Does Encryption Actually Engender Trust?

Cameron C. Gray[a], Dr. S. P. Mansoor[a]

[a]*Bangor University, Bangor, United Kingdom*

Abstract

In the modern Internet age, developers and administrators include encryption in their services as a matter of course. It is frequently described as the crucial enabling technology for many applications. Does encryption actually inspire trust from the users?

This paper examines the link between trust and encryption by soliciting opinions from 79 users including highly knowledgeable professionals as well as novices. Contrary to intuition, the main finding here is that encryption alone does not necessarily improve the amount of trust placed in secured services.

Keywords: encryption, trust, analysis, HCI, attitudes
2010 MSC: 97-P70, 68-P25, 94-A60, 68-M12, 68-U35, 90-B18

1. Introduction

Confidentiality, Integrity and Availability (the CIA triad) are the three quoted properties for a secure communication system. Confidentiality ensures that only the intended recipients are able to read the message. Integrity assures that the message has not been damaged or altered during transit and Availability means the system must be ready for use whenever required. Of the three, encryption supports the C and I properties. Encryption produces cipher-text that only the bearer of the correct key can transform back into the message. Integrity is ensured through hashing functions, a one-way transformation which produces a unique output for every unique input.

Technologists and researchers are almost universally in favour of encryption due to the data protection it provides. Yet very few [1] consider the human aspect of this proposition. Is including encryption purely a 'developer concern' that the users need not be aware of? We aim to examine if and how the use of encryption

Email addresses: c.gray@bangor.ac.uk (Cameron C. Gray), s.mansoor@bangor.ac.uk (Dr. S. P. Mansoor)

affects the attitudes of users of secured systems. The hypothesis of this study is that encryption inspires social trust in on-line systems.

The rest of this paper is organised as follows. Section 2 presents a survey of existing literature surrounding our subject. Section 3 describes the experimental protocol and metrics used. Section 4 presents the results produced by the experiment, which are then analysed and discussed in Section 5. Section 6 provides our final summation and conclusions.

2. Literature Survey

2.1. Encryption Methods

The origins and operations of encryption algorithms are almost relegated as a historical curiosity due to the availability of pre-written libraries [2]. Research still continues into the validity of these algorithms and techniques [3, 4, 5], but this is almost invisible to the world at large until a potentially catastrophic breach occurs [6, 7].

Existing evaluations of cryptography schemes assess their mathematical soundness [8, 9, 10], comparative performances [11, 12, 13, 14], as well as various utility metrics [15, 16] including privacy [17, 18, 19].

2.2. Trust in Electronic Commerce

Research into causes and indicators of trust in electronic commerce found that making consumers feel in control of the commerce process positively influences their behaviour [20, 21, 22]. Further studies suggest methods to increase the trust in the process or generate more trust from visitors [23, 24]. Gefen and Heart [25] focus on the end-goal of commerce - the financial benefit - and the role that trust plays to enable that goal. McKnight and Chervany [26] identify a complex interplay of factors that cause a site to be trusted.

The topic has been examined from the opposite side. 'What is needed to inspire trust so that the trusting party may be exploited?' [27, 28]. One of Jakobsson's findings is that using the Verisign's 'protected by' logo causes participants to believe the content is safe. The finding holds true when the content used is not secured or secured using an alternative vendor's services.

These studies, however, do not address whether the technology itself is responsible for the trust. It has been documented that geographical and cultural customs and identities also play a role in determining the overall trustworthiness of any given e-commerce proposition [29, 30, 31].

2.3. Trust within Ubiquitous Computing

Cloud computing introduces a data protection problem as storage can be located anywhere on the planet. Langhenrich has questioned the wisdom of current cloud security models that try to mimic the human trust decision in software [32]. Whilst Ko et. al. present a method of causing trust in cloud resources by introducing accountability as the missing motivator [33]. Ceutillo, Molva and Strufe have attempted to devise a storage scheme that replaces the shared mathematical keys with real-world trust relationships in order to protect data and privacy [34].

2.4. Human-Computer Interaction (HCI)

The HCI studies have focused on the usability aspects of the encryption tools [35, 36]. These studies advocate hiding superfluous information regarding the underlying technology in favour of a simple, easy to notice prompts. The studies based on user attitudes place the participants in a very specific scenario, asking what factors are most important in that scenario [37, 38]. In these studies 'security' ranks among the top three factors, but the nature of this security is not explored.

3. Methods

3.1. Hypotheses

We seek an answer to the question 'Does encryption engender trust?' by raising the following sub-hypotheses:

SH1. Experience with cryptography increases trust in institutions, people and services protected by cryptography.

SH2. Encryption strengthens the pre-existing trust in people and institutions providing on-line services.

SH3. There is a link between participants' experience with cryptographic products and their views on the causes of possible failings of cryptography.

SH4. Traits that prompt trust in people are similar to the traits used to evaluate trust in secured systems.

SH5. Stronger identification (of the user) through cryptographic signatures reduces the likelihood of system abuse.

3.2. Questionnaire

A questionnaire was prepared to gather the participants' data, and was deployed via the LimeSurvey on-line questionnaire tool. The questions were broken into four groups:

G1. User information (industry, career level, operating system usage).

G2. Experience with encryption.

G3. Trusting institutions and people.

G4. Trusting encryption.

The questions for groups G2-G4 are shown in Appendix A.

3.3. Metrics

Let $\mathbf{x}^{(2)} = [x_1^{(2)}, \ldots, x_9^{(2)}]^T$ be the participant's answers to Question 1, reflecting their experience of encryption. The Previous Experience Metric (PEM) is defined as:

$$\mathrm{PEM}(\mathbf{x}^{(2)}) = \sum_{i=1}^{9} (3 - x_i^{(2)}). \tag{1}$$

As the answers are coded using 1 for 'yes', 2 for 'uncertain' and 3 for 'no', the highest. The lowest value of PEM is 0, corresponding to answer 'no' to each questions; the largest value, indicating the most extensive experience is 1.

The measure for the non-contextual trust participants have in institutions, NCT, is calculated as the sum of the answers to Question 2, $\mathbf{x}^{(3)} = [x_1^{(3)}, \ldots, x_8^{(3)}]^T$. The Non-contextual Trust Metric (NCT) is

$$\mathrm{NCT}(\mathbf{x}^{(3)}) = \sum_{i=1}^{8} (3 - x_i^{(3)}). \tag{2}$$

This metric is coded and scaled using the same method as for our PEM.

The System Traits Importance Metric (STIM) is obtained from Question 4, where the answers were encoded as 1 for 'increase', 0 for 'same' and -1 for 'decrease'

$$\mathrm{STIM}(\mathbf{x}^{(5)}) = \sum_{i=1}^{4} (x_i^{(5)} + 1) \tag{3}$$

Value -1 for STIM indicates indicates largest decrease of importance while value $+1$ indicates largest increase.

The Encryption-based Scenario Trust (EST) metric comes from Question 5, where answers were encoded again as 1 for 'yes', 2 for 'uncertain' and 3 for 'no'.

The EST measure, scaled between 0 (most negative response) and 1 (most positive response) is

$$\mathrm{EST}(\mathbf{x}^{(6)}) = \sum_{i=1}^{8}(3 - x_i^{(6)}). \tag{4}$$

Question 6 asked the participants about the value of various aspects of encryption taking into account the widely publicised Heartbleed [6] and POODLE [7] attacks. The answers were encoded as 1 for 'increase', 0 for 'same' and -1 for 'decrease'. The Impression of Encryption Metric (IEM), scaled between 0 and 1, is

$$\mathrm{IEM}(\mathbf{x}^{(7)}) = \sum_{i=1}^{4}(x_i^{(7)} + 1) \tag{5}$$

3.4. Statistical Methods

This study measures several factors independently therefore reliability must be measured separately for each, using Cronbach's Alpha [39]. In order to prove our sub-hypotheses, we will need to find correlations between the various metrics. As the data is based on numerically coded responses, it remains essentially ordinal. We have therefore chosen the Spearman's Rank Correlation [40] algorithm. Each sub-hypothesis requires a different correlation, shown below:

- SH1: PEM v. EST metric
- SH2: NCT metric v. EST metric
- SH3: PEM v. IEM
- SH4: Ranking of Personal Traits v. STIM

Proof for sub-hypothesis 5 will be obtained through the relative proportions in the responses to question 7. As this is a direct question, no further statistical analysis is required.

4. Results

4.1. Demographics

We presented an identical questionnaire to a convenience sample [41] of Internet-related industrial professionals, both technical and non-technical university students and other self-selecting individuals. There were no qualification criteria of any kind. Out of the total respondents, 79 participants fully completed the questionnaire and gave consent for their data to be used. The breakdown of the participants by industrial sector is shown in Figure 1.

Eighty eight percent of the respondents indicated that they use the three major operating systems (Microsoft Windows™, Linux and OS X™) most often. The remainder either use a mobile operating system or one that was not listed. Figure 2 shows the full breakdown.

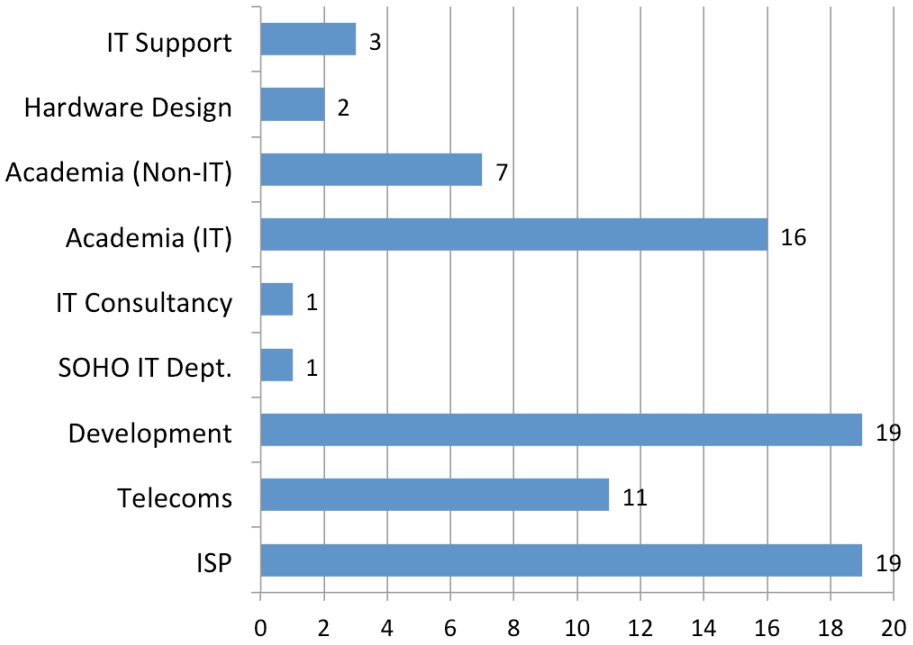

Figure 1: Participant Count by Industrial Sector

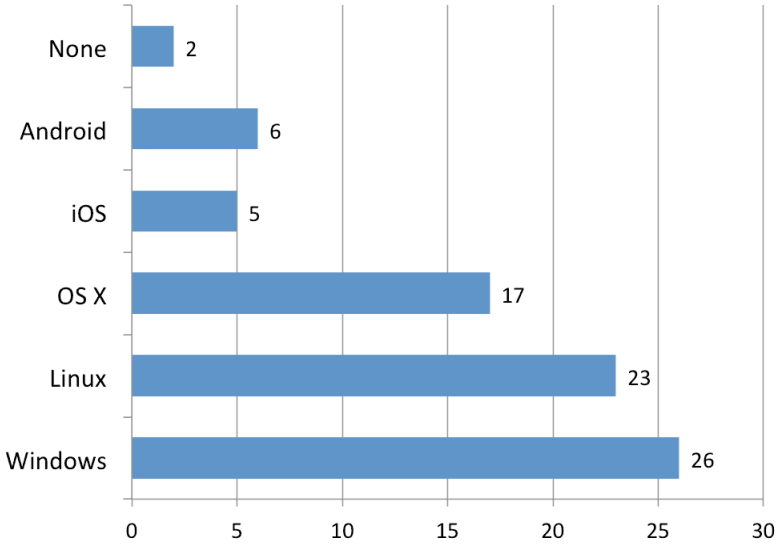

Figure 2: Participant Count by Most Utilised Operating System

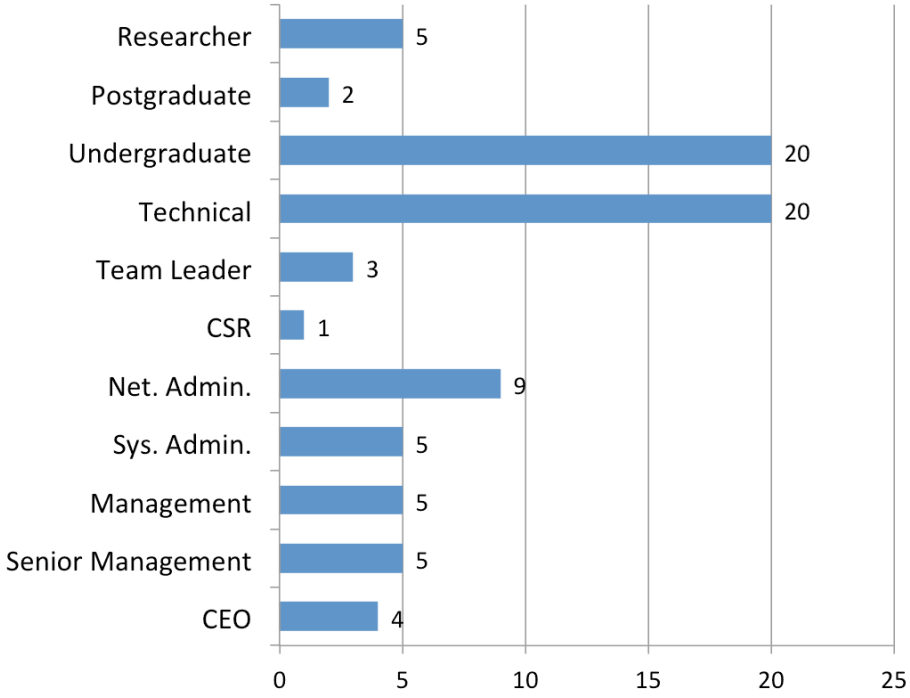

Figure 3: Participant Count by Occupation Level.CSR - Customer Service Representative

Whilst the study relies on a convenience sample, the occupational levels of the participants shows a much needed variety (Figure 3).

4.2. Metric & Comparative Results

Figures 4 to 6 show the scatter plots of the relationships between the various metrics required to prove sub-hypotheses 1-3.

The IEM is comprised of four components, all seeking the relative importance of differing components *after* publicised exploits on cryptographic software. Figure 7 shows the relative percentage of responses.

Figure 8 shows the relative percentages of participant responses when ranking personality traits in order of importance. Rank 1 being the most importance and 8, the lowest. For those traits that could be recognised in a system, participants were asked to rate their relative importance. The distribution of responses is shown in Figure 9. Figure 10 shows the relative percentages influenced by each hypothetical system response for abuse.

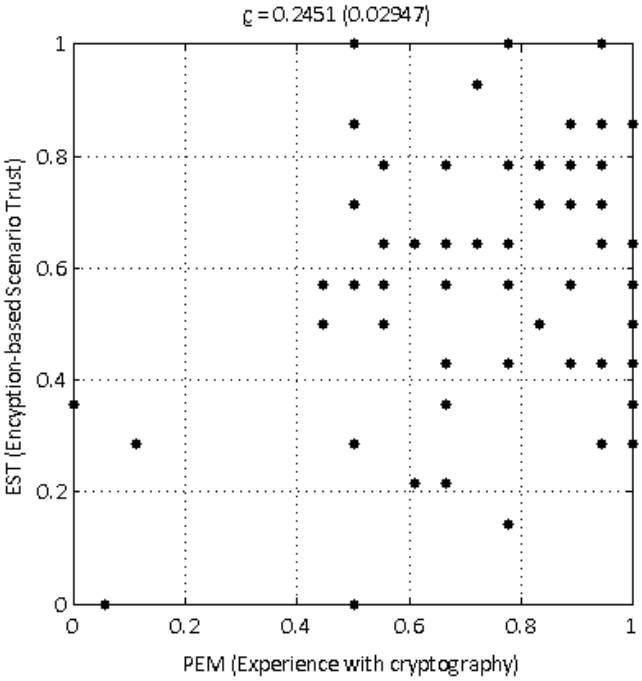

Figure 4: Scatter-plot of PEM and EST Metrics

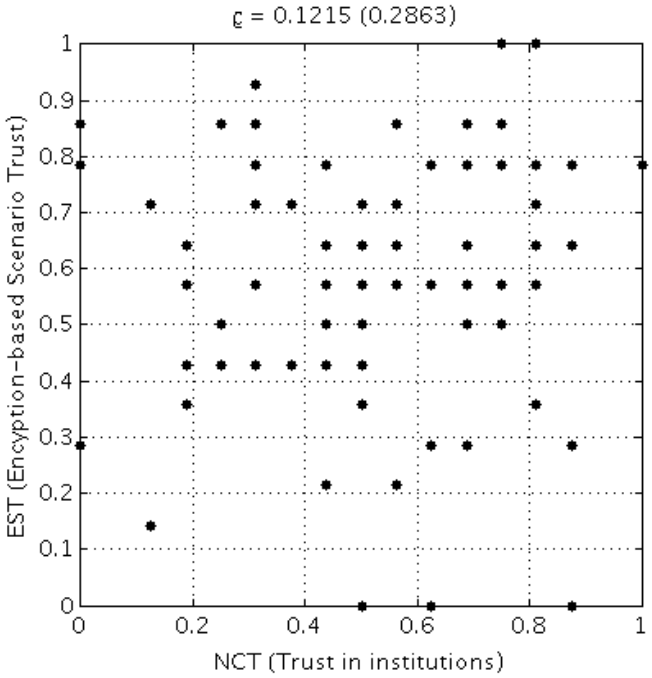

Figure 5: Scatter-plot of EST and NCT Metrics

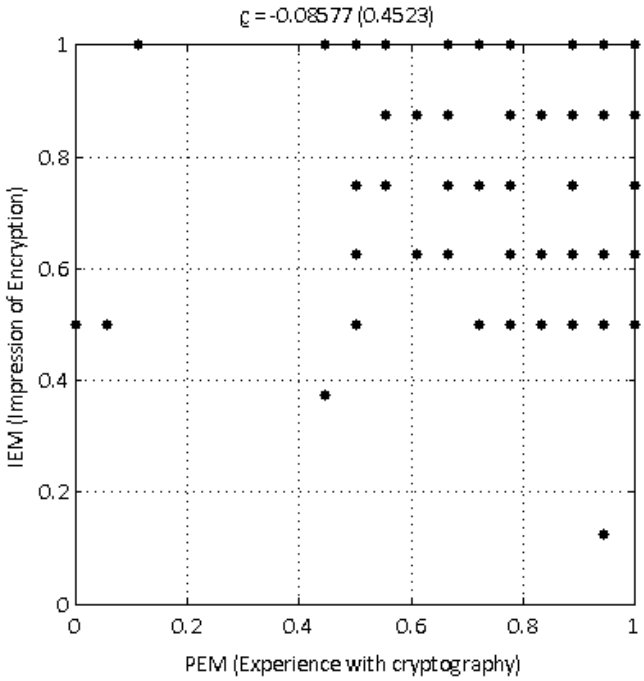

Figure 6: Scatter-plot of PEM against IEM

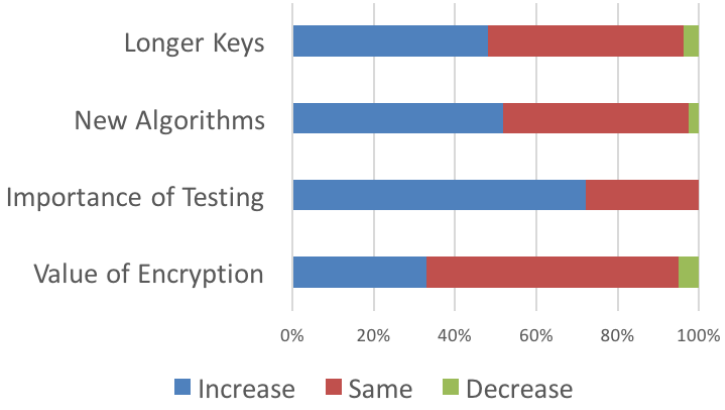

Figure 7: Response Distribution for Value of Features After Cryptography Exploits

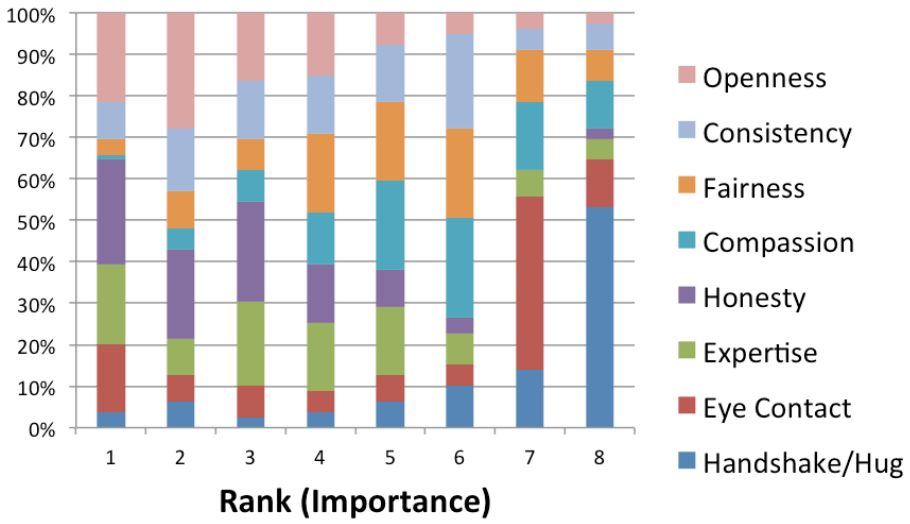

Figure 8: Personal Trait Importance for Inspiring Trust

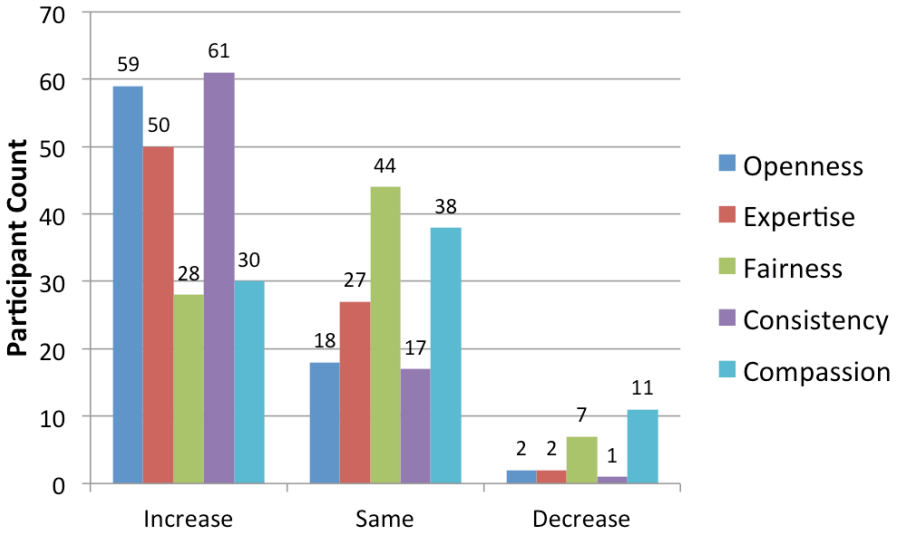

Figure 9: Relative Importance of Traits When Trusting a System

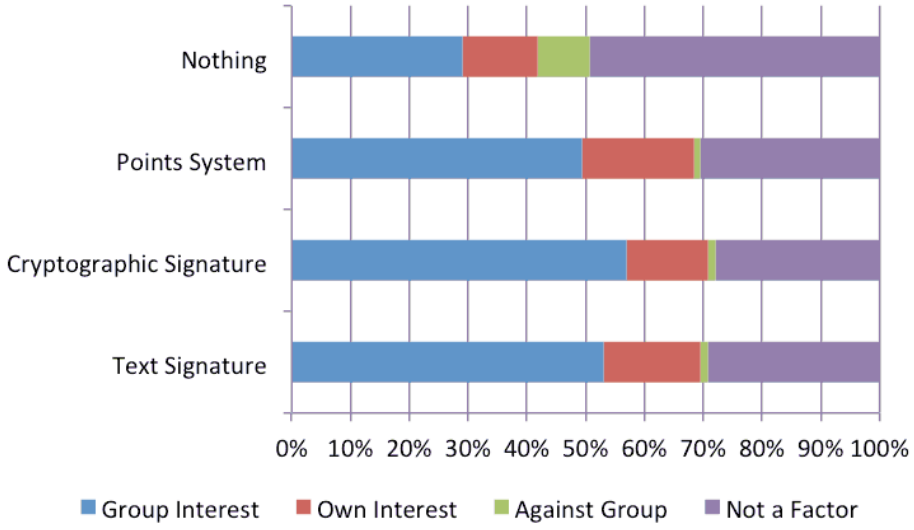

Figure 10: Hypothetical Responses by Threat/Punishment Type

4.3. Reliability

The α value calculated for our PEM, was 0.85191. Removing any feature results in a lower α value, as such this is not required for using PEM in further analysis. The NCT metric features produce an α value of 0.71394. When feature 5 (trust in a takeaway pizza company) is removed, the α value increases to 0.73273. Removing this feature detracts from the utility of the NCT metric, therefore we have decided not to remove it. The α value calculated for STIM, IEM and the EST metric are below the usual benchmark for 'acceptable' reliability (0.7 [42]). The values are 0.57377, 0.63993 and 0.69088 respectively, removing any constituent feature from any metric results in a lower value. Cronbach's Alpha measures similarity between elements in a single scale. We are studying the impact of these factors, so varying responses are expected and welcomed.

5. Analysis

As detailed in Section 3.4, we were looking for correlations between our metrics. The scatter-plot of PEM against EST shows a relationship, borne out by the rank correlation. The coefficient shows a weaker positive correlation between the metrics (0.2451), significant at $\alpha = 0.05$ levels. This helps support our sub-hypothesis 1, showing that more knowledge appears to lead to a greater trust in encryption scenarios. Among software development professionals there is a negative correlation -0.55 (at $\alpha = 0.05$), indicating that developers hold encryption in high regard, but have no personal experience in utilising

the technologies. This has relevance to our question as most services utilise encryption techniques 'behind the scenes'.

There is no statistically significant correlation between our NCT metric, measuring trust in institutions, and our EST metric, measuring trust in encryption scenarios. We cannot draw any conclusions from this as the metrics are not strict 'before and after' situations. Even when examining subgroups, with greater than 10 members, there is a negative correlation (-0.44) for OS X users. There is an opposite correlation for those in academia studying IT disciplines. However, these are only significant at an $\alpha = 0.1$ level. It is not possible to use this data to prove sub-hypothesis 2. The scatter- plot (Figure 5) suggests there may be some general relationship, but is confounded by other factors.

Whilst attempting to prove sub-hypothesis 3, we have found no significant correlations between the two metrics, PEM and IEM, as a whole or within any sub-populations. However, if we take each component of the IEM separately we find a $\alpha < 0.05$ significant positive correlation (0.2244) between our EST metric and the views on new algorithms solving cryptographic exploits. This correlation, in itself, is not but belies deeper understanding of cryptography as there is an almost opposite significant correlation between the participants' experience (the PEM) at -0.2348.

Correlating traits that make either people or systems trustworthy presents a challenge. Some of these traits cannot be possessed by a system, such as honesty or warmth. The mode of responses in each of the positions, revealed an bias toward intrinsically human traits. From most important to least; Honesty, openness, honesty, fairness, compassion, compassion, eye contact and a firm handshake/warm hug. Two alternative traits, expertise and consistency, were selected but not as the top selection in each rank. There is no statistically significant correlations between STIM and any of the top 5 rankings individually. There is a correlation with participants' sixth ranking choice - however, we consider this to be unrelated. As such we cannot statistically prove sub-hypothesis 4. When examining the numeric results as relative proportions, we find that the less favoured traits and more important to trusting a system than a person. Alan Turing touched on a similar set of view in 'Computing Machinery and Intelligence' [43]. Anecdotally, we can say that computers are trusted less but held to a higher standard of accuracy. For example, many would be rightfully annoyed if an ATM failed to dispense a correct amount, but would dismiss the mistake if made by a human teller. Our data supports sub-hypothesis 4 in that the same traits are used to compare trustworthiness, however they are applied in differing orders and weights.

When examining the effect of encryption influencing user behaviour (our sub-hypothesis 5), numerically we find that the most benevolent behaviour is caused when a cryptographic signature is used. It may only be a 6% improvement over a text attribution, however this represents a 27% improvement over the control situation (no consequence). It can be argued that hypothetical situations do not

provide the proper stimuli to force participants to act in their true nature. We have considered and dismissed this effect, as it allows participants to overstate their disobedience when they would be unlikely to act that way in reality.

There are some statistical correlations that we are able to draw. Participants' responses when a text signature is enforced has a negative correlation (-0.2377) at $\alpha < 0.05$ significance to their NCT score. Also when using text signatures, there is a positive correlation (0.2347) with their PEM score, at the same significance level. Interestingly, 25.31% (20/79) of participants indicated that no potential consequence would sway their decision, but no participant would deliberately act against the group in all four situations. Using Cronbach's Alpha we investigated the internal reliability of this question (with all four sub-questions), revealing $\alpha = 0.8942$. If the 'No consequence' option were removed this value increases to 0.9193. The Spearman's correlation of sub-questions were high;

- Text Attribution v. Cryptographic Signature - 0.7838 ($p < 0.01$),
- Text Attribution v. Points System - 0.6754 ($p < 0.01$),
- Text Attribution v. Points System - 0.6754 ($p < 0.01$),
- Cryptographic Signature v. Points System - 0.7034 ($p < 0.01$).

The odd correlation found was between a points system and no consequence, $\rho = 0.5955, p < 0.01$. This may be because of a 'delayed reaction' to the hypothetical abuse. We believe the combination of strong internal reliability and strong correlations, in addition to the numerical evidence, means that we can prove sub-hypothesis 5 true.

6. Conclusions

As with most Human/Computer Interaction (HCI) studies, the technology plays a minor part, fighting for attention among the cognitive, social and psychological biases present in the participants. We can conclude that encryption is a large enough factor to justify its' place within the development/deployment landscape above and beyond the technological protection it provides. However, we cannot empirically prove that encryption enhances trust in the services that use it. We have shown that various sub-hypotheses can be proven which lends weight to the main hypothesis - if it could be tested independently and removing all confunding factors.

In the constant quest to develop better, more usable and friendly software the underlying details often get lost. This is a manifestation of the the 'out of sight, out of mind' syndrome. Were the encryption in products and services given more prominent status, along the lines of '... data protected by XYZ', in marketing materials and in the service itself - the link would most likely be stronger.

The link between trust and encryption may also have been weakened by the rash of media revelations about intelligence efforts. Especially with cases where service providers have allowed access to users' data. In many of these cases (such as the NSA's PRISM programme) the intelligence community were allowed access inside the provider after all encryption protections had been removed. This undermines trust in those, and potentially all similar, services and simplification by mainstream media can mis-attribute the failings to the technology.

References

[1] A. Odlyzko, Economics, psychology, and sociology of security, in: Financial Cryptography, Springer, 2003, pp. 182–189.

[2] J. W. Moore, The use of encryption to ensure the integrity of reusable software components, in: Software Reuse: Advances in Software Reusability, 1994. Proceedings., Third International Conference on, IEEE, 1994, pp. 118–123.

[3] D. Khovratovich, C. Rechberger, A. Savelieva, Bicliques for preimages: attacks on Skein-512 and the SHA-2 family, in: Fast Software Encryption, Springer, 2012, pp. 244–263.

[4] M. Eichlseder, F. Mendel, M. Schläffer, Branching Heuristics in Differential Collision Search with Applications to SHA-512., IACR Cryptology ePrint Archive 2014 (2014) 302.

[5] F. Mendel, T. Nad, M. Schläffer, Improving Local Collisions: New Attacks on Reduced SHA-256., in: EUROCRYPT, Vol. 7881, Springer, 2013, pp. 262–278.

[6] Z. Durumeric, J. Kasten, D. Adrian, J. A. Halderman, M. Bailey, F. Li, N. Weaver, J. Amann, J. Beekman, M. Payer, et al., The matter of heartbleed, in: Proceedings of the 2014 Conference on Internet Measurement Conference, ACM, 2014, pp. 475–488.

[7] B. Möller, T. Duong, K. Kotowicz, This POODLE Bites: Exploiting The SSL 3.0 Fallback (2014).

[8] E. Biham, A. Shamir, Differential cryptanalysis of DES-like cryptosystems, Journal of CRYPTOLOGY 4 (1) (1991) 3–72.

[9] X. Wang, X. Lai, D. Feng, H. Chen, X. Yu, Cryptanalysis of the Hash Functions MD4 and RIPEMD, in: Advances in Cryptology–EUROCRYPT 2005, Springer, 2005, pp. 1–18.

[10] X. Wang, H. Yu, How to break MD5 and other hash functions, in: Advances in Cryptology–EUROCRYPT 2005, Springer, 2005, pp. 19–35.

A. Questionnaire

Question Group 2: Experience with Encryption

1. Have you had experience with the following: [Yes, No or Uncertain]

- Using End-to-End Encryption Technology?
- Use of Person to Person Encryption via E-mail?
- Using Transport Level Encryption?
- Encrypting Data Sent via Other Unsecured Means?
- Using Disk Encryption Software?
- Using Encrypted Remote Access Technology?
- Purchasing an SSL Certificate?
- Generating your own Keypair?
- Attending a Key Signing Event?

Question Group 3: Trust in Institutions and People

2. Do you consider the following institutions trustworthy: [Yes, No or Uncertain]

- The Bank/Building Society where your Current Account is held?
- Your National Government?
- UNICEF?
- A University?
- Your Local Takeaway Pizza Delivery Company?
- A Mainline Train Operator?
- The Researchers Conducting this Survey?
- An Investment Bank?

3. Please rank, in order of importance, these elements that contribute to being able to trust a person you have just met for the first time: [1-8]

- Firm Handshake / Warm Hug
- Good Eye Contact
- Expertise
- Honesty
- Compassion / Care / Diligence
- Fairness
- Consistency / Predictability
- Openness / Transparency

4. Does the importance of the following factors increase, decrease or remain unchanged in importance when deciding to trust a system instead of a person: [Increase, Same or Decrease]

- Openness / Transparency
- Expertise
- Fairness
- Consistency / Predictability
- Compassion / Care / Diligence

Question Group 4: Trust in Encryption

5. Are you likely to trust: [Yes, No or Uncertain]

- An E-mail Cryptographically Signed by the Sender?
- A News Website with an SSL Certificate?
- A Supermarket Website without an SSL Certificate?
- A 'Self-Signed' Certificate?
- A File both Encrypted for you and Signed by the Sender?
- An 'unsigned' PGP Key?
- An 'Extended Validation' SSL Certificate?
- An SSL-encrypted website with the 'open padlock' icon in a browser?

6. There have been two high profile exploits targeting encryption in recent months, Heartbleed and POODLE. Do these vulnerabilities alter your impression of the following aspects: [Increase, Same or Decrease]

- Value of encryption overall?
- Importance of testing encryption products?
- Need for new encryption algorithms?
- Need for longer encryption keys/more computationally difficult encryption?

7. You are participating in a hypothetical 'crowd-sourced' system. If the system 'tagged' your contributions using each row, what would you be most likely to do: [Act in Group Interest, Act in Own Interest Only, Deliberately Act Against Group Interest or Will not Affect Decision]

- Attribution (Text Comment)
- Attribution (Cryptographic Signature)
- Used a Reputation Points System
- Nothing

[11] A. J. Elbirt, W. Yip, B. Chetwynd, C. Paar, An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists, Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 9 (4) (2001) 545–557.

[12] V. Gupta, S. Gupta, S. Chang, D. Stebila, Performance analysis of elliptic curve cryptography for SSL, in: Proceedings of the 1st ACM workshop on Wireless security, ACM, 2002, pp. 87–94.

[13] N. Smart, A comparison of different finite fields for elliptic curve cryptosystems, Computers & Mathematics with Applications 42 (1) (2001) 91–100.

[14] A. Nadeem, M. Y. Javed, A performance comparison of data encryption algorithms, in: Information and communication technologies, 2005. ICICT 2005. First international conference on, IEEE, 2005, pp. 84–89.

[15] K. G. Paterson, G. Price, A comparison between traditional public key infrastructures and identity-based cryptography, Information Security Technical Report 8 (3) (2003) 57–72.

[16] M. Feldhofer, J. Wolkerstorfer, Strong crypto for rfid tags-a comparison of low-power hardware implementations, in: Circuits and Systems, 2007. ISCAS 2007. IEEE International Symposium on, IEEE, 2007, pp. 1839–1842.

[17] S. Pearson, Privacy, security and trust in cloud computing, in: Privacy and Security for Cloud Computing, Springer, 2013, pp. 3–42.

[18] M. Van Dijk, A. Juels, On the impossibility of cryptography alone for privacy-preserving cloud computing., HotSec 10 (2010) 1–8.

[19] S. Pearson, A. Benameur, Privacy, security and trust issues arising from cloud computing, in: Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, IEEE, 2010, pp. 693–702.

[20] M. Koufaris, W. Hampton-Sosa, Customer trust online: examining the role of the experience with the web-site, Department of Statistics and Computer Information Systems Working Paper Series, Zicklin School of Business, Baruch College, New York.

[21] D. H. McKnight, V. Choudhury, C. Kacmar, Developing and validating trust measures for e-commerce: An integrative typology, Information systems research 13 (3) (2002) 334–359.

[22] B. J. Corbitt, T. Thanasankit, H. Yi, Trust and e-commerce: a study of consumer perceptions, Electronic commerce research and applications 2 (3) (2003) 203–215.

[23] F. N. Egger, Trust me, i'm an online vendor: towards a model of trust for e-commerce system design, in: CHI'00 extended abstracts on Human factors in computing systems, ACM, 2000, pp. 101–102.

[24] J. Riegelsberger, M. A. Sasse, J. D. McCarthy, Shiny happy people building trust?: photos on e-commerce websites and consumer trust, in: Proceedings of the SIGCHI conference on Human factors in computing systems, ACM, 2003, pp. 121–128.

[25] D. Gefen, E-commerce: the role of familiarity and trust, Omega 28 (6) (2000) 725–737.

[26] C. N. L. McKnight, D Harrison, What trust means in e-commerce customer relationships: an interdisciplinary conceptual typology, International journal of electronic commerce 6 (2) (2001) 35–59.

[27] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, What instills trust? a qualitative study of phishing, in: Financial Cryptography and Data Security, Springer, 2007, pp. 356–361.

[28] R. Dhamija, J. D. Tygar, M. Hearst, Why phishing works, in: Proceedings of the SIGCHI conference on Human Factors in computing systems, ACM, 2006, pp. 581–590.

[29] D. Gefen, T. H. Heart, On the need to include national culture as a central issue in e-commerce trust beliefs, Journal of Global Information Management (JGIM) 14 (4) (2006) 1–30.

[30] H. A. Aljifri, A. Pons, D. Collins, Global e-commerce: a framework for understanding and overcoming the trust barrier, Information Management & Computer Security 11 (3) (2003) 130–138.

[31] D. Stolle, Trusting Strangers-The Concept of Generalized Trust in Perspective, OZP-INSTITUT FUR STAATS UND POLITIKWISSENSCHAFT- 31 (4) (2002) 397–412.

[32] M. Langheinrich, When trust does not compute-the role of trust in ubiquitous computing, in: Workshop on Privacy at UBICOMP, Vol. 2003, 2003.

[33] R. K. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, B. S. Lee, Trustcloud: A framework for accountability and trust in cloud computing, in: Services (SERVICES), 2011 IEEE World Congress on, IEEE, 2011, pp. 584–588.

[34] L. A. Cutillo, R. Molva, T. Strufe, Safebook: A privacy-preserving online social network leveraging on real-life trust, Communications Magazine, IEEE 47 (12) (2009) 94–101.

[35] J. Johnston, J. H. P. Eloff, L. Labuschagne, Security and human computer interfaces, Computers & Security 22 (8) (2003) 675 – 684. doi:http://dx.doi.org/10.1016/S0167-4048(03)00006-3.

[36] S. Sheng, L. Broderick, C. A. Koranda, J. J. Hyland, Why Johnny Still Cant Encrypt: Evaluating the Usability of Email Encryption Software, in: Symposium On Usable Privacy and Security, 2006.

[37] Z. Liao, M. T. Cheung, Internet-based e-banking and consumer attitudes: an empirical study, Information & Management 39 (4) (2002) 283–295.

[38] A. Hassol, J. M. Walker, D. Kidder, K. Rokita, D. Young, S. Pierdon, D. Deitz, S. Kuck, E. Ortiz, Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging, Journal of the American Medical Informatics Association 11 (6) (2004) 505–513.

[39] L. J. Cronbach, Coefficient alpha and the internal structure of tests, psychometrika 16 (3) (1951) 297–334.

[40] C. Spearman, The proof and measurement of association between two things, The American journal of psychology 15 (1) (1904) 72–101.

[41] M. N. Marshall, Sampling for qualitative research, Family practice 13 (6) (1996) 522–526.

[42] J. A. Gliem, R. R. Gliem, Calculating, interpreting, and reporting cronbachs alpha reliability coefficient for likert-type scales, Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education, 2003.

[43] A. M. Turing, Computing machinery and intelligence, Mind (1950) 433–460.