concerns in the ”video” condition, whereas they decreased privacy concerns in the ”no video” condition.

V. Discussion and Conclusion

Reflecting the results, we see evidence for a general negative relationship between privacy-intrusive technology and intention to use. Furthermore, we only see a positive effect of community features in the case of non-privacy-intrusive technology. The significant negative effect of powerful yet privacy intrusive security technology is in line with current research [1]. While video surveillance indeed has a negative privacy aspect, it is also a potential means for security improvement. Obviously, negative aspects of privacy outperform benefits of improved security.

We expected that both non-intrusive and intrusive devices would benefit from a community. Therefore, we are surprised about the interaction effect of community with privacy-intrusive technology. Our research suggests, that a positive community effect can only be achieved with non-privacy intrusive functionality. In line with [7], we encourage further research to explore the potentials of IoT-enabled security communities.

Acknowledgment

The present work is supported by the Bosch IoT Lab at the University of St.Gallen, Switzerland. The authors are grateful to the reviewers for their helpful suggestions.

References

[1] D. H. Nguyen, A. Bedford, A. G. Bretana, and G. R. Hayes, “Situating the Concern for Information Privacy Through an Empirical Study of Responses to Video Recording,” in *SIGCHI*, 2011.

[2] S. Axelsson, “The Base-Rate Fallacy and the Difficulty of Intrusion Detection,” *ACM Trans. Inf. Syst. Secur.*, 2000.

[3] D. P. Rosenbaum, “The Theory and Research Behind Neighborhood Watch: Is it a Sound Fear and Crime Reduction Strategy?” *Crime Delinq.*, 1987.

[4] T. Bennett, K. Holloway, and D. P. Farrington, “Does Neighborhood Watch Reduce Crime? A Systematic Review and Meta-analysis.” *J. Exp. Criminol.*, 2006.

[5] L. Sims and G. Britain, “Neighbourhood watch: findings from the 2000 British Crime Survey,” 2001.

[6] A. M. Zeki, E. E. Elnour, A. a. Ibrahim, C. Haruna, and S. Abdulkareem, “Automatic Interactive Security Monitoring System,” in *Int. Conf. Res. Innov. Inf. Syst.* Ieee, Nov. 2013.

[7] A. J. B. Brush, J. Jung, R. Mahajan, and F. Martinez, “Digital Neighborhood Watch: Investigating the Sharing of Camera Data Amongst Neighbors,” in *ACM Conf. Comput. Support. Coop. Work*, 2013.

[8] C. Masden, C. Grevet, R. Grinter, E. Gilbert, and W. K. Edwards, “Tensions in Scaling-up Community Social Media : A Multi-Neighborhood Study of Nextdoor,” in *ACM Conf. Hum. factors Comput. Syst.*, 2014.

[9] M. Buhrmester, T. Kwang, and S. D. Gosling, “Amazon’s Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?” *Perspect. Psychol. Sci.*, 2011.

[10] J. Davis and D. Fred, “A technology acceptance model for empirically testing new end-user information systems: Theory and results,” Ph.D. dissertation, 1985.

[11] T. Dinev and P. Hart, “An extended privacy calculus model for e-commerce transactions,” *Inf. Syst. Res.*, 2006.

[12] P. Shrout and J. Fleiss, “Intraclass correlations: uses in assessing rater reliability.” *Psychol. Bull.*, 1979.

[1] http://canary.is/