3-2016

Man vs. machine: Investigating the effects of adversarial system use on end-user behavior in automated deception detection interviews

Jeffrey Gainer Proudfoot
Bentley University

Randall Boyle
Weber State University

Ryan M. Schuetzler
University of Nebraska at Omaha, rschuetzler@unomaha.edu

Decision Support Systems 85 (2016) 23–33

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Man vs. machine: Investigating the effects of adversarial system use on end-user behavior in automated deception detection interviews

Jeffrey Gainer Proudfoot [a,*], Randall Boyle [b], Ryan M. Schuetzler [c]

[a] Bentley University, 175 Forest Street, Waltham, MA 02452, USA
[b] Weber State University, 1337 Edvalson St., Ogden, UT 84408, USA
[c] University of Nebraska at Omaha, 1110 S. 67th Street, Omaha, NE 68182-0392, USA

ARTICLE INFO

Article history:
Received 25 March 2015
Received in revised form 17 February 2016
Accepted 18 February 2016
Available online 3 March 2016

Keywords:
Deception
Credibility assessment
Adversarial system
Countermeasures
Mandatory technology adoption
Concealed information test (CIT)

ABSTRACT

Deception is an inevitable component of human interaction. Researchers and practitioners are developing information systems to aid in the detection of deceptive communication. Information systems are typically adopted by end users to aid in completing a goal or objective (e.g., increasing the efficiency of a business process). However, end-user interactions with deception detection systems (adversarial systems) are unique because the goals of the system and the user are orthogonal. Prior work investigating systems-based deception detection has focused on the identification of reliable deception indicators. This research extends extant work by looking at how users of deception detection systems alter their behavior in response to the presence of guilty knowledge, relevant stimuli, and system knowledge. An analysis of data collected during two laboratory experiments reveals that guilty knowledge, relevant stimuli, and system knowledge all lead to increased use of countermeasures. The implications and limitations of this research are discussed and avenues for future research are outlined.

1. Introduction

A vital consideration of information systems research is the growing use of mandatory systems. These systems have the capacity to measure user behavior without the express consent or instigation of the user. Traditional technology adoption research has been conducted from the perspective that use is voluntary and focused on a reward or positive outcome for the user. Primarily, this research has focused on systems interaction contexts in which users want to use the system to help them accomplish certain tasks, or make them more effective in their work [1–3]. Prior efforts have focused on user perceptions of system usefulness, ease of use, job relevance, image, output quality, computer self-efficacy, perception of external control, computer playfulness, enjoyment, and usability [4]. Most system interactions today are of this type—voluntary and reward-focused [5,6]. While some research has looked at the involuntary adoption of systems, the outcome was still focused on task effectiveness and the ability of the system to improve overall organizational effectiveness [7,8]. However, many of these factors are not relevant to interactions with systems in which the interaction is compulsory (e.g., a full-body scanner at an airport), and could result in a punitive outcome for the user (e.g., being detained at the airport). Systems of this nature, hereafter referred to as *adversarial systems*, introduce a new context of research where users are placed in situations in which they *must* interact with the system, have *no control* over the data that are collected, and could be subject to a *punitive outcome* (see Table 1 for definitions of key terms used in this paper).

Deception detection is one context in which a user and a system may be working in opposition [9]. In this context, the human–computer interaction principle of a system supporting the user—or the system and user complementing one another [13]—is violated. Traditional computer-aided deception detection often includes the use of a polygraph device coupled with accompanying sensors to aid in determining the veracity of a person's statements. A polygraph device requires the direct measurement of a person's heart rate, skin conductance, respiration, and blood pressure by a trained polygraph examiner [14]. This process is expensive, obtrusive, and not easily scalable to a large number of interactions. A growing body of information systems research addresses the development of computing devices that will permit deception detection to be automated, unobtrusive, cost effective, and potentially more accurate and scientifically valid [15–20]. A system capable of conducting automated deception detection interviews has the potential to be utilized in any number of government or organizational contexts and applications. These include employment screening and the identification of insider security threats, a key concern of information security researchers [21–25]. Despite recent progress in the development of deception detection systems, several elements of

* Corresponding author at: Smith Technology Center 402, Information and Process Management Department, Bentley University, 175 Forest Street, Waltham, MA 02452, USA. Tel.: +1 781 891 2068.
E-mail addresses: jproudfoot@bentley.edu (J.G. Proudfoot), Boyle.WeberState@gmail.com (R. Boyle), ryan@schuetzler.net (R.M. Schuetzler).

http://dx.doi.org/10.1016/j.dss.2016.02.008

Table 1
Term definitions.

Term	Definition
Adversarial system	A system typified by involuntary use, little or no user control, and potentially punitive outcomes.
Countermeasure	An action taken to mitigate the effectiveness of a detection system [9].
Concealed Information Test (CIT)	A recognition-based criminal interviewing technique designed to detect a person's guilty knowledge of a crime (or other topic of interest) [10,11].
Deception	A message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver [12].

users' interactions with such systems have yet to be investigated. Specifically, three key areas related to user behavior with adversarial systems that information systems researchers have yet to address include: (1) the impact of guilty knowledge, (2) the impact of relevant stimuli being presented during the interaction and (3) the impact of increasing a user's knowledge about the system.

First, deceptive users working to avoid detection by a deception detection system would perceive the system to be adversarial. Accordingly, users would likely attempt to mitigate the system's effectiveness by altering their behavior to appear innocent. Actions taken to mitigate the effectiveness of a detection system are called *countermeasures*. The practice of using countermeasures to appear innocent has been witnessed and studied extensively in polygraph examinations [26]. Extant work on countermeasures has been limited to the investigation of (a) countermeasures employed against the polygraph [27], and (b) the impact of traditional polygraph countermeasures on newly developed information systems designed to detect deception [9]. Most deception indicators targeted by new deception systems are different from those targeted by the polygraph; accordingly, researchers must explore novel ways in which users will manipulate their behavior to appear truthful.

Second, all forms of deception detection interactions require the selection of questions or stimuli that will elicit deception indicators from users. Even the most valid deception interaction formats can be difficult to administer due to limitations in selecting relevant questions/stimuli to be used during the interaction [28]. Research is needed to explore how a lack of relevant stimuli during a deception detection interaction will influence countermeasure use.

Third, deception researchers developing new systems often conduct studies in which participants have no concept of the purpose of the system or any concept of its operations [15–17]. This limits ecological validity as real-world users—especially those with a vested interest in deceiving the system—would have a substantial amount of knowledge about the functionality of a real-world system when it is deployed for use. We see this currently with the polygraph, with widely available resources teaching how to "beat" a polygraph examination. Understanding how increased system knowledge will affect countermeasure use warrants further investigation.

This research investigates variations in behavior that occur when users interact with an adversarial deception detection system. These variations are manifested as countermeasures. The use of countermeasures is predicted to vary in response to the following three manipulations: (1) the presence or lack of guilty knowledge in system users, (2) the system's inclusion or omission of relevant stimuli during the interaction, and (3) the user being aware or unaware of the capabilities/functionality of the system. This research contributes to existing knowledge by demonstrating that there are substantial differences in the way users interact with adversarial deception detection systems based on a presence or lack of: guilty knowledge, relevant stimuli, and system knowledge. The remainder of the paper is organized as follows. First, we discuss relevant literature. Next, we specify hypotheses based on relevant theory. Third, we outline the methodology used for two data collections. Fourth, we provide an analysis of the data and discuss the implications of our work. Finally, we present limitations and avenues for future research.

2. Literature review

We have identified countermeasures as a strategy that users can employ to mitigate the accuracy of adversarial deception detection systems. We now examine the use of adversarial deception detection systems by drawing from three key areas of literature: technology acceptance and adversarial systems, automated deception detection systems, and deception countermeasures.

2.1. Technology acceptance and adversarial systems

One of the most widely studied theoretical models in the field of information systems is the Technology Acceptance Model (TAM) [29]. This model attempts to predict system adoption by measuring a system's *perceived usefulness* and *perceived ease of use* [6]. Evaluations of a variety of system types have used the TAM model to predict system adoption, including email, ecommerce, and executive information systems [4,30,31]. Fundamentally, TAM suggests that a user will adopt a system if it enhances his or her job performance, and that using it will be free of effort [2]. TAM has been an effective theoretical model for studying adoption of systems used in the workplace that attempt to increase productivity, effectiveness, or produce a positive outcome.

However, TAM may not be useful for understanding the adoption and use of new types of systems, which we have termed adversarial systems. For example, a user may be required to submit to a polygraph examination as part of the pre-employment screening process with a new employer [32,33]. Interacting with this system would be compulsory and not directly related to the work the prospective employee will be doing. It is also unlikely that interacting with a polygraph system will affect long-term job performance after being hired. Users have very little control over the examination process, structure, or the data that are collected [14,34].

The ways users interact with adversarial systems are fundamentally different from the ways users interact with traditional information systems. Instead of wanting to use the system to improve their own productivity, users may choose to actively work against the adversarial system. This shift in users' perceptions of such systems requires a new theoretical understanding of how users will interact with these systems. For example, Venkatesh and Bala [4] found that user *experience* had a moderating effect on the relationships between perceived ease of use on behavioral intention, and perceived ease of use on perceived usefulness. However, within the context of an adversarial system, there is no system adoption. The behavioral intention may be to circumvent the system, not use the system. Insufficient theoretical development has been done to understand how increasing experience may affect the way users interact with adversarial systems. In fact, due to the fundamentally different nature of adversarial systems, an entirely new theoretical framework of systems use may be warranted. The findings presented herein can be used to guide the future development of such a framework.

2.2. Automated deception detection systems

Deception is a persisting element of interpersonal communication. However, detecting deception is notoriously difficult for humans. Reliable deception identification rates hover around 54% [35]. Innovators have long sought information systems that can be used to augment or replace the human element in this interaction context. The polygraph is the most widely recognized and used technology for veracity assessments. Despite decades of empirical research and extensive laboratory and field testing, its validity and accuracy remain a point of uncertainty and debate [36–38]. Exacerbating the questionable utility of polygraph use is a problem of scalability. Traditional polygraph interviews require

skilled criminal examiners to conduct time-consuming multiphasic interviews with specialized sensors attached to the interviewee. Government agencies, private organizations, and researchers are all seeking to develop more robust, scalable, and automated technological solutions in response to the limitations of the polygraph [15]. An optimal solution would be a system capable of conducting an automated non-intrusive interview measuring behavioral and physiological responses of the interviewee. Responses could be analyzed in real time and used to support a human decision maker. A wealth of research has already been done with the aim of creating a system capable of conducting automated deception detection interviews. The following list includes examples of topics that have already been explored in this context:

- System use for decision support [19,20]
- Incorporation of an automated embodied conversational agent (ECA) [15]
- Identification and validation of sensors used to collect/interpret verbal, nonverbal, and physiological responses [16,39–41]
- Identification of an optimal interviewing protocol [42,43]
- Design of an optimal interface and form factor [17,44]
- System acceptance and use by human operators [18]

One of the most important aspects in developing such a system is the nature and structure of the interaction. A majority of the studies listed in the previous paragraph have used the Concealed Information Test (CIT) as the governing framework for the interaction. The CIT is a recognition-based criminal interviewing technique utilized sparsely by criminal examiners and law enforcement agencies [45]. Its limited use persists despite a wealth of scientific evidence grounded in theoretical support and extensive empirical testing pointing to its validity [46–48].

In a CIT, groups of stimuli called *foils* are presented to the examinee with one stimulus in each foil considered 'crime-relevant.' This item is referred to as the *target item*. The remaining stimuli in the foil serve as a baseline of behavior to which responses associated with the target item can be compared. These stimuli are named *non-target items*. A CIT is often comprised of several foils as the statistical likelihood of an erroneous classification diminishes as the number of foils increases. Electrodermal activity (EDA), or skin conductivity, is the dominant physiological response measured during a CIT. However, other measures can be used in conjunction with EDA [10]. The CIT interview is shorter and more adaptable than a standard polygraph examination. This makes it a good candidate for automation, especially with the use of new sensors that can remotely measure behavioral and physiological activity [28]. However, the accuracy of the CIT and other interviewing techniques can be reduced if countermeasures are successfully used by the interviewee. The following section provides an overview of various countermeasure techniques utilized to thwart the polygraph and other deception detection systems.

2.3. Countermeasures

Psychophysiological deception detection is based on detecting a physiological response that is linked to psychological processes. For decades, research in deception detection involving the polygraph has investigated the effectiveness of countermeasures at evading detection [49,50]. Unfortunately, advances on the part of law enforcement or research have been met by efforts on the part of criminals to circumvent or thwart those advances. In the case of the polygraph, entire books and websites have been devoted to teaching people how to beat a polygraph examination [26].

There are several ways deceivers can increase their chances of passing a polygraph exam undetected. Polygraph methods center on creating an individual baseline for truthful responses that is then used to detect aberrations when the individual is lying. Countermeasures are generally used to manipulate the baseline so the baseline and deceptive responses are indistinguishable. By increasing arousal during truthful questions, liars are able to muddy their results and receive a truthful judgment [e.g., 51]. Some of the physical countermeasures studied for the polygraph are tongue biting [52] and pressing toes against the floor [50,52]. During a deception detection interaction like the CIT, countermeasures are employed during the presentation of several non-relevant items to increase physiological responses, thus reducing the reliability of the scoring system of these tests.

Mental countermeasures are employed throughout the interview, rather than just when the baseline questions are asked [51]. Some mental countermeasures function by increasing the cognitive demands on deceivers, thus distracting them from the examination and suppressing their responses [50,51]. One common mental countermeasure of this type is mental arithmetic. Simply counting backward by 7 from any large number is an effective method of passing an exam [50]. Other mental countermeasures are recalling past emotional events [49] or mentally repeating your name [53].

Of course, the effectiveness of many of these countermeasures is dependent on the type of the exam and the sensors being used to detect deception. The vast majority of countermeasures research has focused on sensors used with the polygraph, including the pneumograph and finger electrodes. As innovative sensors and novel testing strategies are employed, new types of countermeasures will emerge in an attempt to circumvent those tests. For example, the P300 is an electroencephalography-based test using electrical impulses in the brain to detect the arousal associated with deception. Despite its relatively new development, the effectiveness of countermeasures against this test has already been established [53,54]. Additionally, functional Magnetic Resonance Imaging (fMRI) is being investigated for deception detection, while research on countermeasures effectiveness proceeds in parallel [55].

Due to the nature of deception detection, it is clear that the study of mechanisms to detect deception must proceed hand-in-hand with the investigation of methods to avoid detection. An approach to deception detection involving the fusion of multiple non-contact sensors has recently shown promise [15,16]. Previous research on this type of deception detection has obtained accuracy rates comparable to the polygraph. A recent investigation of polygraph countermeasures showed limited effectiveness against a combination of sensors, supporting the multi-sensor fusion approach to detection [9]. However, the results of that research were limited to polygraph countermeasures. Because of the novel nature of this suite of sensors, we must also determine if the use of new types of countermeasures may allow deceivers to more effectively evade detection. Furthermore, understanding how certain variables (e.g., relevant stimuli and system knowledge) influence countermeasure use is of critical importance to the development and use of these systems.

3. Theory and hypotheses

Deception is a complicated process, through which one party deliberately attempts to manipulate the beliefs of another, often for personal gain. Many different theories have been proposed to cover the breadth of phenomena observed during deception. Cognitive load theory proposes, for example, that cues to deception are caused by the increased cognitive load carried by deceivers who must simultaneously recall the truth and the deception [56]. Interpersonal deception theory (IDT) proposes that deception is a complex process involving strategic use of behaviors by the deceiver in order to appear truthful [56]. These strategic behaviors are deliberately selected to be congruent with what the deceiver thinks the target of their deception would be expecting from someone truthful. In a broader sense, the strategic aspects of deceptive behavior fall into the category of impression management.

Impression management is the process through which people attempt to control others' impressions of them [57]. In the case of deception, the deceiver is attempting to create a truthful impression in his or her targets. Impression management theory breaks down the process

into two components: impression motivation and impression construction [57]. *Impression motivation* is the reason the impression management takes place. People may have many different reasons and levels of motivation to manipulate the impressions others have of them. A job candidate has a strong desire for the interviewer to perceive him or her as a good fit for the position. A politician wants to appear trustworthy and honest when interacting with voters. These motivations cause individuals in such positions to engage in strategic behaviors of *impression construction* in order to engender the desired response from their audience. Impression construction consists of the verbal and nonverbal behaviors associated with creating the desired impression [58].

During a CIT, both guilty and innocent individuals are motivated to create an impression of innocence. The findings of several studies using a CIT-based interviewing format confirm that individuals deceiving during a systems-based deception detection interaction exhibit strategic behaviors in an effort to avoid detection [17,40,43]. The results of these studies indicate that there are differences between the behavior of deceivers and truth tellers. Specifically, these differences are as follows: (1) deceivers fixate on the center of the screen longer than truth tellers [43], (2) deceivers experience longer vocal response latencies relative to truth tellers [40], and (3) deceivers exhibit increased stimuli avoidance when questions relevant to their deception are present (even during repeat screenings) [17]. In order to counter natural responses to deception, individuals may engage in deliberate countermeasures. If the individual is in an unknown situation or examination, these countermeasures are termed spontaneous countermeasures [59]. Both guilty and innocent people can and do engage in spontaneous countermeasures [59]. However, the impression motivation should be much stronger in guilty individuals because they have both a more difficult task and more at stake if the test classifies them as deceptive. We propose the following hypothesis:

H1. Participants with guilty knowledge have a higher propensity to use countermeasures than those without guilty knowledge.

It is important to note that the deception literature referenced previously is based on experiments in which deceivers are presented with stimuli relevant to their deception. Relevant stimuli are presented as a means of triggering behavioral or physiological responses indicative of deceit. A hindrance to effective CIT interviewing is the necessity to identify relevant target items that can trigger deception indicators [28]. What has yet to be explored is the presence of behavioral differences between deceivers who *are* exposed to relevant stimuli and those who *are not* exposed to relevant stimuli. This issue is of critical importance for practical reasons, as persons completing real-life screening interviews could be deceiving but may not encounter relevant questions during the interaction, and thereby appear truthful.

It is the contention of this research that deceivers who are not exposed to relevant stimuli will continue to act strategically in order to appear truthful, thus differentiating themselves from truth tellers. However, the propensity for persons not exposed to relevant stimuli to act strategically will not be as persistent as persons encountering relevant stimuli. This contention is grounded in defensive response theory, often referred to as the fight-or-flight response [60], which states that a person's perception of threatening stimuli will result in a defensive behavior (i.e., a reaction to the threat) [61,62]. This sequence can be broken into three distinct components: a perceived threat, a defensive reflex, and a form of behavior modification [17]. Relevant literature investigating automated deception detection screening systems has stated that "defensive behaviors are driven by a perceived threat and therefore can be different from behavioral reactions to stimuli perceived to be non-threatening" [17,63]. In the context of using an automated system to identify deception, a sender of deceptive messages will be much more threatened by the system if the system presents stimuli that are relevant to the user's deception. This increase in perceived threat will trigger defensive responses (i.e., the use of strategic behaviors designed to mitigate the system). The following hypothesis is proposed:

H2. Participants seeing relevant stimuli have a higher propensity to use countermeasures than participants who do not see relevant stimuli.

Furthermore, experience with a system can change the way a user views and uses a system [64]. Substantial experience with an adversarial system may decrease the effectiveness of the system (i.e., reduce its ability to detect deception) as users become more confident using the system [9]. At point is the difference between *experience* with a system and *knowledge* about a system. For example, a user may have little experience with a system (i.e., never participated in a deception detection interview), yet know a lot about how a system works by reading about it online [26]. Users may also lack experience and knowledge about how a system works. However, as participants gain knowledge about the system, their behavior is likely to change, regardless of whether they have anything to hide. The Hawthorne Effect proposes that the mere act of observation may modify behavior [65,66]. In the case of a deception detection system, that behavioral modification should manifest itself by increasing behaviors (i.e., countermeasures) the system views as innocent, and decreasing those viewed as guilty [67]. Accordingly, the following hypothesis is proposed:

H3. Participants with knowledge of the system have a higher propensity to use countermeasures than participants without that knowledge.

The effect of system knowledge on countermeasure use is expected to be stronger for participants in the guilty condition. Without any guilty knowledge, participants have marginal emotional investment in the outcome of the interview, or in the functioning of the system, and thus low impression motivation. Without impression motivation, system knowledge should have a minimal effect on impression construction behaviors. With guilty knowledge, however, participants can be expected to use their knowledge of the system and of their crime to devise countermeasures to improve their chances of being deemed innocent. In this way both the impression motivation and the impression construction processes are affected. The following hypothesis is proposed:

H4. System knowledge strengthens the relationship between guilty knowledge and countermeasure use.

The complete research model for this study is presented in Fig. 1.

4. Methodology

Two laboratory experiments were conducted to test the specified hypotheses. Participants from both studies were undergraduate students recruited from business courses at a large western university. No participant reported any previous experience with law enforcement, criminal investigations, or deception detection. One participant reported hearing information about the experiment prior to participating; data from that participant were discarded. The average age of participants in the first study ($N = 77$) was 23.7 years; 78.1 percent were male. The average age of participants in the second study ($N = 114$) was 21.2 years; fifty-seven percent were male. Three experimental manipulations were used to test the hypotheses: (1) the presence or lack of guilty knowledge in system users, (2) the system's inclusion or omission of relevant stimuli during the interaction, and (3) the user being aware or unaware of the capabilities/functionality of the system. Refer to Table 2 for a concise overview of the treatments constituting our experimental design.

Participants were randomly assigned to one of the possible conditions outlined in Table 2. Participants in the control groups were told to pack a bag with benign items and pass through a screening interview. Control group members possessed no knowledge of any criminal activity and had no reason to deceive. Guilty knowledge was manipulated by

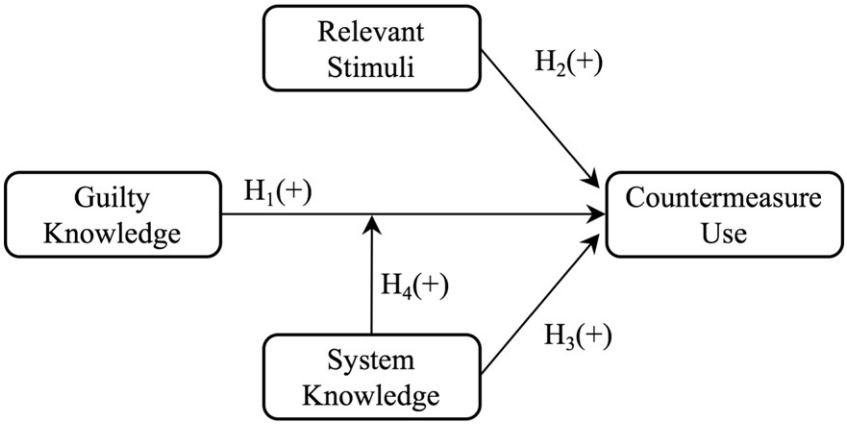

Fig. 1. Research model.

having members of the three manipulation groups smuggle a banned item through the screening interview. Participants in the manipulation groups were instructed that they were associates of a well-known criminal enterprise operating in the area. They were given instructions to pack the bag and deliver it to one of three possible criminal collaborators waiting for them in the atrium of the business school building. Participants were shown pictures of the collaborators and told to memorize their faces so that they could successfully hand off the bag to the correct individual once their task was complete. One of the items they were told to place in the bag was a simulated improvised explosive device (IED, see Fig. 2). Clothing, books, and other items were provided to help conceal the IED in the bag. The IED, the faces of the criminal collaborators, and the name of the criminal organization would serve as the guilty knowledge that manipulation group members would have to conceal to pass the screening interview (i.e., they were used as target items during the CIT).

After packing the bag, all participants continued to the screening area. Upon entering the screening area, participants were led by one of the researchers to an interviewing kiosk (see Fig. 3) and positioned in front of it. Participants were instructed to place their bag on the floor next to the kiosk during the interview. The interviewing kiosk consisted of a computer monitor and several sensors attached to a central computer. The height of the computer screen was adjusted to account for the height of each participant. To manipulate system knowledge, participants in the second study were informed about the format of the interview (a CIT) and the measurement capabilities of its sensors. Participants given system knowledge were specifically told that they would be presented with images of faces, banned items, and the names of criminal organizations. They were further told that the system would be measuring their eye movements and speech while they viewed these images. This information was conveyed to participants prior to the deception detection interview by displaying a series of seven slides on the screen (listed in Table 3 as 'Automated Overview of System Functionality').

During the CIT, several foils of image groups appeared on the screen. Each foil contained image groups of either faces, banned items, or the names of criminal organizations. Refer to Fig. 4 for an example of an image group of banned items displayed by the system during one of the foils. For each of the image groups presented, participants were asked the same question: "Are you familiar with any of these faces/items/criminal organizations?" Participants were required to respond verbally to each question by stating "Yes" or "No". The presence or lack of relevant stimuli was manipulated by configuring the set of images displayed during each interaction. An interaction containing relevant stimuli consisted of images of the IED, the three criminal collaborators, and the name of the criminal organization all appearing randomly during the interaction. The set of non-relevant stimuli contained face, banned item, and criminal organization images not relevant to the mock crime.

After completing the interview, participants were informed that the bag did not need to be delivered to the criminal collaborators. Participants were then ushered into a separate room to take a post-test survey wherein they answered questions about their experience during the interview. It was during this survey that participants reported on their behavior and the use of countermeasures during the interaction. Each participant was asked if he or she used any tactics to appear truthful. If the participant answered in the affirmative, they were asked to identify the countermeasures that they employed.

There were no significant differences between the procedures in the first and second studies aside from the intended manipulations. The differences in experimental conditions for each group are summarized in Table 3. Bolded items indicate how each manipulation group differed from the control group.

Table 2
Experiment manipulations.

Study 1	Study 2
Control Group 1	*Control Group 2*
Guilty Knowledge: No	Guilty Knowledge: No
Relevant Stimuli: No	Relevant Stimuli: No
System Knowledge: No	System Knowledge: Yes
Manipulation Group 1	*Manipulation Group 2A*
Guilty Knowledge: Yes	Guilty Knowledge: Yes
Relevant Stimuli: Yes	Relevant Stimuli: Yes
System Knowledge: No	System Knowledge: Yes
	Manipulation Group 2B
	Guilty Knowledge: Yes
	Relevant Stimuli: No
	System Knowledge: Yes

5. Results

The frequencies of self-reported countermeasure use associated with the three manipulations employed in this research are as follows: guilty knowledge (49.2%), no guilty knowledge (14.5%), relevant stimuli (53.2%), no relevant stimuli (25.0%), system knowledge (44.7%), and no system knowledge (24.7%) (depicted in Table 4). The percentage of participants using countermeasures in the no guilty knowledge group, who had no motivation to deceive, was surprisingly high (14.5%).

To test H1 through H3, a multiple logistic regression model using multiple predictors was fitted to the data to test the occurrence of countermeasures. The outcome variable was countermeasure use (1 = yes, 0 = no), and the predictors were guilty knowledge (1 = yes, 0 = no), system knowledge (1 = yes, 0 = no), and relevant stimuli (1 = yes, 0 = no). A multiple logistic regression test was chosen because all of

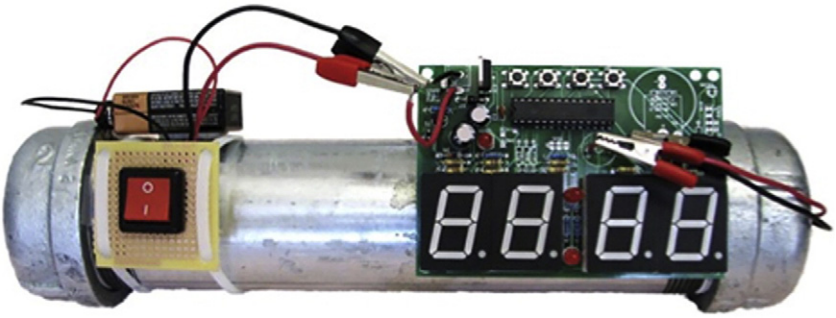

Fig. 2. Simulated explosive device packed by participants in the manipulation groups.

the independent variables and the dependent variable are dichotomous. The minimum sample size for a multiple logistic regression is 10 cases per independent variable [68] and it does not assume normality, linearity, or homoscedasticity [69]. Results from a power analysis ($\alpha = 0.05$, power = 0.80, odds ratio = 2.6, and medium effect size) indicate that the minimum sample size is 117. This study has a sample size of 191, resulting in power = 0.94.

The results shown in Table 5 indicate significant support for H1 (Wald's $\chi^2 = 3.891$, $p = 0.049$). Participants with guilty knowledge were 2.6 times more likely to use countermeasures than participants without. Support was also found for H2 (Wald's $\chi^2 = 5.905$, $p = 0.015$). Participants exposed to relevant stimuli were 2.9 times more likely to use countermeasures than participants who were not exposed to relevant stimuli. H3 was also supported (Wald's $\chi^2 = 8.737$, $p = 0.003$), as participants with knowledge of the system were 3.3 times more likely to use countermeasures than participants without. The specified logistic regression model exhibited good fit against the data (Cox and Snell $R^2 = 0.170$. Nagelkerke $R^2 = 0.232$).

Fig. 3. Interviewing kiosk.

To test H4, scores for guilty knowledge and system knowledge were standardized by calculating z-scores for each. These standardized scores were then multiplied together to create the moderating variable. The moderating variable was then added to the existing model. Results indicate no support for H4. Addition of the moderating variable had no substantial effect on the amount of variance explained by the model. Cox and Snell R^2 changed from $R^2 = 0.170$ to $R^2 = 0.172$, and Nagelkerke R^2 changed from $R^2 = 0.232$ to $R^2 = 0.235$. Results also indicate that the variable itself was not a significant predictor in the model (Wald's $\chi^2 = 0.530$, $p = 0.467$, $\beta = -0.335$, SE $\beta = 0.460$). Thus, we find that system knowledge did not strengthen the relationship between guilty knowledge and countermeasure use. The results from hypothesis testing are summarized in Table 6.

In addition to the formal hypotheses summarized in Table 6, post-hoc exploratory analysis was done on the type and variety of countermeasures reported in Study 2 in an effort to better understand how countermeasures are used by each experimental group. Countermeasures were categorized to group similar measures together; ultimately, ten categories were formed with one category labeled 'Other' for countermeasures used by only one participant. A listing of the category names, each with an accompanying description, is provided in Table 7.

When participants learned about the functionality of the deception detection system they were told that the system would be monitoring their eye movements and speech. Five of the ten categories listed in Table 7 describe manipulations of eye behavior, namely: blurred viewing, center of screen, consistent viewing, equal viewing, and haphazard viewing. Only two of the ten categories are associated with speech, specifically: temporal response control and tone control. It is interesting to note that some participants reported using physiological pain manipulation (e.g., pinching oneself to elicit a fabricated physiological response); this type of tactic is often employed to thwart the accuracy of sensors used for polygraph interviews.

The relative use of each countermeasure was calculated for each condition; an aggregate value for all three conditions combined was also calculated. Refer to Table 8 for a listing of these values and a graphical representation in Fig. 5. The most frequently used countermeasure in any condition was the use of equal viewing behavior employed by participants in the control group. Members of the control group largely used eye-based countermeasures but also had the highest percentage of countermeasures allocated to the 'Other' category. 'Consistent Viewing' is the highest-scoring category for both manipulation groups. The participants with guilty knowledge who did not see relevant stimuli had the most variety in the types of countermeasures that were used,

Table 3
Experimental task steps by condition.

Control (*Studies 1* & *2*)	No relevant stimuli (*Study 2*)	Relevant stimuli (*Studies 1* & *2*)
1. Pre-test survey	1. Pre-test survey	1. Pre-test survey
2. Pack bag with benign items	2. Pack bag with items	2. Pack bag with items
3. Went to screening area	a. Will deliver bag to criminal collaborators	a. Will deliver bag to criminal collaborators
4. Automated overview of system functionality (*Study 2*)	b. Shown faces of collaborators	b. Shown faces of collaborators
5. Interview at kiosk	c. Told activities were associated with drug cartel	c. Told activities were associated with drug cartel
6. Asked if they were familiar with items shown	d. Placed simulated IED in bag with other items	d. Placed simulated IED in bag with other items
7. Shown generic faces, benign items, and generic names	3. Went to screening area	3. Went to screening area
8. Told bag did not need to be delivered	4. Automated overview of system functionality (*Study 2*)	4. Automated overview of system functionality (*Study 2*)
9. Post-test survey	5. Interview at kiosk	5. Interview at kiosk
	6. Asked if they were familiar with items shown	6. Asked if they were familiar with items shown
	7. Shown generic faces, benign items, and generic names	7. Shown faces of waiting criminals, picture of the IED, and name of the drug cartel
	8. Told bag did not need to be delivered	8. Told bag did not need to be delivered
	9. Post-test survey	9. Post-test survey

while participants with guilty knowledge who did see relevant stimuli primarily employed eye-based and voice-based countermeasures.

6. Discussion

This research looked at variations in behavior that occur when users interact with an adversarial deception detection system. These variations manifested as countermeasures. Countermeasures were expected to increase in response to the following three manipulations: (1) the presence of guilty knowledge in system users, (2) the system's inclusion of relevant stimuli during the interaction, and (3) the user being aware of the functionality of the system. The results of this research make important contributions to a variety of research streams. We discuss the implications of these contributions, along with limitations and avenues for future research, in the following sections.

6.1. Implications for research

The hypothesis test for H1 revealed that participants possessing guilty knowledge had a higher propensity to use countermeasures (2.6 times) than truth tellers. Forty-nine percent of participants with guilty knowledge used countermeasures; thus, the effect of guilt or attempted concealment on countermeasure use was substantial. However, fifteen percent of participants lacking a need to be deceptive also used countermeasures. This finding reveals a substantial pitfall associated with trying to use the presence of countermeasures as a means of identifying deceivers. Further, this finding supports the impression motivation component of deception. Even innocent participants have some motivation to appear innocent, and thus employed impression construction techniques to create the impression of truthfulness. Based on the results of this study, it can be inferred that some users will actively try to circumvent any adversarial system, even if they are innocent. Researchers and system designers must account for these attempts at circumvention when developing deception detection systems.

Formulating interactions and sets of interview questions that are constituted of information relevant to a past crime is one of the most challenging aspects of identifying deception [10,28]. Past research studies have had distinct truthful and deceptive groups to simplify the research design and clearly quantify the ability of the system to effectively identify deception [9,15,16]. This research included a treatment in which deceivers were not asked by the system about their deception. This manipulation (tested by H2) was an effort to reveal how

Fig. 4. Sample slide containing banned items.

Table 4
Countermeasure use.

Used countermeasure?	Total sample (N)	Guilty knowledge	No guilty knowledge	Relevant stimuli	No relevant stimuli	System knowledge	No system knowledge
Yes	70	60	10	42	28	51	19
No	121	62	59	37	84	63	58
Summary	191	122	69	79	112	114	77
Percent used CM	36.6%	49.2%	14.5%	53.2%	25.0%	44.7%	24.7%

the presence of relevant questions influences user behavior. In congruence with defensive response theory, H2 was supported as participants presented with threatening/relevant stimuli were more likely to use behavior modifications/countermeasures (2.9 times) than participants who were not presented with relevant stimuli during the interaction. Fifty-three percent of participants shown relevant items used countermeasures. Surprisingly, twenty-five percent of participants who were *not* shown relevant items still used countermeasures. This result demonstrates that deception detection systems are effective at eliciting countermeasure use even if stimuli relevant to the deception are not shown. Exploratory analysis of the data indicated that the types of countermeasures used by members of each experimental group was quite different. Accordingly, an analysis focusing on the types of countermeasures used could provide a means of differentiating between truthful and deceptive individuals.

Third, prior research has looked at how experience with a system changes how a user interacts with and uses that system [4,6,70]. This research demonstrates that the mere knowledge of how a deception detection system works, even with no prior experience, significantly changes how users interact with the system. Knowledge of how a deception detection system works may reduce its effectiveness. The significant test for H3 supports prior findings. Providing users with knowledge about the deception detection system led to an increase in countermeasure use by deceivers from twenty-five percent to forty-five percent. More knowledge of how a system works will lead to significantly greater attempts (3.3 times) to circumvent the system. Results from this study show that when studying deception detection systems, or other types of adversarial systems, effort must be taken to understand the impact of users' knowledge of the system on the study's results. Performing research using only participants with little or no knowledge of the system may inadvertently harm the external validity of the study. With regard to adversarial systems, it is reasonable to believe that users may seek out information about the system before using it (e.g., buy a book on how to pass a lie detector test before an assessment [26]). It is also likely that information about the system will be disseminated to the public. As such, simulating interviewee knowledge of the system in a laboratory setting will yield more ecologically valid data and result in a system that is more robust and ready for use in real-world applications.

H4 was not supported as there was no moderating effect of system knowledge on the relationship between guilty knowledge and countermeasure use. While both guilty knowledge and system knowledge have significant direct effects (H1 and H3 respectively), having prior knowledge about the system did not strengthen the relationship between guilty knowledge and countermeasure use. Researchers looking at repeated use of adversarial systems (i.e., biannual polygraph exams) can be confident that prior knowledge about the system will not differentially affect countermeasure use among participants with guilty knowledge.

Finally, this study serves as a reminder that experimental participants are not passive observers, or even passive participants in any interactive sense. This is illustrated by the fact that a sizeable portion of members of the control group utilized countermeasures despite having no information to conceal or need to be deceptive. Just as survey questions or observation can modify behavior [65,66,71], so too can the measurement of behavior in sensor-driven studies. Researchers must consider the implications of their measurement and understand that members in all treatments (including the control group) are influenced by the very act of being measured, thereby potentially dampening the generalizability of empirical work to the real world.

Table 5
Logistic regression analysis of countermeasure use for H1-H3.

Predictor	β	SE β	Wald's χ^2	df	p	e^{β} (Odds ratio)
Constant	−2.462	0.433	30.91	1	<0.001	0.059
Guilty Knowledge	0.953	0.483	3.891	1	0.049	2.593
Relevant Stimuli	1.081	0.445	5.905	1	0.015	2.947
System Knowledge	1.181	0.4	8.737	1	0.003	3.258
Test			Wald's χ^2	df	p	
Overall model evaluation			35.507	3	<0.001	

Note: Cox and Snell $R^2 = 0.170$. Nagelkerke $R^2 = 0.232$.

6.2. Implications for practice

The results of this study offer several valuable insights for practice. First, we find that while participants with guilty knowledge are more likely to use countermeasures, there is still a strong percentage of innocent people who employed countermeasures. This effect is magnified by the introduction of system knowledge. For the deployment of automated deception detection systems in the field, it is important to consider how people will react to the system when they know what is being measured. It would be unrealistic to assume naïveté on the part of all persons who interact with a system, even among those who are innocent. Out of curiosity it is possible, even likely, that an interested person may investigate the technology behind a deception detection system. System designers must understand this and incorporate it into the algorithms they employ. For example, attempting to view all items on the screen consistently could be a countermeasure employed either due to deception or because an innocent person presumes that is the expected innocent behavior. The mere detection of employed countermeasures is not sufficient to establish deception.

Additionally, the exploratory analyses confirm that participants employed an extensive set of countermeasures during the interview, many of which have not been previously identified or reported in extant literature and are thus considered novel. These countermeasures varied by experimental condition. For example, twenty-eight percent of the countermeasures used by the control group consisted of equal viewing, but only five percent of the countermeasures used by the group not exposed to relevant stimuli consisted of equal viewing. Similarly, nineteen percent of the countermeasures used by the group not exposed to relevant stimuli were attempts at vocal temporal response control, but the control group reported zero attempts at vocal temporal response control. Practitioners both developing and using new forms of deception detection systems need to account for the inevitability that new types of countermeasures will constantly be developed and employed by users, regardless of how novel the systems or sensors used for data collection may be.

6.3. Limitations and avenues for future research

One of the contributions of this research is the investigation of how knowledge of a screening system affects countermeasure use. Providing

Table 6
Hypothesis results.

Hypothesis		Wald's $\chi 2$	P	Outcome
H1	Participants with guilty knowledge have a higher propensity to use countermeasures than those without guilty knowledge.	3.891	0.049	Accept*
H2	Participants seeing relevant stimuli have a higher propensity to use countermeasures than participants who do not see relevant stimuli.	5.905	0.015	Accept*
H3	Participants with knowledge of the system have a higher propensity to use countermeasures than participants without that knowledge.	8.737	0.003	Accept**
H4	System knowledge strengthens the relationship between guilty knowledge and countermeasure use.	0.53	0.467	Reject

* Significant at $p < 0.05$.
** Significant at $p < 0.01$.

participants with knowledge of a deception detection system in a laboratory setting could be perceived as a limitation of the study as system knowledge could alter user perceptions and behavior. However, it is our contention that increasing system knowledge improves realism and generalizability as the use of these systems in the real world would result in public knowledge concerning their operations. In light of this inevitability, research investigating how users interact with screening systems when they are *aware* of their operations should help to bridge the ecological validity gap between laboratory and real-world interactions. It is also worth noting that providing an overview of the CIT interview format/sensors prior to the administration of a traditional CIT is a standard protocol [10]. Adopting this protocol in an automated screening system context more closely adheres to CIT best practices (a practice largely ignored in prior automated screening research). It should be noted that additional knowledge and experience with the system might reduce the effectiveness of the system as users become more comfortable and confident in their ability to manipulate the system. Additional studies looking at repeated exposure to the deception detection system and the CIT are warranted.

Relatedly, this study is limited somewhat by the use of a mock crime experimental task with student participants rather than real criminals. While there are certainly differences between a student participant smuggling a banned item in a laboratory and a criminal smuggling illegal contraband through an actual law enforcement checkpoint, this limitation may not be as impactful as it initially seems. Throughout the history of the study of deception, laboratory experiments have been used as proxies for criminal interviews to understand the mechanisms behind deception and its detection [72–74]. Questions are often raised about the validity of these experiments when generalizing to real-world applications [73,75]. Several studies comparing field studies to well-designed laboratory experiments have found the results to be generalizable [75,76], and deception effects have even been shown to be greater (and thus more easily detectable) in the field than in a laboratory [75]. Thus, the results of mock crime experiments may be generalized to a broader context, though further study will be required to confirm the model with a sample from the field [73].

Future research should also examine the impact of countermeasures found in this study on the accuracy of automated deception detection systems. The exploratory part of Study 2 found that the type and quantity of countermeasure use varied across experimental conditions. A separate study will be required to more fully explore how and why specific countermeasures are used by truthful and deceptive users engaged in a deception detection interaction. Furthermore, the impact of individual countermeasures on Type I and Type II errors will provide a rich area of study. Depending on the application of a system (e.g., border screening), an increase in misclassifications could prove to be a limiting factor in the system's real-world capabilities. It is, however, doubtful that an automated screening system will be used to remove humans completely from the decision-making process. Rather, a successive hurdles approach could be used wherein an automated system provides an initial classification, and a human passes the final judgment. Additionally, previous research has examined polygraph-style mental and physical countermeasures in a CIT [9], but the effectiveness of the spontaneous countermeasures employed by participants in this experiment would require further study.

Finally, while the operationalization of this research focused on user interactions with an automated deception detection system, the broader context of this work is the exploration of user interactions with adversarial systems. The lion's share of technology adoption and use research assumes cooperation between system and user, however, new systems and novel interaction formats are creating exceptions to this traditional view. Within the context of interaction with an adversarial system there is no system adoption. The ways users interact with adversarial systems are fundamentally different from the ways users interact with traditional information systems. Instead of wanting to use the system to improve their own productivity or achieve an objective, users may choose to actively work against an adversarial system. In other words, the behavioral intention may be to circumvent the system, not to use the system. This

Table 7
Post-hoc categorization of countermeasures.

Countermeasure category	Description
Blurred viewing	Blurring eyes to avoid viewing any of the images on the screen.
Center of screen	Averting eye gaze from images and fixating on the center of the screen.
Consistent viewing	Using the same pattern of viewing images for each slide (e.g., looking at the image in the top-left quadrant first, then looking at the image in the top-right quadrant, etc.).
Emotion control	Attempting to control emotional states to avoid detection (e.g., acting calm or bored during the interview).
Equal viewing	Attempting to view each image on a slide for an equal duration.
Haphazard viewing	Using a variety of viewing patterns during the interview.
Ignoring interview	Zoning out during the interview in an effort to avoid viewing stimuli.
Physiological pain manipulation	Inflicting pain on oneself to fabricate physiological responses.
Temporal response control	Attempting to match vocal response latency for each response.
Tone control	Attempting to use the same tone for each vocal response.
Other	Tactics comprising this category include: averting eye gaze from target stimuli, attempting to control facial expressions, controlling eye blinks, attempting to forget target items, and matching head movements to verbal responses.

Table 8
Percentage of use for each countermeasure type (by condition).

Type	Countermeasure	All	NGK + NRS	GK + NRS	GK + RS
Visual	Blurred viewing	3%	0%	0%	6%
	Center of screen	9%	9%	10%	9%
	Consistent viewing	20%	18%	22%	20%
	Equal viewing	14%	28%	5%	15%
	Haphazard viewing	6%	9%	0%	9%
	Ignoring interview	3%	0%	10%	0%
Vocal	Temporal response control	11%	0%	19%	9%
	Tone control	12%	9%	5%	17%
Emotional	Emotion control	9%	9%	14%	6%
Physiological	Physiological pain manipulation	5%	0%	5%	6%
Other	Other	8%	18%	10%	3%
	Total	100%	100%	100%	100%

Note: NGK + NRS = No guilty knowledge + no relevant stimuli; GK + NRS = guilty knowledge + no relevant stimuli; GK + RS = guilty knowledge + relevant stimuli.

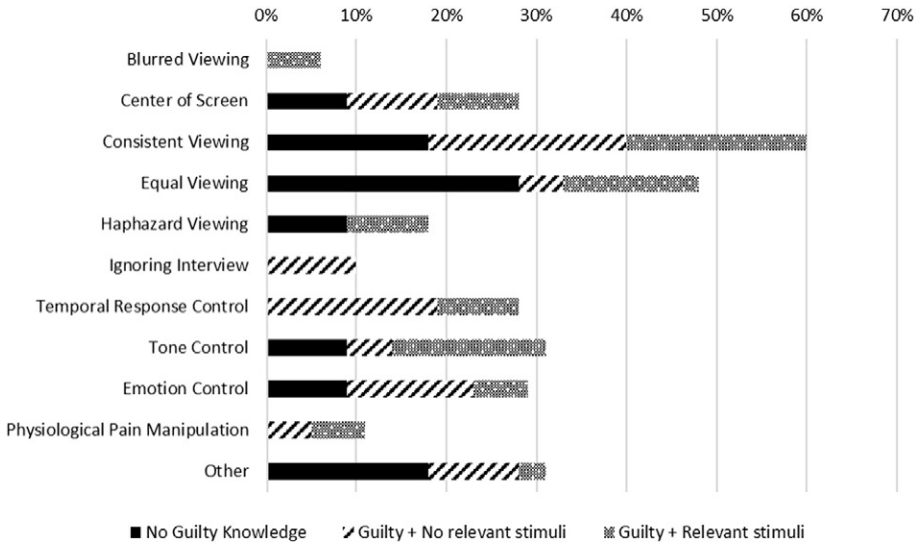

Fig. 5. Percentage of use for each countermeasure type by condition.

shift requires a new theoretical understanding of how users will perceive such systems and how users will choose to interact with such systems. Future research can build on this work to help illuminate technology use when the goals of the system and the user are in opposition.

7. Conclusion

The advancement of technology is resulting in a preponderance of new devices and systems that can be used in entirely novel ways. One such area is the introduction of systems and sensors that can be used to measure user behavior and physiology in an interaction not instigated or wanted by the user. Such adversarial systems are typified by involuntary use, little or no user control, and potentially punitive outcomes. The purpose of this research was to investigate user behavior in such a context; this context was operationalized using a deception detection interaction leveraging an automated interviewing system. Theoretically-grounded hypotheses were specified and two laboratory studies were performed to measure the influence of the following three variables on the use of behavioral countermeasures: (1) guilty knowledge, (2) relevant stimuli, and (3) system knowledge. Analysis of the data revealed that guilty knowledge, exposure to relevant stimuli during the system interaction, and increased system knowledge before the interaction all contributed to the use of countermeasures. These findings have important implications for researchers and practitioners (1) developing deception detection systems and (2) seeking to better understand how users interact with adversarial systems.

Acknowledgements

This research was supported by the U.S. Department of Homeland Security, through the National Center for Border Security and Immigration (Grant # 2008-ST-061-BS0002), and the Center for Identification Technology Research (CITeR), a National Science Foundation (NSF) Industry/University Cooperative Research Center (I/UCRC) (Project #12F-13W-12). However, any opinions, findings, and conclusions or recommendations herein are those of the authors and do not necessarily reflect views of the U.S. Department of Homeland Security or the Center for Identification Technology Research. The views, opinions, and/or findings in this document are those of the authors. We also acknowledge contributions made by Jay F. Nunamaker, Jr. and Judee K. Burgoon in advising this research, as well as support provided by a number of researchers affiliated with the Center for the Management of Information (CMI).

References

[1] S.A. Brown, V. Venkatesh, S. Goyal, Expectation confirmation in technology use, Information Systems Research 23 (2012) 474–487.
[2] V. Venkatesh, M.G. Morris, G.B. Davis, F.D. Davis, User acceptance of information technology, MIS Quarterly 27 (2003) 425–478.
[3] V. Venkatesh, J.Y.L. Thong, X. Xu, Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology, MIS Quarterly 36 (2012) 157–178.
[4] V. Venkatesh, H. Bala, Technology acceptance model 3 and a research agenda on interventions, Decision Sciences 39 (2008) 273–315.
[5] A. Elbanna, H.C. Linderoth, The formation of technology mental models: the case of voluntary use of technology in organizational setting, Information Systems Frontiers 17 (2015) 95–108.
[6] V. Venkatesh, F.D. Davis, A theoretical extension of the technology acceptance model: four longitudinal field studies, Management Science 46 (2000) 186–204.
[7] I. Adamson, J. Shine, Extending the new technology acceptance model to measure the end user information system satisfaction in a mandatory environment: a bank's treasury, Technology Analysis & Strategic Management 15 (2003) 441–455.
[8] O. Sorebo, T.R. Eikebrokk, Explaining IS continuance in environments where usage is mandatory, Computers in Human Behavior 24 (2008) 2357–2371.
[9] N.W. Twyman, R. Schuetzler, J.G. Proudfoot, A.C. Elkins, A Systems Approach to Countermeasures in Credibility Assessment Interviews, International Conference on Information Systems, Milan, Italy, 2013.
[10] D.J. Krapohl, J.B. McCloughlan, S.M. Senter, How to use the concealed information test, Polygraph 35 (2009) 34–49.
[11] D.T. Lykken, The GSR in the detection of guilt, Journal of Applied Psychology 43 (1959) 385–388.
[12] M. Knapp, M.E. Comaden, Telling it like it isn't: a review of theory and research on deceptive communications, Human Communication Research 5 (1979) 270–285.
[13] C. Nass, B. Fogg, Y. Moon, Can computers be teammates? International Journal of Human-Computer Studies 45 (1996) 669–678.
[14] C.R. Honts, D.C. Raskin, J.C. Kircher, The Scientific Status of Research on Polygraph Techniques: the Case for Polygraph Tests, Modern Scientific Evidence: the Law and Science of Expert Testimony, vol. 2, West Publishing Company, St. Paul, Minnesota 2002, pp. 446–483.
[15] J.F. Nunamaker Jr., D.C. Derrick, A.C. Elkins, J.K. Burgoon, M.W. Patton, Embodied conversational agent-based kiosk for automated interviewing, Journal of Management Information Systems 28 (2011) 17–48.
[16] N.W. Twyman, A.C. Elkins, J.K. Burgoon, J.F. Nunamaker Jr., A rigidity detection system for automated credibility assessment, Journal of Management Information Systems 31 (2014) 173–201.
[17] N.W. Twyman, P.B. Lowry, J.K. Burgoon, J.F. Nunamaker Jr., Autonomous scientifically controlled screening systems for detecting information purposefully concealed by individuals, Journal of Management Information Systems 31 (2014) 106–137.
[18] A.C. Elkins, N.E. Dunbar, B. Adame, J.F. Nunamaker Jr., Are users threatened by credibility assessment systems? Journal of Management Information Systems 28 (2013) 249–261.
[19] M.L. Jensen, P.B. Lowry, J.K. Burgoon, J.F. Nunamaker Jr., Technology dominance in complex decision making: the case for aided credibility assessment, Journal of Management Information Systems 27 (2010) 175–201.
[20] M.L. Jensen, P.B. Lowry, J.L. Jenkins, Effects of automated and participative decision support in computer-aided credibility assessment, Journal of Management Information Systems 28 (2011) 203–236.
[21] C. Posey, T.L. Roberts, P.B. Lowry, R.J. Bennett, J.F. Courtney, Insiders' protection of organizational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors, MIS Quarterly 37 (2013) 1189–1210.

[22] M. Siponen, A. Vance, Neutralization: new insights into the problem of employee information systems security policy violations, MIS Quarterly 34 (2010) 487–502.
[23] A. Vance, P.B. Lowry, D. Eggett, Using accountability to reduce access policy violations in information systems, Journal of Management Information Systems 29 (2013) 263–289.
[24] M. Warkentin, R. Willison, Behavioral and policy issues in information systems security: the insider threat, European Journal of Information Systems 18 (2009) 101.
[25] R. Willison, M. Warkentin, Beyond deterrence: an expanded view of employee computer abuse, MIS Quarterly 37 (2013) 1–20.
[26] C. Clifton, Deception Detection: Winning the Polygraph Game, Paladin Press, Boulder, Colorado, 1991.
[27] C.R. Honts, J.C. Kircher, Mental and physical countermeasures reduce the accuracy of polygraph tests, Journal of Applied Psychology 79 (1994) 252–259.
[28] I. Matsuda, H. Nittono, J.J.B. Allen, The current and future status of the concealed information test for field use, Frontiers in Psychology 3 (2012) 1–11.
[29] F. Davis, Perceived usefulness, perceived ease of use, and user acceptance of information technology, MIS Quarterly 13 (1989) 319–340.
[30] E. Karahanna, D. Straub, The psychological origins of perceived usefulness and ease-of-use, Information Management 35 (1999) 237–250.
[31] A. Rai, D.S. Bajwa, An empirical investigation into factors relating to the adoption of executive information systems: an analysis of EIS for collaboration and decision support, Decision Sciences 28 (1997) 939–974.
[32] M.J. Farah, J.B. Hutchinson, E.A. Phelps, A.D. Wagner, Functional MRI-based lie detection: scientific and societal challenges, Nature Reviews Neuroscience 15 (2014) 123–131.
[33] D.T. Lykken, Psychology and the lie detector industry, The American Psychologist 29 (1974) 725–739.
[34] M. Kleiner, Handbook of Polygraph Testing, Academic Press, London, 2002.
[35] C.F. Bond, B.M. DePaulo, Accuracy of deception judgments, Personality and Social Psychology Review 10 (2006) 214–234.
[36] S. Aftergood, Polygraph testing and the DOE national laboratories, Science 290 (2000) 939–940.
[37] G. Ben-Shakhar, M. Bar-Hillel, M. Kremnitzer, Trial by polygraph: reconsidering the use of the guilty knowledge technique in court, Law and Human Behavior 26 (2002) 527–541.
[38] K. Fiedler, J. Schmid, T. Stahl, What is the current truth about polygraph lie detection? Basic and Applied Social Psychology 24 (2002) 313–324.
[39] D.C. Derrick, A.C. Elkins, J.K. Burgoon, J.F. Nunamaker Jr., D. Zeng, Border security credibility assessments via heterogeneous sensor fusion, IEEE Intelligent Systems 25 (2010) 41–49.
[40] J.G. Proudfoot, Identifying Deception Using Novel Technology-Based Approaches to Uncover Concealed Information(Dissertation) University of Arizona, 2014.
[41] N.W. Twyman, J.K. Burgoon, A.C. Elkins, J.G. Proudfoot, Alternative Cues in Concealed Information Testing, 46th Annual Hawaii International Conference on System Sciences, Maui, HI, 2013.
[42] D.C. Derrick, K. Moffit, J.F. Nunamaker Jr., Eye Gaze Behavior as a Guilty Knowledge Test: Initial Exploration for Use in Automated, Kiosk-Based Screening, 44th Annual Hawaii International Conference on System Sciences, Kauai, HI, 2011.
[43] J.G. Proudfoot, N.W. Twyman, J.K. Burgoon, Eye Tracking and the CIT: Utilizing Oculometric Cues to Identify Familiarity with Wanted Persons, 46th Annual Hawaii International Conference on System Sciences, Maui, HI, 2013.
[44] D.C. Derrick, J.L. Jenkins, J.F. Nunamaker Jr., Design principles for special purpose, embodied, conversational intelligence with environmental sensors (SPECIES), AIS Transactions on Human-Computer Interaction 3 (2011) 62–81.
[45] A. Osugi, Daily Application of the Concealed Information Test: Japan, in: B. Verschuere, G. Ben-Shakhar, E. Meijer (Eds.), Memory Detection: Theory and Application of the Concealed Information Test, Cambridge University Press, Cambridge 2011, pp. 253–275.
[46] G. Ben-Shakhar, E. Elaad, The validity of psychophysiological detection of information with the guilty knowledge test: a meta-analytic review, Journal of Applied Psychology 88 (2003) 131–151.
[47] B. Verschuere, G. Crombez, T. Degrootte, Y. Rosseel, Detecting concealed information with reaction times: validity and comparison with the polygraph, Applied Cognitive Psychology 24 (2010) 991–1002.
[48] Y. Yokoi, Y. Okazaki, M. Kiriu, T. Kuramochi, T. Ohama, The validity of the guilty knowledge test used in field cases, Japanese Journal of Criminal Psychology 39 (2001) 15–27.
[49] G. Ben-Shakhar, K. Dolev, Psychophysiological detection through the guilty knowledge technique: effect of mental countermeasures, Journal of Applied Psychology 81 (1996) 273–281.
[50] C.R. Honts, M.K. Devitt, M. Winbush, J.C. Kircher, Mental and physical countermeasures reduce the accuracy of the concealed knowledge test, Psychophysiology 33 (1996) 84–92.
[51] E. Elaad, G. Ben-Shakhar, Effects of mental countermeasures on psychophysiological detection in the guilty knowledge test, International Journal of Psychophysiology 11 (1991) 99–108.
[52] C.R. Honts, D.C. Raskin, J.C. Kircher, Effects of physical countermeasures and their electromyographic detection during polygraph tests for deception, Journal of Psychophysiology 1 (1987) 241–247.
[53] A. Sokolovsky, J. Rothenberg, E. Labkovsky, J. Meixner, J. Rosenfeld, A novel countermeasure against the reaction time index of countermeasure use in the P300-based complex trial protocol for detection of concealed information, International Journal of Psychophysiology 81 (2011) 60–63.
[54] J. Rosenfeld, M. Soskins, G. Bosh, A. Ryan, Simple, effective countermeasures to P300-based tests of detection of concealed information, Psychophysiology 41 (2004) 205–219.
[55] G. Ganis, J. Rosenfeld, J. Meixner, R. Kievit, H. Schendan, Lying in the scanner: covert countermeasures disrupt deception detection by functional magnetic resonance imaging, NeuroImage 55 (2011) 312–319.
[56] D.B. Buller, J.K. Burgoon, Interpersonal deception theory, Communication Theory 6 (1996) 203–242.
[57] M.R. Leary, R.M. Kowalski, Impression management: a literature review and two-component model, Psychological Bulletin 107 (1990) 34–47.
[58] E.E. Jones, T.S. Pittman, Toward a General Theory of Strategic Self-Presentation, in: J. Suls (Ed.), Psychological Perspectives on the Self, Erlbaum, Hillsdale, N.J. 1982, pp. 231–262.
[59] C.R. Honts, S.L. Amato, A.K. Gordon, Effects of spontaneous countermeasures used against the comparison question test, Polygraph 30 (2001) 1–9.
[60] W.B. Cannon, Bodily Changes in Pain, Hunger, Fear and Rage: An Account of Recent Research into the Function of Emotional Excitement, Appleton-Century-Crofts, New York, U.S.A., 1929
[61] B.A. Campbell, G. Wood, T. McBride, Origins of Orienting and Defensive Responses: An Evolutionary Perspective, in: P.J. Lang, R.F. Simons, M. Balaban (Eds.), Attention and Orienting: Sensory and Motivational Processes, Lawrence Erlbaum Associates, Malwah, NJ 1997, pp. 41–67.
[62] K. Roelofs, M.A. Hagenaars, J. Stins, Facing freeze: social threat induces bodily freeze in humans, Psychological Science 21 (2010) 1575–1581.
[63] W. Ambach, R. Stark, M. Peper, D. Vaitl, Separating deceptive and orienting components in a concealed information test, International Journal of Psychophysiology 70 (2008) 95–104.
[64] V. Venkatesh, F.D. Davis, A model of the antecedents of perceived ease of use: development and test, Decision Sciences 27 (1996) 451–481.
[65] H.A. Landsberger, Hawthorne Revisited, Cornell, Ithaca, 1958.
[66] R. McCarney, J. Warner, S. Iliffe, R. van Haselen, M. Griffin, P. Fisher, The Hawthorne effect: a randomized, controlled trial, BMC Medical Research Methodology 7 (2007) 730–738.
[67] B.M. DePaulo, J.J. Lindsay, B.E. Malone, L. Muhlenbruck, K. Charlton, H. Cooper, Cues to deception, Psychological Bulletin 129 (2003) 74–118.
[68] J.F. Hair, R.E. Anderson, R.L. Tatham, W.C. Black, Multivariate Analysis, fifth ed. Simon and Schuster Co., Upper Saddle River, NJ, 1998.
[69] F.Y. Hsieh, D.A. Block, M.D. Larsen, A simple method of sample size calculation for linear and logistic regression, Statistics in Medicine 17 (1998) 1623–1634.
[70] V. Venkatesh, Determinants of perceived ease of use: integrating control, intrinsic motivation, and emotion into the technology acceptance model, Information Systems Research 11 (2000) 342–365.
[71] G. Godin, P. Sheeran, M. Conner, G. Delage, M. Germain, A. Belanger-Gravel, et al., Which survey questions change behavior? Randomized controlled trial of mere measurement interventions, Health Psychology 29 (2010) 636–644.
[72] R.I. Thackray, M.T. Orne, A comparison of physiological indices in detection of deception, Psychophysiology 4 (1968) 329–339.
[73] J.A. Podlesny, D.C. Raskin, Physiological measures and the detection of deception, Psychological Bulletin 84 (1977) 782–799.
[74] D.C. Raskin, J.C. Kircher, Validity of Polygraph Techniques and Decision Methods, in: D.C. Raskin, C.R. Honts, J.C. Kircher (Eds.), Credibility Assessment: Scientific Research and Applications, Academic Press, San Diego, CA 2013, pp. 65–132.
[75] D.A. Pollina, A.B. Dollins, S.M. Senter, D.J. Krapohl, A.H. Ryan, Comparisons of polygraph data obtained from individuals involved in mock crimes and actual criminal investigations, Journal of Applied Psychology 89 (2004) 1099–1105.
[76] J.C. Kircher, D.C. Raskin, Human versus computerized evaluations of polygraph data in a laboratory setting, Journal of Applied Psychology 73 (1988) 291–302.

Jeffrey Gainer Proudfoot is an Assistant Professor in the Information and Process Management Department at Bentley University. Jeff's research centers on information security and privacy with emphases on automated credibility assessment and insider threat detection. Jeff has contributed to over $1 million in Department of Homeland Security (DHS), Center for Identification Technology Research (CITeR), and National Science Foundation (NSF) grants, of which over $500k was awarded with Jeff operating as a PI or a co-PI. His work has been published or is forthcoming in several journals including the *Journal of Management Information Systems*, *Journal of Information Technology - Teaching Cases*, *Information Technology for Development*, *Journal of Nonverbal Behavior*, and *International Journal of Sociology and Social Policy*.

Randall J. Boyle received his Ph.D. in Management Information Systems from Florida State University in 2003. He also has a master's degree in Public Administration and a B.S. in Finance. His research areas include deception detection in computer-mediated environments, secure information systems, the effects of IT on cognitive biases, the effects of IT on knowledge workers, and e-commerce. He has published in several academic journals and has authored several textbooks, including Using MIS 8e, Experiencing MIS 6e, Corporate Computer and Network Security, 4th ed., Applied Information Security, 2nd ed., and Applied Networking Labs, 2nd ed.

Ryan M. Schuetzler is an Assistant Professor in the Information Systems and Quantitative Analysis department at the University of Nebraska at Omaha. He received his Ph.D. in Management Information Systems at the University of Arizona. His research interests include interpersonal deception, nonverbal behavior, intelligent agents, and human-computer interaction. His research has been published in *CAIS*, *Group Decision & Negotiation*, and the *Journal of Nonverbal Behavior*, as well as numerous conferences.