Journal of Corporate Real Estate

Physical location of smart key activators - a building security penetration test
Jan-Willem Bullee, Lorena Montoya, Marianne Junger, Pieter Hartel,

Received 31 May 2017
Revised 8 December 2017
13 January 2018
Accepted 15 January 2018

Physical location of smart key activators – a building security penetration test

Jan-Willem Bullee
Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, Enschede, The Netherlands

Lorena Montoya
Faculty of Science and Technology, University of Twente, Enschede, The Netherlands

Marianne Junger
Faculty of Behavioral, Management and Social Sciences, University of Twente, The Netherlands, and

Pieter Hartel
Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, The Netherlands

Abstract

Purpose – When security managers choose to deploy a smart lock activation system, the number of units needed and their location needs to be established. This study aims to present the results of a penetration test involving smart locks in the context of building security. The authors investigated how the amount of effort an employee has to invest in complying with a security policy (i.e. walk from the office to the smart key activator) influences vulnerability. In particular, the attractiveness of a no-effort alternative (i.e. someone else walking from your office to the key activators to perform a task on your behalf) was evaluated. The contribution of this study relates to showing how experimental psychology can be used to determine the cost-benefit analysis (CBA) of physical building security measures.

Design/methodology/approach – Twenty-seven different "offenders" visited the offices of 116 employees. Using a script, each offender introduced a problem, provided a solution and asked the employee to hand over their office key.

Findings – A total of 58.6 per cent of the employees handed over their keys to a stranger; no difference was found between female and male employees. The likelihood of handing over the keys for employees close to a key activator was similar to that of those who were further away.

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TREsPASS). This publication reflects only the author's views and the Union is not liable for any use that may be made of the information contained herein.

Journal of Corporate Real Estate
Vol. 20 No. 2, 2018
pp. 138-151
Emerald Publishing Limited
1463-001X
DOI 10.1108/JCRE-05-2017-0014

Research limitations/implications – The results suggest that installing additional key activators is not conducive to reducing the building's security vulnerability associated with the handing over of keys to strangers.

Originality/value – No research seems to have investigated the distribution of smart key activators in the context of a physical penetration test. This research highlights the need to raise awareness of social engineering and of the vulnerabilities introduced via smart locks (and other smart systems).

Keywords Building management, Security, Social engineering, Building layout, Distance decay, Smart key

Paper type Research paper

1. Introduction

Real estate represents the second largest expense for most companies; hence, buildings are becoming increasingly automated to increase efficiency and drive costs down (Macht, 2016). This transformation brings about a paradigm shift in the sense that the reactive, closed and proprietary system approach to building management is no longer an option. (Macht, 2016). Digital information is crucial in this transformation, but it could introduce security risks. This paper explores a particular type of security risk that building automation involves, particularly one faced by Facility Management (FM) departments.

FM departments typically operate, maintain, improve and adapt an organisation's building infrastructure. Their role is to assist in creating an environment that supports the organisation's primary objective (Atkin and Brooks, 2009). Among other tasks, FM departments protect the organisation, their employees and assets from threats (Enoma, 2008). Vulnerability reduction involves identifying which measures are likely to counteract the threat(s). To this end, penetration testing helps establish the level of risks an organisation faces. The results of a penetration test therefore constitute inputs for a cost-benefit analysis (CBA) of security measures.

Managing building access control using metal keys is challenging for organisations having a large number of employees and multiple buildings. To maintain both privacy and security, employees are restricted to a limited number of rooms, resulting in an employee being in possession of several keys. In addition, losing or revoking a key is costly, considering that the lock has to be replaced and keys redistributed to guarantee the same level of protection. Furthermore, security can be compromised as some metal keys can be duplicated even on the basis of a photograph (Greenberg, 2014). Finally, there is no time restriction for the opening or closing of locks and there is no possibility to log access. To overcome these drawbacks, smart locks (also known as digital, electronic or mechatronic) locks can be used.

In a smart lock, the electronic components are an addition or a replacement of the traditional lock system. Smart locks use external authentication methods such as card readers or RFID tags, whereas traditional locks use metal keys (Hounsham, 2009). Furthermore, smart locks usually are part of a centralised access control system and either:

- receive a signal as to whether to grand access; or
- have an internal logic for making access decisions (Verma and Tripathi, 2010).

The benefit of using a smart lock system compared to a metal key system is the flexibility in managing access control for a large number of users (Weiner *et al.*, 2013).

New technology creates new threats and risks. A smart lock system contains six elements (Hounsham, 2009). For each element, the attack vector is listed:

(1) physical barrier (e.g. door): physical attack;
(2) electromechanical lock (e.g. motorised lock): physical and electrical attack;
(3) access control system (e.g. computer system): electronic attack;
(4) authentication device (e.g. card reader): electronic attack and surveillance;
(5) authentication method (e.g. swipe card): spoofing attack and electronic attack; and
(6) users (e.g. customer or admin): social engineering.

Each attack vector is briefly described below:

- A physical attack involves physical violence, tampering or misuse of chemicals.
- The electrical attack involves attempting to open a lock using simple electrical tools, e.g. by using a battery or a strong magnet. An example of the latter involves holding a strong magnet near the lock to move an internal pin and rotate the lock (Schneier, 2005).
- Electronic attacks target the computers, computer programmes or the computer network. At the 2016 DEF CON hackers conference, two security researchers presented their analysis results conducted on a dozen electronic locks (Rose and Ramsey, 2016). They performed a fuzzy electronic attack, which aimed at finding an error state. They succeeded and thus opened the lock.
- A spoofing attack involves one person or programme successfully impersonating another by falsifying data. The same two researchers at DEF CON 2016 performed this attack by retransmitting captured valid data. When no check is made on who is sending data, the reuse of a captured valid data stream is sufficient to unlock the door (Rose and Ramsey, 2016).
- Surveillance is the monitoring of user behaviour and activities. An example of such an attack is tailgating or piggybacking, which involves walking together with person who is authorised to gain access.
- Social engineering: the use of deception and manipulation to achieve a goal. Currently, the social engineering vulnerabilities caused by smart lock systems are unknown. Therefore, this topic will be investigated and discussed in more detail in the following section.

1.1 Social engineering

Social engineering is a type of attack that includes the use of social disguises and psychological tricks to make targets assist offenders in their attack (Abraham and Chengalur-Smith, 2010). An example of social engineering is the so-called "cold calls", a telephone scam that has been carried out by offenders claiming to belong to Microsoft's technical support department (Arthur, 2010). By convincing the targets that there is "a problem associated with their PC", offenders get access to bank accounts and defraud people. Offenders are aware that humans are a weak link in the security chain and therefore try to trick people into violating security policies. Social engineering is not bound to a single modality, e.g. social engineering via email also exists and is known as "phishing" email. One of the dangers of social engineering is that these attacks are designed to appear harmless

and look legitimate (The Federal Bureau of Investigation, 2013). People tend to think that they are immune to social engineering attacks, such as a cold call or a phishing email. However, this does happen, and it results from a cognitive bias called "optimism bias". This theory states that people believe that positive events are more likely to happen to them than to others (Weinstein, 1980). The inverse of this theory is also true; "negative events are more likely to happen to others".

How does one become a victim of social engineering? Once a person is targeted, the offender can use social influences to change the odds of compliance in his favour. Six social influences (referred to as persuasion principles) were investigated by Cialdini (2009): Authority, Conformity, Reciprocity, Commitment, Liking and Scarcity.

Authority is the principle that describes people's tendency to comply with the request of authoritative figures. If people are unable to make a thorough decision, the responsibility to do so is transferred to the group or someone they believe to be in charge. Crisis and stress activate the behavioural trait of responsibility transition. *Conformity*, or social proof, is the act of imitating the behaviour of other people. Members of the in-group have a stronger feeling of group safety compared with members of the out-group (Asch, 1951). *Reciprocity* refers to the giving of something in return. The target feels indebted to the requester for making a gesture, and even the smallest gift puts the requester in an advantageous position. *Commitment* refers to the likelihood of sticking to a cause or idea after making a promise or adhesion. In general, when a promise is made, people will honour it, which increases the likelihood of compliance (Cialdini, 2009). *Liking* puts a person in a favourable position. People tend to like others who are similar regarding interests, attitudes and beliefs. *Scarcity* occurs when a product, service or information has limited availability. People, therefore, perceive an increased value and attractiveness towards these products which makes them more desired than others.

To understand the type of security breach involved, we next provide a scenario. The office of a university lecturer is located on a second floor and can only be accessed by the lecturer who has the key. There is an exam in the office which is available both in printed form and in digital form i.e. stored in the computer. The PC is connected to the internet and is protected by a password which is only known to the lecturer. When the lecturer is away, the office is locked. An offender can obtain the exam by either: hacking into the PC of the lecturer or obtaining a physical copy from the office of the lecturer. To hack into the PC, the attacker needs: to bypass the firewall and then guess the password of the lecturer. The key, on the other hand, can be obtained by:

- manipulating the lecturer (i.e. social engineering) to obtain access to the office; or
- by picking the lock of the lecturer's office.

This paper involves the design and results of a penetration test aiming to investigate the extent to which the lecturer can be manipulated (i.e. socially engineered) into handing over his digital office key. The effort it takes the employee to activate his key is a key part of the manipulation carried out, hence this research aims to establish whether a relation exists between the distribution of key activators across the buildings and the handing over of keys.

1.2 Research question

The aim of this research was to answer the following question: "To what extent does the distribution of smart key lock activators in an office building promote secure behaviour?" One hypothesis was thus formulated which is provided later in the text. As there is (to the best of our knowledge) no literature available on the ideal placement of smart key lock activators in the context of a penetration test, we hypothesise that the amount of physical

effort needed to activate an office key influences the willingness of an employee to hand it over to a stranger.

2. Methods

The sample consisted of 116 subjects who work in two buildings on the University of Twente. Only people present in their office and whose office door had a specific type of lock were approached. The locks involved are smart locks and manufactured by WinkHaus (2014).

2.1 Subject selection

Professors, secretaries, support and laboratory staff members were excluded from the study to minimise disruption of primary activities. The pool of scientific staff subjects consisted therefore of PhD-candidates, Post-Doc researchers as well as of Assistant and Associate Professors.

The nationality and gender ($\chi^2 = 1.147$, $df = 1$, $p = 0.284$)[1] distribution of the data collected was comparable to the overall distributions of the target population. As the p-value is above 0.05, we cannot reject the hypothesis that there is no relation between gender and being a participant in the experiment. Hence, these are independent. However, those who participated in the experiment were older; 35 vs 41 years ($t = -3.311$, $df = 290$, $p = 0.001$). As the p-value is below the 0.05, we reject the hypothesis that there is no difference in the mean age of the subjects, therefore there is a difference in age.

2.2 Researchers

The researchers (i.e. the "offenders") performing the study consisted of 27 bachelor/master students (9 females and 18 males). The average age of the researchers was 21.42 years (SD = 1.38). In a previous research, the effect of both target and offender gender on compliance was tested and as no such effect was found (Bullée *et al.*, 2015); in this experiment, we set no restriction with regards to approaching subjects of the same gender.

2.2.1 Procedure. The Institutional Review Board (IRB) of the University approved the study before data collection was carried out. All subjects were individually approached by a researcher between 10 a.m. and 6 p.m. on a "normal" Thursday during term time. To avoid suspicion, researchers never made consecutive visits to members of the same department. After five visits, they had to come back to the base of operations (i.e. the first author's office) to obtain the names and locations of the next target, which was randomly selected from a list of all possible targets.

The researchers were randomly assigned to a target, however if the researcher recognised a target, this target was randomly assigned to another researcher. Each researcher approached the subject using the following script:

> Hi, I am [Name] and I work for Facility Management. I have a question regarding the door locks. We received several complaints about the door lock and the keys. Has unlocking the door ever been problematic for you? We have contacted the manufacturer about the malfunctioning and they had received other similar complaints. In order to solve the problem, the manufacturer sent us a measuring device to test the keys that are in use. I have to admit that I do not exactly know what the box measures, but the data collected is necessary for the manufacturer to analyse the situation and hopefully find a solution to the problem. Can I have your key for measurement?
>
> *After measuring the key*: I have to inform you that after reading your key, the key has been reset and needs reactivation downstairs. It is no problem for me to reactivate the key for you.
>
> **Request**: Is it OK with you if I do the reactivation of your key downstairs?

Each target was subjected to the same request. After the researcher obtained the key (refer to Figure 1) and walked away, he/she came back to return the key and orally debriefed the subject with regards to social engineering and handed a printed debriefing statement. During the debriefing session, the subject was asked some demographic information, the length of employment, their route to the activation point and to explain why they had (or not) handed the key over. Finally, the importance of not sharing information about the study with colleagues was explained; all subjects acknowledged this and agreed not to disclose anything. This was checked during the debriefing and none of the subjects stated having had prior knowledge of the study. Furthermore, no targets reported having received awareness training on the topic of social engineering, neither did they participate in other social engineering experiments. However, it is unknown whether they had been previously victims of social engineering.

2.3 Variables

The variables used in the analysis were: *compliance*, *building*, *target gender*, *offender gender*, *age*, *years of service*, *distance* and *floors*. Effort was measured using the variables *distance* and *floors*, as the literature shows that climbing stairs requires more effort than walking (refer to Appendix for more information on metabolic equivalent of task (MET)). The dependent variable *compliance* measured whether the subject complied with the request to hand over the keys. The dichotomous variable was dummy coded as 0 = did not comply, 1 = did comply. The independent categorical variable *building* measured the building where the subject was approached (1 = building 1, 2 = building 2). The independent dichotomous variable *gender* was measured for both the subjects and the researchers (i.e. offenders) and was dummy coded (0 = female, 1 = male). The independent continuous variable *age* measured the age in whole years at the moment of the attack. The independent continuous variable *years of service* measured the

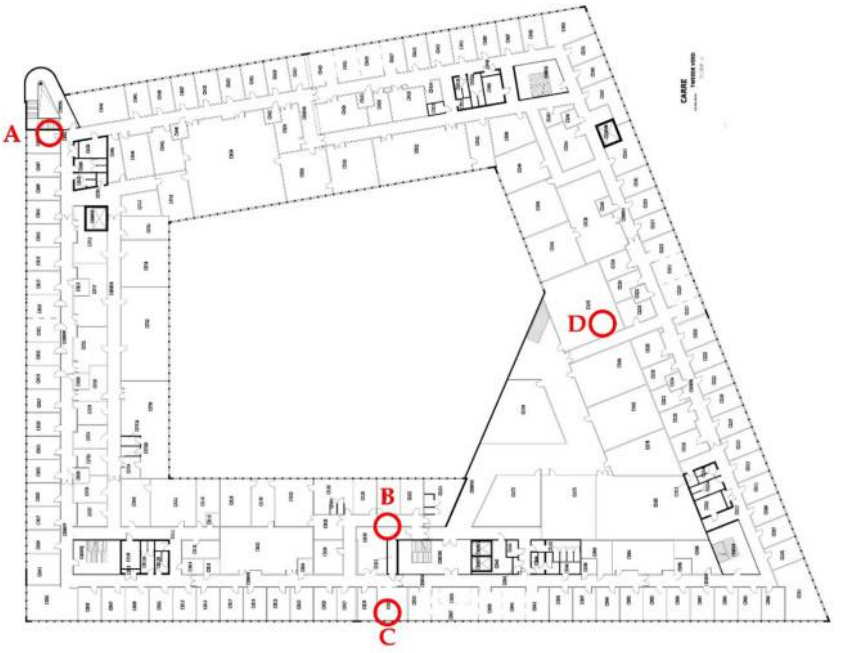
Figure 1.
WinkHaus smart key

length of a subject's employment for the organisation at the moment of attack. The independent continuous variable *distance* measured the distance the subject had to travel from the office to the activation point (1 = 1 metre of distance). The independent continuous variable *floors* measured the number of floors the subject had to travel from the office to the floor where the key activator is (1 = 1-floor difference).

2.4 Buildings

Building 1 has a circular layout. This building has five floor levels, refer to Figure 2 for the layout of its third floor. The main entrance is near Activator C; the side entrance is near Activator D and there is a further entrance in the form of a passage from another building near Activator A.

Building 2 has a very traditional rectangular layout. There is one straight corridor with offices on both sides. This building has five floor levels, refer to Figure 3 for a layout of its third floor. There are entrances near both activators.



Notes: Activator A is on floor 2; B is on floor 3; C is on floor 1; D is on floor 1

Figure 2.
Layout building 1, the red circles indicate the location of the digital key activators

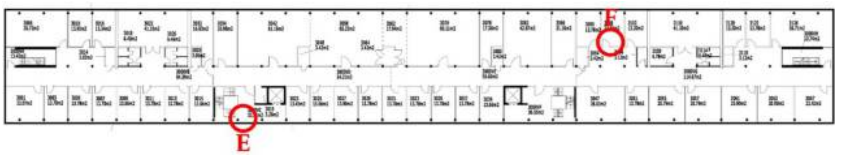


Figure 3.
Layout building 2, the red circles indicate the location of both digital key activators on floor 1

2.5 Analysis

The hypothesis was tested using logistic regression and a Kruskal–Wallis test. The following three logistic regression analysis assumptions were met: sufficient sample size, no multicollinearity and no outliers (Pallant, 2010). The data set had at least ten events per variable (EPV), which is considered as a minimum required for running a logistic regression (Peduzzi *et al.*, 1996). The variance inflation factor (VIF) was 2.02 for all the variables, which is below the cut-off value of 10, indicating no multicollinearity (Pallant, 2010). In the case of dichotomous variables, this means that one value should be placed in exactly one category.

The data did not fulfil the assumptions required to perform a *t*-test, i.e. data being normally distributed and the standard deviation of the populations being equal. Normality of the samples was tested using a Shapiro–Wilk test for normality (sample 1: $W = 0.885$, $N = 45$, $p = 0.000$ and sample 2: $W = 0.799$, $N = 64$, $p = 0.000$). As the p-value is below 0.05, the assumption of both the samples being normally distributed was rejected. Therefore, a *t*-test was inappropriate and a non-parametric alternative was used instead (i.e. Kruskal–Wallis test).

3. Results

A total of 116 subjects were contacted in the field study. The following variables had no effect on compliance and are therefore not further mentioned in this paper:

- *building* ($\chi^2 = 0.007$, df = 1, $p = 0.933$);
- *offender sex* ($\chi^2 = 0.574$, df = 1, $p = 0.449$);
- *target sex* ($\chi^2 = 0.045$, df = 1, $p = 0.153$);
- *age* ($\beta = 0.973$, $p = 0.115$); and
- years of service ($\beta = 0.991$, $p = 0.657$).

The performance (i.e. success) of the offenders ranged between 0 and 100 per cent. The number of "attacks" per offender ranged between 1 and 17. Refer to Table I for an overview of the success of each offender. A correlation was found between the number of attacks performed and the success rate of an offender ($r = 0.905$, $p = 0.000$).

H1. The amount of physical effort influences the willingness of an employee to hand over his office key to a stranger.

Out of the 116 targets, 68 (58.62 per cent) handed over their key. There was no significant difference in the *distance* from the office to the activator for those who did not surrender their key ($M = 27.2$, SD = 21.2) and those who did surrender their key ($M = 26.2$, SD = 23.3); $\chi^2 = 0.447$, $df = 1$, $p = 0.504$. For an overview of distances per building per floor, refer to Table II. The distance was tested for each building individually; there was no distance effect found in either building (Building 1: $\chi^2 = 0.222$, $df = 1$, $p = 0.637$, Building 2: $\chi^2 = 2.086$, $df = 1$, $p = 0.149$). Neither *distance*, number of *floors* nor *building* affected compliance. When controlling for one another, no effect was found either, refer to Table II. *H1* is therefore rejected in favour of *H1b*: "The amount of physical effort does not influence the willingness to hand over one's office key to a stranger".

During the debriefing, the subjects were asked to indicate why they did (or did not) hand over their key. Reasons for handing over the key included: "The story regarding the keys

Attempts	Success
1	0 (0.00%)
1	0 (0.00%)
1	0 (0.00%)
1	0 (0.00%)
1	0 (0.00%)
1	1 (100%)
1	1 (100%)
1	1 (100%)
2	0 (0.00%)
2	1 (50.00%)
2	1 (50.00%)
2	1 (50.00%)
2	2 (100%)
2	2 (100%)
2	2 (100%)
2	2 (100%)
3	1 (33.33%)
3	2 (66.67%)
3	3 (100%)
4	0 (0.00%)
5	3 (60.00%)
7	4 (57.14%)
9	5 (55.56%)
12	8 (66.67%)
14	12 (85.71%)
15	10 (66.67%)
17	6 (35.29%)

Table I.
Overview of attacks and success rates per offender

	Building 1						Building 2					
Floors	Did not comply			Did comply			Did not comply			Did comply		
0	31.89	(19.34)	7	47.28	(31.20)	5	–			–		
1	39.12	(12.49)	5	28.40	(14.75)	12	21.70	(8.20)	3	18.60	(11.39)	5
2	35.40	(40.57)	4	39.60	(25.54)	3	23.08	(13.07)	9	12.66	(6.26)	12
3	37.20	(0)	1	40.80	(0)	1	20.67	(3.20)	6	11.37	(8.47)	6
4	–			–			8.41	(5.28)	7	15.09	(8.36)	15
Total	35.15	(22.31)	17	35.09	(21.17)	21	18.23	(10.56)	25	14.19	(8.17)	38

Table II.
Overview of distances to the activator per building per number of floors for those who did and did not comply

Notes: The columns depict for each floor: the average distance from the subject's office to the activator, its standard deviation (in brackets) and its sample size

seemed legitimate", "I wanted to help Facility Management to solve the problem" and "Difficulty unlocking the door is a known problem". Reasons for not handing over the key included: "I don't know you", "I can reactivate the key myself", "My private keys are on the same key chain" and "This key can open multiple doors".

During the offender debriefing, it was reported that none of the subjects checked whether or not their key was deactivated by trying to lock their door. Furthermore, no subjects followed or accompanied offenders to the activation point.

4. Discussion

This study investigated whether the effort an employee has to invest in complying with a security policy (operationalised as distance and number of floors to the key activation point) influences the outcome of a penetration test involving a social engineering attack.

The likelihood of handing over the key for employees close to the activation point was similar than that of those further away. There was no difference between the two buildings. We therefore conclude that, in this context, there is no effect of physical effort on the compliance with a social engineering attack. From a CBA point of view, it is therefore not necessary to install additional activation points. However, as the majority of the employees handed over their office key to a stranger, the social engineering threat should be taken seriously and potential investments in countermeasures (e.g. awareness campaigns or employee training) should be evaluated (Table III).

The success rate of an offender increases with the number of attempts. The experience curve uses this phenomenon to explain an increase in productivity (Hirschmann, 1964; Hax and Majluf, 1982). By repeating a task over and over, skill is developed allowing it to be done more efficiently, confidently and with less hesitation. This concept is relevant for a social engineering attack. The level of offender nervousness was not measured before the first target was approached. This could explain the difference in offender success rates among those who only performed only a few attacks.

Our findings therefore suggest that people do not consider the effort when deciding whether to surrender their office key. Previous research, using the same experimental design, showed that using authority (operationalised via the type of clothing) also had no effect; however, informing people of the dangers, characteristics and countermeasures associated with social engineering proved to have a significant positive effect on neutralising the offender (Bullée *et al.*, 2015).

4.1 Limitations

This study has two limitations:

(1) The results of this study are based on a homogeneous sample of university personnel. Therefore, generalisation should be considered with caution. Besides the difficulty of obtaining data from similar organisations, using one's own data gives the most accurate insight.

(2) Effort was only operationalised via physical means. Possibly operationalisation including journey time together with distance and floors might reflect effort more adequately.

Table III. Comparison of the four models. The columns depict for each variable: the odds ratio (OR), its lower and upper 95 per cent confidence intervals [in brackets] and its significance level

Variable	Model 1: (d)		Model 2: (f)		Model 3: (df)		Model 4: (dfb)	
Distance	0.999	[0.982, 1.016]			0.991	[0.967, 1.016]	0.990	[0.964, 1.017]
Floors			1.064	[0.804, 1.407]	1.036	[0.744, 1.442]	1.062	[0.711, 1.587]
Building							0.878	[0.272, 2.833]
Constant	1.434	[0.796, 2.582]	1.085	[0.535, 2.203]	1.553	[0.496, 4.858]	1.866	[0.249, 14.00]

Notes: *$p < 0.05$; **$p < 0.01$; ***$p < 0.001$; D = distance; F = floors; B = building; Model 1 ($\chi^2 = 0.02$, $p = 0.896$), N = 110, pseudo $R^2 = 0.000$; Model 2 ($\chi^2 = 0.19$, $p = 0.665$), N = 112, pseudo $R^2 = 0.001$; Model 3 ($\chi^2 = 0.77$, $p = 0.681$), N = 102, pseudo $R^2 = 0.006$; Model 4 ($\chi^2 = 0.82$, $p = 0.846$), N = 102, pseudo $R^2 = 0.006$

4.2 Recommendations for practitioners

The results show that almost 60 per cent of the subjects surrendered their key. Therefore, it is advisable to develop an awareness campaign to counter this vulnerability. However, the use of awareness campaigns should be considered carefully for several reasons. In an attempt to reduce the disclosure of personal information among visitors of a shopping district, Junger *et al.* (2017) used two types of warnings. Although there was a general lack of effect for both interventions, there were indications of an adverse effect of the warnings. The study of Bullée *et al.* (2016) found that awareness raising is only effective for a short time. One should therefore keep in mind that a single round of awareness training is insufficient. High levels of repetition of the same message is not the solution either; this can produce adverse results (Stewart and Martin, 1994). The solution is likely to lie somewhere in the middle.

Regarding social engineering experiments, careful planning and consideration is necessary. As this typically involves conducting experiments on humans (e.g. employees), some ethical considerations must be taken into account (Belmont Report, 1979). Particular challenging is the use of deception as it conflicts with ethical principles (Code of Federal Regulations, 2005).

An alternative to overcome the problem of giving keys away is to use biometrics because it eliminates the sharing and disclosure of access tokens. A disadvantage is its monetary cost.

Finally, we present two suggestions for future research. First, the system tested required each employee to activate the key on a daily basis. The suggestion for future research is to test the decrease of the interval. Second, an alternative study could include a different medium, such as a swipe card or an RFID token which does not require activation.

Note

1. The following two data assumptions must be met for Chi-Square analysis: independence and minimum frequency of 5 observations per cell (Field *et al.*, 2012). Independence relates to putting a single observation in only one cell. In case one assumption is not met, the Fisher's Exact test should be used instead.

References

Abraham, S. and Chengalur-Smith, I. (2010), "An overview of social engineering malware: trends, tactics, and implications", *Technology in Society*, Vol. 32 No. 3, pp. 183-196, doi: 10.1016/j.techsoc.2010.07.001.

Ainsworth, B.E., Haskell, W.L., Herrmann, S.D., Meckes, N., Bassett, D.R., Tudor-Locke, C. and Leon, A.S. (2011), "2011 Compendium of physical activities: a second update of codes and met values", *Medicine and Science in Sports and Exercise*, Vol. 43 No. 8, pp. 1575-1581.

Arthur, C. (2010), "Virus phone scam being run from call centres in India", [Newspaper Article], avaiable at: www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres

Asch, S.E. (1951), "Effects of group pressure upon the modification and distortion of judgments", In Guetzkow, H. (Ed.), *Groups, Leadership, and Men*, pp. 177-190, Carnegie Press, Pittsburgh, PA.

Atkin, B. and Brooks, A. (2009), *Total Facilities Management*, John Wiley & Sons, Hoboken, NY.

Aziz, A.R. and Teh, K.C. (2005), "Physiological responses to single versus double stepping pattern of ascending the stairs", *Journal of Physiological Anthropology and Applied Human Science*, Vol. 24 No. 4, pp. 253-257, doi: 10.2114/jpa.24.253.

Bassett, D.R., Vachon, J.A., Kirkland, A.O., Howley, E.T., Duncan, G.E. and Johnson, K.R. (1997), "Energy cost of stair climbing and descending on the college alumnus questionnaire", *Medicine and Science in Sports and Exercise*, Vol. 29 No. 9, pp. 1250-1254.

Belmont Report (1979), "The belmont report: ethical principles and guidelines for the protection of human subjects of research".

Brooks, A.G., Gunn, S.M., Withers, R.T., Gore, C.J. and Plummer, J.L. (2005), "Predicting walking mets and energy expenditure from speed or accelerometry", *Medicine and Science in Sports and Exercise*, Vol. 37 No. 7, pp. 1216-1223.

Bullée, J.H., Montoya, L., Junger, M. and Hartel, P.H. (2016), "Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention", in Mathur, A. and Roychoudhury, A. (Eds), *Proceedings of the inaugural singapore cyber security R&D conference (sg-crc 2016), Singapore, Singapore*, Vol. 14, pp. 107-114, *IOS Press*, *Amsterdam*, doi: 10.3233/978-1-61499-617-0-107.

Bullée, J.H., Montoya, L., Pieters, W., Junger, M. and Hartel, P.H. (2015), "The persuasion and security awareness experiment: reducing the success of social engineering attacks", *Journal of Experimental Criminology*, Vol. 11 No. 1, pp. 97-115, doi: 10.1007/s11292-014-9222-7.

Byrne, N.M., Hills, A.P., Hunter, G.R., Weinsier, R.L. and Schutz, Y. (2005), "Metabolic equivalent: one size does not fit all", *Journal of Applied Physiology*, Vol. 99 No. 3, pp. 1112-1119, doi: 10.1152/japplphysiol.00023.2004.

Cialdini, R. (2009), Influence, HarperCollins.

Code of Federal Regulations (2005), Title 45: Public Welfare, Department of Health and Human Services, Part 46: Protection of Human Subjects.

Cole, A. and Ogbe, J. (1987), "Energy intake, expenditure and pattern of daily activity of Nigerian male students", *The British Journal of Nutrition*, Vol. 58 No. 3, pp. 357-367.

Crouter, S.E., Clowers, K.G. and Bassett, D.R. (2006), "A novel method for using accelerometer data to predict energy expenditure", *Journal of Applied Physiology*, Vol. 100 No. 4, pp. 1324-1331, doi: 10.1152/japplphysiol.00818.2005.

Enoma, N.A. (2008), "Developing key performance indicators for airport safety and security: a study of three scottish airports", Unpublished doctoral dissertation, Heriot-Watt University.

Field, A., Miles, J. and Field, Z. (2012), *Discovering Statistics Using r*, SAGE Publications, London.

Greenberg, A. (2014), "The app I used to break into my neighbor's home", available at: www.wired.com/2014/07/keyme-let-me-break-in/ (accessed 18 November 2016).

Hax, A.C. and Majluf, N.S. (1982), "Competitive cost dynamics: the experience curve", *Interfaces*, Vol. 12 No. 5, pp. 50-61.

Hirschmann, W.B. (1964), "Profit from the learning-curve", *Harvard Business Review*, Vol. 42 No. 1, pp. 125-139.

Hounsham, T. (2009), "Evaluating access control locks against low technology attacks", In *43rd Annual 2009 International Carnahan Conference on Security Technology*, *IEEE*, *Zurich*, pp. 329-334, doi: 10.1109/CCST.2009.5335514.

Jette, M., Sidney, K. and Blümchen, G. (1990), "Metabolic equivalents (mets) in exercise testing, exercise prescription, and evaluation of functional capacity", *Clinical Cardiology*, Vol. 13 No. 8, pp. 555-565.

Jones, A.Y., Chak, D.M., Kwong, C.K., Leung, W.W., Ngan, K.K., Pang, C.W. and Choi, B.K. (2006), "Oxygen consumption during stair ascent and descent a comparison between subjects with normal and impaired vision", *Hong Kong Physiotherapy Journal*, Vol. 24 No. 1, pp. 23-27, doi: http://dx.doi.org/10.1016/S1013-7025(07)70005-2.

Junger, M., Montoya, L. and Overink, F.-J. (2017), "Priming and warnings are not effective to prevent social engineering attacks", *Computers in Human Behavior*, Vol. 66 No. 1, pp. 75-87, doi: http://dx.doi.org/10.1016/j.chb.2016.09.012.

Kozey, S.L., Lyden, K., Howe, C.A., Staudenmayer, J.W. and Freedson, P.S. (2010), "Accelerometer output and met values of common physical activities", *Medicine and Science in Sports and Exercise*, Vol. 42 No. 9, p. 1776.

Macht, H. (2016), "The digitisation of buildings is here", available at: www.smartbuildingsmagazine.com/features/the-digitisation-of-buildings-is-here (accessed 10 January 2018).

Pallant, J. (2010), *Spss Survival Manual: A Step by Step Guide to Data Analysis Using SPSS*, McGraw-Hill Education, New York, NY.

Parkka, J., Ermes, M., Antila, K., Van Gils, M., Manttari, A. and Nieminen, H. (2007), "Estimating intensity of physical activity: a comparison of wearable accelerometer and gyro sensors and 3 sensor locations", *Engineering in Medicine and Biology Society, 2007. EMBS 2007. 29th Annual International Conference of the IEEE, Lyon*, pp. 1511-1514, doi: 10.1109/IEMBS.2007.4352588.

Peduzzi, P., Concato, J., Kemper, E., Holford, T.R. and Feinstein, A.R. (1996), "A simulation study of the number of events per variable in logistic regression analysis", *Journal of Clinical Epidemiology*, Vol. 49 No. 12, pp. 1373-1379, doi: 10.1016/S0895-4356(96)00236-3.

Rose, A. and Ramsey, B. (2016), "Picking bluetooth low energy locks a quarter mille away", available at: www.youtube.com/watch?v=KrOReHwjCKI (accessed 10 November 2016).

Schneier, B. (2005), "Flaw in winkhaus blue chip lock", available at: www.schneier.com/blog/archives/2005/03/flaw_in_winkhau.html (accessed 12 November 2017).

Stewart, D.W. and Martin, I.M. (1994), "Intended and unintended consequences of warning messages: a review and synthesis of empirical research", *Journal of Public Policy & Marketing*, Vol. 13 No. 5, pp. 1-19.

The Federal Bureau of Investigation (2013), "Internet social networking risks", Vol. 2013 No. 4 October, US Department of Justice, available at: www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks (accessed 23 October 2013).

Verma, G.K. and Tripathi, P. (2010), "A digital security system with door lock system using rfid technology", *International Journal of Computer Applications*, Vol. 5 No. 11, pp. 6-8, (Published By Foundation of Computer Science).

Weiner, M., Massar, M., Tews, E., Giese, D. and Wieser, W. (2013), "Security analysis of a widely deployed locking system", *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 929-940, *ACM, New York, NY*, doi: 10.1145/2508859.2516733.

Weinstein, N.D. (1980), "Unrealistic optimism about future life events", *Journal of Personality and Social Psychology*, Vol. 39 No. 5, p. 806, doi: 10.1037/0022-3514.39.5.806.

Winkhaus (2014), Winkhaus access organisation – product manual.

Further reading

Mei Yin, D.B., Kamal, M.I., Azmanuddin, N.S., Ali, S.H.S., Othman, A.T. and Chik, R.Z.W. (2016), "Electronic door access control using myaccess two-factor au- thentication scheme featuring near-field communication and eigenface-based face recognition using principal component analysis", *Proceedings of the 10th International Conference on Ubiquitous Information Management and Communication*, pp. 1:1-1:8, *ACM, New York, NY, USA*, doi: 10.1145/2857546.2857548.

Ong, A. (2015), "Homebuilt: how to assemble an electronic door lock", *IEEE Potentials*, Vol. 34 No. 5, pp. 43-47, doi: 10.1109/MPOT.2015.2428751.

Salto (2016), Wire-free electronic locking solutions – product overview 2016.

SimonsVoss. (2015), Product catalogue 2015.

Appendix. A metabolic equivalent of task

MET is a physiological measure to express the energy cost of physical activities (Jette *et al.*, 1990). The measure used is a ratio (i.e. the rate of energy consumption), based on the oxygen consumption, compared to an average person seated in a chair at rest. The reference rate is, set by convention, at 3.5 ml $O_2 \cdot kg^{-1} \cdot min^{-1}$ or equivalently: 1 MET $\equiv 1\ {}^{kcal}/_{kg*h} \approx 17.5W$ for a person of 70 kg. It should be noted that this measure depends on the body mass of a person. Therefore, the energy consumption for the same task will differ across persons (Jette *et al.*, 1990). The METs are established for many different activities (e.g. gardening, rowing or tennis). The average MET for:

- climbing stairs is 6.23 (Ainsworth *et al.*, 2011; Brooks *et al.*, 2005; Kozey *et al.*, 2010; Jette *et al.*, 1990; Byrne *et al.*, 2005);
- descending stairs is 4.35 (Bassett *et al.*, 1997; Cole and Ogbe, 1987; Crouter *et al.*, 2006; Jette *et al.*, 1990; Kozey *et al.*, 2010; Parkka *et al.*, 2007); and
- walking horizontally is dependent of speed in km/h (METs = −0.17 + [speed * 0.79]) (Aziz and Teh, 2005; Bassett *et al.*, 1997; Jones *et al.*, 2006; Parkka *et al.*, 2007; Kozey *et al.*, 2010), for an overview of descriptives refer to Table AI.

METs are a measure that therefore allows expressing task intensity, whereby climbing stairs (i.e. the average of walking down and up) involves more effort than walking.

Table AI. Descriptive statistics of METs for 3 different activities

Activity	Samples	Avg METs (SD)	Minimum	Maximum
Walking	11	4.88 (1.07)	1.8	5.0
Stairs climbing	5	6.23 (2.15)	4.0	9.6
Stairs descending	7	4.35 (1.60)	2.9	6.4

Corresponding author
Jan-Willem Bullee can be contacted at: j.h.bullee@utwente.nl