Making Effective Home Security Available to Everyone - Towards Smart Home Security Communities

Marcus Koehler[1] and Felix Wortmann[2]

[1] University of St. Gallen, 9000, St. Gallen, Switzerland,
marcus.koehler@unisg.ch,
[2] felix.wortmann@unisg.ch

Abstract. The Internet of Things significantly reduces the prices of home security systems, thereby making home security available to everyone. Prior research provides the technical foundation for Smart Home security. However, frequent false alarms still remain a severe challenge. While current work in this domain mainly focuses on the improvement of sensors and algorithms, this study proposes a semi-automatic approach to tackle the false positives. It combines the concept of neighborhood watch communities with IoT technology in order to develop a Smart Home security community. Therefore, (1) this paper shows a positive influence of community features in the case of non-intrusive devices. Furthermore, (2) it points out the influence of personal relationships on perceived security. In consequence, there is a clear opportunity to strengthen security systems by establishing neighborhood watch communities.

Key words: Internet of Things, Smart Home, Security, Intrusion detection, Semi-Automatic, Neighborhood Watch

1 Introduction

Smart Home security communities build upon two fundamental concepts: neighborhood watch communities and Smart Home security devices.

During the late 1960s, the neighborhood watch movement has emerged in the USA. It comprises of three different crime prevention and detection activities: engraving property, community organization, and block watch [1]. Engraving property is the announcement of a neighborhood community in order to deter possible criminals. The community organization increases the local social capital and thereby fosters a shared response to critical situations. Finally, block watch involves citizens in surveillance plans, which for instance comprise of patrols.

The impacts of neighborhood watch programs are promising. 40% of the US citizens [2] and 29% of the UK citizens [3] live in areas protected by neighborhood watch initiatives. A recent meta-analysis [2] shows that 15 of 18 studies prove the crime-reducing effect of neighborhood watch.

Current Smart Home security systems purely rely on a purely technical approach. In an attempt to create an overview of the current market, we clustered

Table 1. Overview of Smart Home Security Solutions

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

existing solutions. We thereby assure mass market compatibility by setting a price limit of 500 USD. Clustering criteria were functionality and obtrusiveness. The functionality can be split into preventive, detective and reactive properties. Obtrusiveness can be classified depending on the use of video cameras in indoor environments and implied privacy concerns [4]. Three clusters can be identified (see Tab. 1): (1) Purely preventive solutions, (2) non-obtrusive alarm systems, and (3) obtrusive alarm systems.

How reliable can a security system perform its task? The base-rate fallacy [5] describes the difficulty of designing effective intrusion detection systems. Effectiveness is the ratio of relevant alarms to false alarms of the system. The absolute number of relevant alarms is low for security systems due to the low frequency of intrusions. In contrary, a high number of false alarms is likely even by reliable systems due to the commonness of the regular status. The base-rate fallacy is particularly relevant in the case of the presented low-cost systems.

Smart Home security communities try to leverage the crime-reducing effect of neighborhood watch approaches by using technology. First studies following this combination exist. Zeki et al. [6] present a technical approach which enables the sharing of video streams in order to evaluate the severity of an unusual event. The impact of such a solution is analyzed by a qualitative study of Microsoft research [7]. This study evaluates the use of shared outdoor cameras in order to detect suspicious activities. It shows the potential of such a solution, however also pointing out privacy concerns caused by the cameras fields of view and the constant use of the system.

In conclusion, the positive influence of neighborhood watch communities has been shown by various researchers [2]. The idea to complement these communities with Internet of Things based technologies is not new. However, due to privacy concerns, research efforts have been restricted to communities which use street cameras [7]. In contrast to existing approaches, our research focuses on the liaison of indoor security and communities.

The structure of this paper follows. First, this section introduced the field of Smart Home security communities and presented related work. Second, the following chapter evaluates users' intention to participate in a Smart Home security community and thereby especially focuses on privacy aspects. Third, we study the potential composition of a Smart Home security community. Finally, we discuss the gained results and further research directions.

2 Smart Home Security Communities - Evaluating the Idea

As a first step, we want to understand the value of Smart Home security communities for our security device. Thus, we address the following research questions. (1) 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? (2) Do powerful, yet privacy-intrusive security features such as video surveillance, increase or decrease potential users intention to use a Smart Home security system? (3) Do community and powerful, yet privacy-intrusive security features, have an interaction effect on users intention to use a Smart Home security system?

2.1 Study Design

We acquired 160 participants via Amazon Mechanical Turk [8] in exchange 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 ”Security Light” system and its motion detection technology. (2) More intrusive: The description of the Canary system[1] is taken as an example for a video based security 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 access the security system information. 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 measured the effects of our experiment. The metric assessing the intention to use was adapted from Davis [9]. To better understand the influence of privacy as a key constraint of intention to use [4], we measured privacy concerns based on Dinev and Hart [10].

2.2 Study Result

To assess the impact of community-based and privacy intrusive security features on the intention to use, we conducted a two-way Anova. 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. Furthermore, there was no significant main effect of community features on intention to use, F(1,160) =.37, p >.05. 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.

[1] http://canary.is/

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.

Applying these results, the study shows the value of a security community for our security solution. Due to privacy concerns, the study furthermore suggests a negative impact of a community on obtrusive security solutions.

3 Smart Home Security Communities - Understanding the Composition

As a second step, we want to study the composition of a Smart Home security community. We especially want to focus on the impact of private participants compared to institutions or companies.

3.1 Study Design

We acquired 50 participants via Amazon Mechanical Turk [8] in exchange for a small monetary compensation. Each participant had to evaluate eight person groups according to three criteria.

Person groups included private contacts and professionals. Private contacts were family, friends, neighbors, connections from a social network, and other users of a fictive security community named Beta. Professionals comprised the local police, security companies, and insurance companies. Person groups were shuffled during the study to avoid order effects.

Evaluation criteria comprised of three items: The ability of a person to act ("This person/institution could act appropriate in case of an intrusion."), perceived privacy ("I feel comfortable giving this person/institution access to the private data captured by the Beta security system") based on Dinev and Hart [10], and the intention to use ("I would ask this person/institution to support me in protecting my home and give him/her full access to the Beta app.") according to Davis [9].

3.2 Study Result

Figure 1 illustrates the results of our study. Three main findings follow: (1) The perceived ability to act is higher for family members and friends then for professional institutions while raising less privacy issues. (2) Users prefer sharing

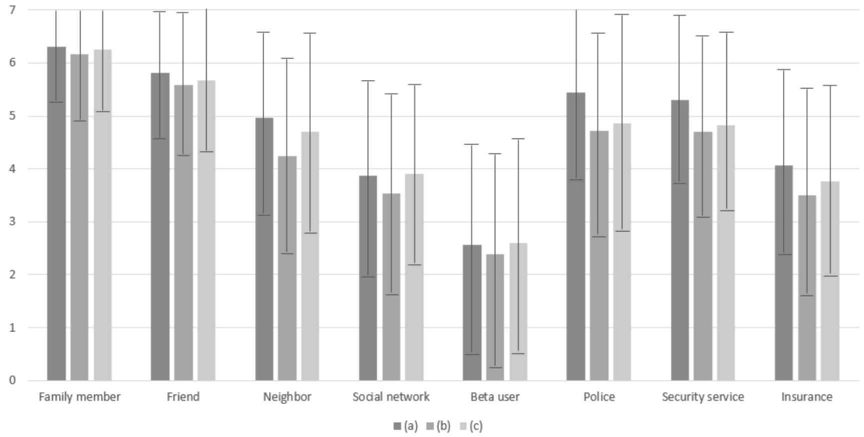

Fig. 1. Means and standard deviation of (a) ability to act, (b) perceived privacy during data sharing and (c) intention to invite in community depending on person characteristics.

data with family members and friends compared to their neighbors. (3) Anonymous members of social networks or security communities are the least preferable partners.

In consequence, security communities should leverage existing relationships to family members or friends. They can include neighbors or professionals. Furthermore, our study suggests not to rely on pure on-line relationships within the security community.

4 Discussion and Conclusion

Reflecting on the results, we see evidence for a general negative relationship between privacy-intrusive technology and the intention to participate in a security community. We expected that both non-intrusive and intrusive devices would benefit from a community. Therefore, we are surprised about the interaction effect between communities and privacy-intrusive technology. Our research suggests, that a positive community effect can only be achieved with non-privacy intrusive functionality.

We are furthermore surprised about the high perceived ability of family members and friends to act in case of an intrusion. Even though their means to intervene are limited, their perceived ability to act is the base for trustworthy Smart Home security solutions.

In line with [7], we encourage further research to explore the potentials of IoT-enabled security communities. We also see the potential to generalize the topic of Smart Home security communities and to apply to other research fields, e.g. ambient assisted living. AAL ensures the health, safety, and well-being of elderly people by the supervision of daily activities [11]. The reduction of false classifications, especially the elimination of false positives without the creation of false negatives, is a relevant research question [12]. Here, the local community of Smart Home security communities can be used for the manual verification of alarms.

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 thoughtful comments and helpful suggestions.

References

1. D. P. Rosenbaum. The Theory and Research Behind Neighborhood Watch: Is it a Sound Fear and Crime Reduction Strategy? *Crime Delinq.*, 33(1):103–134, January 1987.
2. Trevor Bennett, Katy Holloway, and David P. Farrington. Does Neighborhood Watch Reduce Crime? A Systematic Review and Meta-analysis. *J. Exp. Criminol.*, 2(4):437–458, December 2006.
3. L Sims and G Britain. Neighbourhood watch: findings from the 2000 British Crime Survey. 2001.
4. David H. Nguyen, Aurora Bedford, Alexander Gerard Bretana, and Gillian R. Hayes. Situating the Concern for Information Privacy Through an Empirical Study of Responses to Video Recording. In *Proc. SIGCHI Conf. Hum. Factors Comput. Syst.*, pages 3207 – 3216, New York, 2011. ACM Press.
5. Stefan Axelsson. The Base-Rate Fallacy and the Difficulty of Intrusion Detection. *ACM Trans. Inf. Syst. Secur.*, 3(3):186–205, 2000.
6. Akram M. Zeki, Elbara Eldaw Elnour, Adamu a. Ibrahim, Chiroma Haruna, and Sameem Abdulkareem. Automatic Interactive Security Monitoring System. In *Int. Conf. Res. Innov. Inf. Syst.*, pages 215–220. Ieee, November 2013.
7. A J Bernheim Brush, Jaeyeon Jung, Ratul Mahajan, and Frank Martinez. Digital Neighborhood Watch: Investigating the Sharing of Camera Data Amongst Neighbors. In *ACM Conf. Comput. Support. Coop. Work*, pages 693–700, 2013.
8. M. Buhrmester, T. Kwang, and S. D. Gosling. Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? *Perspect. Psychol. Sci.*, 6(1):3–5, February 2011.
9. Jr Davis and D Fred. *A technology acceptance model for empirically testing new end-user information systems: Theory and results.* PhD thesis, 1985.
10. T Dinev and P Hart. An extended privacy calculus model for e-commerce transactions. *Inf. Syst. Res.*, 17:61–80, 2006.
11. E Hoque and J Stankovic. AALO: Activity recognition in smart homes using Active Learning in the presence of Overlapped activities. *. . . Healthc. (PervasiveHealth), 2012 6th . . .*, 2012.
12. JA Botia, A Villa, and J Palma. Ambient Assisted Living System for In-home Monitoring of Healthy Independent Elders. *Expert Syst. Appl.*, 39(9):8136–8148, 2012.