Rational Interfaces for Effective Security Software: Polite Interaction Guidelines for Secondary Tasks

Gisela Susanne Bahr[1] and William H. Allen[2]

[1] Florida Institute of Technology, Psychology
[2] Computer Sciences, Melbourne, Florida
{gbahr,wallen}@fit.edu

Abstract. States of the science and practice agree on the failure of security application to engage end users in the assurance of security and privacy in everyday personal computing. We propose as the cause an underlying irrational interface model of security related applications. Irrational Interfaces are counterproductive because they minimize the intended software utility and pay-off. In the case of security interactions, utility is minimized by the assumption of security primacy and the alienation of end user from the decision making process through disruptive messaging and disengaging content. Therefore effective security dialogues must be based on a rational interaction model. We present a small set of simple guidelines based on cognitive psychological research for polite interactions that appropriately optimize user engagement during tasks that users perceive as secondary. The guidelines for secure applications that politely interact with the end user are supported by a pay-off matrix that can be used to predict and evaluate rational secure interface performance. The rational, polite interface is a radical paradigm shift for security applications' design because it integrates end users as active stakeholders and resources in the assurance of security and privacy.

1 Introduction: Rational Interfaces and Broken Security

The state of non-expert users' understanding and utilization of computer related security is dismal. This proposition is substantiated with quotes from two leading experts in human computer interaction and computer security, respectively:

Donald A. Norman [1]: *"Without useable systems, the security and privacy simply disappear, as people defeat the processes in order to get their work done."*

Butler Lampson [2]: *"The main reason that we don't have usable security is that users don't have a model of security that they can understand."*

What is the reason that security applications software for end users do not work? The concept of a rational interface may provide a vantage point that gives us insight to the cause of the dilemma: The states of research and practice agree that interfaces are instrumental to provide information to users and that their design affects cognition in the form of attention and decision making. Rational interfaces empower the user to carry out their purpose for using the interface. Motivations may be task and goal driven such as working on a manuscript, designing a 3D vehicle prototype or virtually socializing with friends. The majority of interfaces are user benevolent and they are

C. Stephanidis and M. Antona (Eds.): UAHCI/HCII 2013, Part I, LNCS 8009, pp. 165–174, 2013.

designed to effectively support users. However, interface design has a dark side, which is evident in the deliberate manipulation of end users towards harmful decisions by malicious software. A real world example is the 9 year old child who is clicking on a fun-looking, animated but malicious popup, and installs a virus. This interface is user malevolent and yet rational with a high pay off because it accomplishes its own questionable purposes.

Our personal computing security is important but it appears that the connection between the expert defenders and the end users is broken. In fact, prior empirical research shows that security matters in personal computing are seen as a secondary task and even a nuisance [3]. We argue that the reasons for the dismal state are irrational interaction models that fail to appropriately involve the end user; instead of earning end user cooperation they generate dislike and annoyance. Based on prior research we propose that the low pay-off results from the *false* assumption that end users perceive security interactions as primary tasks. Built on the questionable assumption that *security has priority,* application designers use interaction models that are effective for primary tasks but not for tasks that end users perceive as secondary and subordinate. To ameliorate this problem we propose a set of simple polite interaction guidelines using a context sensitive smart interface. The guidelines are based on cognitive psychological research and their objective is to make effective security dialogues possible because of our understanding of how end users process information at cognitive and affective levels. One may say that we have chosen our security motto, “If you want a busy person’s attention to help you make a decision, don’t make yourself a nuisance but be polite!” The expected pay-off of polite security computing is mindful user participation in security tasks and positive user affect, which together enable a cooperative relationship between system and user for the long term, deep defense of personal computing. The rationale of this paper is outlined by the following statements:

1. Rational Interfaces are effective because they optimize the intended pay-off of the interface
2. Irrational interfaces are ineffective because they minimize the intended pay-off of the interface
3. Interface design includes pay-off consideration in line with benevolence or malevolence towards the end user.
4. The majority of interfaces have benevolent motivations, like security applications. Malicious Software (malware) does not.
5. Malware is rational because it manipulates the user to its own ends and therefore has high pay-off; Security applications are irrational because they rely on the primacy of security assumption and have low pay-off.
6. The reason for the low pay-off is the false assumption that security has priority. Pay off can be increased by accepting security as a subordinate interaction component.
7. Subordinate interaction components, like security, can be optimized by learning lessons from common human courtesy, which give rise to polite interaction guidelines.
8. The pay-off of polite interaction guidelines must be measured and hence we present a utility matrix for future performance and evaluation.

2 The Dark Side of Rational Interaction

To elucidate rational (high pay-off) interfaces, we turn to the dark side of human computer interaction. A taxonomy of malicious user interfaces may seem an unlikely topic until we accept that they (a) are effective and (b) are similar to security messaging. [4] discussed the impact of malicious interface design on users and they present a brief taxonomy, particularly of abusive advertising practices. The table below lists nine of their eleven rubrics in the left column. (The rubrics “shock” and ‘tricks” were deleted for obvious reasons.) The equivalent techniques used in system and security messaging are listed with examples in the right column. We combine the categories of system and security related communications because prior research has shown that users do not distinguish them [5,6].

Table 1. Taxonomy of Rational, Malicious and Security Interface Techniques

Effective Techniques Of Malicious Interfaces	Ineffective Equivalent in System and Security Messaging
Coercion – Threatening or mandating the user’s compliance.	Windows Vista UAC pop-ups; anti-malware popups blocking downloads until users manually override.
Confusion – Asking the user questions or providing information that they do not understand.	The classic example is “Abort, Retry, Fail” of DOS.
Distraction – Attracting the user’s attention away from their current task by exploiting perception, particularly preattentive processing.	The primary example is the animated corner pop-up used for dialogues and notifications.
Exploiting Errors – Taking advantage of user errors to facilitate the interface designer’s goals.	Not applicable
Forced Work – Deliberately increasing work for the user.	End users regard security task as additional and secondary work.
Interruption – Interrupting the user’s task flow.	Primacy of system and security interrupt the user.
Manipulating Navigation – Creating information architectures and navigation mechanisms that guide the user toward interface goals.	Windows Vista UAC pop-ups.
Obfuscation – Hiding desired information and interface elements.	Misuse of security indicators (Stebila, 2010), Fake UAC-like interfaces.
Restricting Functionality – Limiting or omitting controls that would facilitate user task accomplishment.	Ambiguous security messages combined with Yes/No choices & modal dialogs.

After perusing the table, one might summarize that there is nothing consistent about malicious interfaces except that they successfully deceive the end user; in fact, they manipulate user decision-making in line with the motivation of the interface. Whether malicious interfaces are annoying, loud, quiet or subtle their design is carefully chosen to optimize pay-off. Although sinister intent and successful manipulation of the user for dark purposes is clearly not a goal of our research, these tools and practices may give us food for thought: for example, the effectiveness of malware is based on interaction design that is goal driven and creative; malware that appropriately involves the user is an example of a rational (albeit malicious) interfaces with high pay-off. One must wonder how irrational security applications can defend end users when they are ineffective by definition due to their failure to appropriately interact with end users. The next section reviews the wide range of approaches to end user computing security.

3 Scholarly and Industrial Approaches to Security Interactions

The difficulty of attracting users to engage in security decision making has inspired scholars as well as practitioners and industry to solve this problem. For instance, [7] presented a tool to aid users in making security decisions that enhanced security-related pop-ups by displaying system status information in a more user-friendly manner and providing additional information on the impact of the user's decisions. Their results suggest the possibility of enhancing user decisions, but were not statistically significant. Similarly, recent research has presented new ways to improve the effectiveness of security-related pop-ups and dialogs. [8] studied ways to enhance security dialogs by adding context-sensitive guidance, polymorphic displays and auditing the user's interaction with the dialogs. Their approach had certain elements of coercion and forced work similar to malicious interfaces. The investigators found mixed results but suggested enhancements which may lead to improvements. Likewise, [9] sought to improve security dialog messages. They introduced a new approach to security-related popups called Adaptive Security Dialogs (ASD). The found no single factor that influences users' security behaviors and the investigators concluded that there is a need to conduct further research.

Given the lack of a solution for effective security messaging to engage the user in the decision making process, industry has opted to remove the end user from the security loop. For instance, Dell states on their enterprise website that their security system centralizes and automates security processes and thereby minimally disrupts end users. They acknowledge disruption as a key problem and rely on standard, less effective approaches to address the problem: centralization and automation. For example, automated system reboots are announced in advance and PC infections are diagnosed remotely. There are no data or metrics presented that end users benefit from this approach [10].

Nevertheless, taking the end user out of the loop does not solve the problem. We conducted an informal survey with security experts and IT professionals who work at the frontlines of system defense and are aware of user weaknesses. Along those lines any impromptu Google search on variations of the terms "dumb user and computer security" yields a plethora of documentation and editorials describing how not-so-smart end user decisions have reliably created job security for security professionals. It has been argued that complete automation and the use of artificial intelligence may be the solution to security in the future, but today's end users remain involved in security decision making; they often underperform on this task and unintentionally put their systems at risk. Below is a listing of risky behaviors that were provided by security professionals who responded to an informal survey we conducted on “your favorite not so smart user security decisions”. The results fall into four categories: false beliefs, spontaneous interactions, memory minimization, careless networking. (The complete listing is available http://research.fit.edu/carl/endusers.php).

False Beliefs

- Believing that a bank would ask for account passwords via an email/web link
- Believing that shoddy looking or poorly spelled browser popups are legitimate
- Believing that fake AntiVirus is actually going to help clean a malware infection

Impulsive Spontaneous Interactions

- Passing on email chain letters
- Saying yes to install a pop-up or toolbar in IE
- Not logging out
- Not completing updates

Memorization Minimization

- Shared credentials (user names and passwords)
- Using the same password for many online accounts
- Using weak or easily broken passwords

Careless Networking

- Turning off User Account Control
- Using open or unencrypted wireless public networks
- Not securing home wireless networks with an password key
- Allowing strangers access to their computer via Remote Desktop or Sessions
- Using an insecure login, such as FTP instead of SFTP

Numerous studies have been conducted on the question how end users make use of cyber security tools [11, 12, 13]. In the end, we accept that the dialogue between end user and security applications is broken and that empirical research demonstrates that developing an effective interaction that results in engaging the user in effective security dialogues is not a trivial task and has not been successful. One might argue that effective security messaging is impossible because users do not care about the security of their computer. However, preliminary research may have revealed a crucial component of the solution to this puzzle: *end users do care about security but they do not see security as a primary task.*

4 Security Is a Secondary End User Concern

The section presents a summary of previous research by [3] who investigated end user security interactions mediated by standard pop-ups. They made a number of discoveries, for example: end users consider security related pop-ups annoying and frustrating and do not enjoy pop-ups. They report negative emotions consistently for all pop-ups *regardless* of the ongoing task (gaming, studying or writing an essay), *regardless* of the enjoyment of the task (engaging, boring, difficult, easy) regardless of pop-up dimensions and timing. Without exception, users do not like pop-ups and report being highly annoyed by them.

It does not necessarily follow that dislike and annoyance result in dismissal. Our lives are replete with unpleasant tasks that warrant our attention. Nevertheless, users rank security related pop-ups a secondary task during their computer session while studying, gaming and writing a short essay from memory are considered primary occupations and remain in the foreground of cognitive attention; on the other hand, pop-ups are rated as interruptions and distractions and furthermore users report that they try to ignore them. The self-report measures converged with behavioral measures of eye-tracking. While pop-ups consistently captured initial attention as soon they appeared on screen and elicited relatively stable response times (the time from the first glance until the decision button is clicked), the *actual time users spent looking at the pop-ups* was not stable: after the first two pop-ups, the time spent by users actually looking at the pop-ups dropped sharply. This means that although a given pop-up was on screen, it did not visually engage the user and visual attention was invested in the primary task. It only took two exposures to pop-ups before the participants had adapted to the situation by dismissing the pop-up message. It appears that users operated using a mental model for future pop-up stimuli that classified them as meaningless and disruptive so that they could be eliminated using a "Close or cancel" heuristic, considered relatively safe. Selecting a response that is based on a heuristic is appropriate for a subordinate, secondary task because it does not require content knowledge or deliberation but only the recognition of the situation that triggers the use of the heuristic.

5 A New Way of Thinking: Polite Interactions for Rational Security Interfaces

People use computers. Computers are vulnerable. Users are the first line of defense to protect their vulnerable systems. Instead of eliminating the user through automation or through irrational interfaces, we propose to involve the end user as a stakeholder and leverage their cognitive capacity (yet unequalled by AI) to secure their personal computing environment.

Conventional dualistic approaches to human cognition have divorced reason from affect; at the same time, current cognitive neuroscience makes it clear that decision making and the selections we make from the set of choices are moderated by the limbic system, a system of systems in the human brain involved in emotions, learning and memory [14]. In turn, we suggest that HCI is a collaborative process between human and system, mediated by keyboard, mouse (used by users) and the dynamic changes in the GUI (caused by users and by the system). This process engages users at the motor level (typing, scrolling, etc.), at the visual level (looking at the screen), at cognitive levels (remembering how to use an application, using software, making decisions, etc.) and affective levels (feeling frustration with new software, feeling happiness over an email from an old friend).

If we accept that HCI is a collaborative process between system and user that influences end user cognition, then we must not only examine how the user communicates with the system but how the system communicates with the user and how it makes the user feel. Since they are ubiquitous in human computer dialogues, especially security related messages, we focus on pop-ups here. What are their characteristics? They appear at any time regardless of context; they force interaction regardless of the importance or relevance of their content; they contain text, which triggers an automated reading response in humans [15]. They originate from multiple sources, including the operating system, the web and anti-virus applications, but their provenance is neither distinguishable nor verifiable by end users; they may or may not be urgent; they may be legitimate requests for user interaction or may be malicious, i.e. phishing, etc., attempts. Given these traits one might argue that an anthropomorphized pop up shares some features with an annoying colleague from the security department who is forcing interaction.

6 The Importance of Mutually Courteous HCI

For example, [16] suggested that polite computing is defined by software that respects user information ownership by asking for permissions. Our approach to polite interaction is not based on information ownership but on *information processing*. We focus on the cognitive state of the user who is processing information while working at the computer and who is fully engaged in his or her primary task. To the busy user a security related task is not primary. If we relate this observation to security related pop-ups and consider the characteristics of pop-ups within the context of a social situation, it is obvious why pop-ups fail to engage the user in a meaningful way. One might argue that pop-ups are similar to annoying or rude colleagues who interrupt one's current task and insist on interaction. Conversely, what are the actions of a polite and thoughtful collaborator who needs decision support? For example, the polite co-worker finds a time to interact with you when you are available based on the consideration whether you are already engaged (e.g., on the phone). Once this polite co-worker decides that it is a good time to approach you, he or she asks if you are free. If your reply is positive, only then does the thoughtful and polite coworker articulate the request that motivated the interruption. This polite strategy includes four steps that apply to HCI:

1. Assess whether the person whose attention is required is busy;
2. Approach the person when he or she appears available;
3. Confirm that the person is indeed available;
4. If the response to item three is positive, state the request.

These four steps are self-explanatory because our experience of social interaction makes us aware that interruptions carry the risk of resulting in negative affect and thus will influence the resulting interaction. In addition to abundant anecdotal evidence, related research in HCI has shown the cost of task switching resulting from interruptions and the preference to delay interruptions while engaged otherwise [17, 18, 19]. Similarly to the above, socially savvy humans know that causing an interruption during work flow can provoke annoyance and comprises a poor strategy when attempting to obtain decision support from a colleague. The polite and thoughtful colleague will only interrupt in case of an emergency. From the human interaction analogy it is evident why pop up mediated security messages do not and cannot work.

7 Polite Interaction Guidelines for Security Messaging

Once we model the steps of our polite colleagues, three requirements emerge for a rational interface that optimizes dialogues required by applications that end users view as secondary or subservient:

1. *Do not interrupt the user while the user is engaged in an ongoing task.* This is not a trivial problem but may be solved by monitoring existing user interaction data and using them as signals and heuristics for determining user cognitive engagement. We propose the use of a smart or context sensitive interface to address this guideline.
2. *If you interrupt the user during a task it has to be a true emergency.* This should and must be a rare event. If all dialogues are escalated to the emergency level their importance and distinctiveness are diminished, which de facto reinvents the current pop up practice. This may be accomplished by prioritizing security interactions.
3. *Be subtle and allow the user to choose when to engage.* Once an appropriate time has been detected in the dynamic flow of the user activity, the interruption may be presented as a subtle alert (no text) that puts the security message on the user's cognitive radar but does not require the user to fully engage. Subtle alerting prevents the high cost of externally driven task switching, acts as a mnemonic aide for the user and enables the user to give his or her whole attention when ready. We propose secondary task messaging that is proportionate to the available attention of the end user.

7.1 Utility Matrix for Polite Security Interaction

Security software is motivated to obtain user engagement for decision making (including acknowledgements, and granting permissions) and uses pop-up messages. Current personal computing security applications do not considers users' state and readiness. Instead, they interrupt the user without consideration of his/her primary tasks. This model of security interaction design is irrational because it minimizes user engagement by annoying the user who in turn dismisses security related interactions.

We conclude that a rational security interaction model optimizes user engagement and increases the utility of security messaging by *engaging the user appropriately and timely in the decision making process*. To engage the human user one must consider the user state and optimize likelihood of user compliance. As seen, humans who seek cooperation from other humans (over whom they have little influence or power) use courtesy and timely opportunities. Therefore polite interactions for security messaging have three minimal rules: 1. avoid interruptions of the workflow, 2. avoid drawing user attention unless an emergency arises and 3. provide subtle and graduated alerting aimed at low levels of cognitive processing. In this first version of the pay-off matrix for polite security interaction we have not yet included emergency handling:

Table 2. Pay-off Matrix for Polite Security Interaction

		Security Interaction Model	
		Irrational (disruptive)	**Rational (polite)**
User state	**User is busy**	*Negative Engagement:* User dismisses prompted interaction. Negative user affect over time.	*No engagement:* Application does not act, i.e., does not prompt for input. No negative user affect.
	User is available	*Ambivalent Engagement:* User may or may not engage. Negative affect due to previous interruptions.	*Positive Engagement*: User participates in decision making process. Positive affect over time (liking, feeling protected)

The next step is to define metrics that test the predictions about user behaviors and attitudes. Metric and measurement construct development will be the topic of the next paper. Likewise, formalizing the pay-off matrix as a cooperative game, emergency handling and assessing any changes in user affect and trust over time will be covered in future work.

8 Conclusion

The assumption that security has priority is not valid for end users. Security interaction models are irrational because they built on this assumption and hence have not been effective. Empirical research based on a human information processing model that includes cognition as well as affect, suggests that secondary tasks, such as security applications and malware interactions, can be designed to optimize pay-off. Their effectiveness depends on the end users and how much attention and resources they are inclined to invest in the task. To this end we present 3 simple rules for polite interaction that apply to security interactions but more generally to the optimization of end user involvement in secondary tasks. Specifically, polite interactions rely on system recognition of user activity in order to find opportune times and non-disrupting formats that (a) engage the user in collaborative and more effective security decision making and (b) generate positive affect and trust over time.

References

1. Norman, D.: When security gets in the way. ACM Interactions (11/12), 60–63 (2009)
2. Lampson, B.: Usable security: how to get it. Communications of the ACM 52(11), 25–27 (2009)
3. Bahr, G.S., Ford, R.A.: How and why pop-ups don't work: Pop-up prompted eye movements, user affect and decision making. Computers in Human Behavior 27, 776–783 (2011)
4. Conti, G., Sobiesk, E.: Malicious Interface Design: Exploiting the User. In: Proceedings of the International World Wide Web Conference, WWW (April 2010)

5. Gross, J.B., Rosson, M.B.: Looking for Trouble: Understanding End-User Security Management. In: Proceedings of the Symposium on Computer-Human Interaction for Management of Information Technology, CHIMIT (March 2007)
6. Gross, J.B., Rosson, M.B.: End User Concern about Security and Privacy Threats. In: Proceedings of the Symposium On Usable Privacy and Security, SOUPS (July 2007)
7. Stoll, J., Tashman, C.S., Edwards, W.K., Spafford, K.: Sesame: informing user security decisions with system visualization. In: Proceedings of the Conference on Human Factors in Computing Systems, SIGCHI (April 2008)
8. Brustoloni, J.C., Villamarín-Salomón, R.: Improving Security Decisions with Polymorphic and Audited Dialogs. In: Proceedings of the Symposium On Usable Privacy and Security, SOUPS (July 2007)
9. de Keukelaere, F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L., Zurko, M.E.: Adaptive Security Dialogs for Improved Security Behavior of Users. In: Proceedings of the 12th IFIP TC 13 International Conference on Human-Computer Interaction: Part I, INTERACT (August 2009)
10. Dell Anti-Malware & Virus Management, How it works (link was active November 2012), `http://www.dell.com/content/topics/global.aspx/services/saas/amvm_how_it_work?c=us&cs=555&l=en&s=biz`
11. Shi, P., Xu, H., Zhang, X.: Informing Security Indicator Design in Web Browsers. In: Proceedings of the iConference (February 2011)
12. Sobey, J., Biddle, R., van Oorschot, P.C., Patrick, A.S.: Exploring user reactions to new browser cues for extended validation certificates. In: Jajodia, S., Lopez, J. (eds.) ESORICS 2008. LNCS, vol. 5283, pp. 411–427. Springer, Heidelberg (2008)
13. Stebila, D.: Reinforcing bad behaviour the misuse of security indicators on popular websites. In: Proceedings of the Conference of the Computer-Human Interaction Special Interest Group of Australia on Computer-Human Interaction, OZCHI (2010)
14. Damasio, A.: Descartes' Error: Emotion, Reason, and the Human Brain. Putnam Publishing (1994)
15. Stroop, R.: Studies of Interference in Serial Verbal Reactions. Journal of Experimental Psychology 18, 643–662 (1935)
16. Whitworth, B.: Polite Computing: Software that respects the user. Presented at: Etiquette for Human Computer Work, North Falmouth, Ma, November 15-17. AAAI Fall Symposia Series (2002)
17. Arrington, C.M., Logan, G.D.: The cost of a voluntary task switch. Psychological Science 15, 610–615 (2004)
18. Monsell, S.: Task switching. Trends in Cognitive Sciences 7, 134–140 (2003)
19. Salvucci, D.D., Bogunovich, P.: Multitasking and monotasking: the effects of mental workload on deferred task interruptions. In: Proceedings of the 28th International Conference on Human Factors in Computing Systems (CHI 2010), pp. 85–88. ACM, New York (2010)