A Thief among Us: The Use of Finite-State Machines to Dissect Insider Threat in Cloud Communications

Shuyuan Mary Ho
Florida State University
Tallahassee, FL 32306-2100
smho@fsu.edu

Hwajung Lee
Radford University
Radford, VA 24142. USA
hlee3@radford.edu

Abstract

Insider threats are both social and technological phenomena, and group dynamics can provide important indicators to help counter insider threats. This paper discusses an experimental study that simulates insider betrayal in an online collaborative environment. This study uses the framework of trustworthiness attribution, wherein the authors examine the trustworthiness of a focal individual whose role was in leadership with authority within a trusted team arrangement. Specifically, the authors adopted a finite-state machine (FSM) approach to analyzing patterns of a group's emotional states in order to understand how members collectively distinguish insider betrayal through computer-mediated interactions, social connectivity and coordination. Moreover, these conditions help us understand how human observations of betrayal can be leveraged to provide early warnings to betrayal. Of the four simulated case studies conducted, two provide baseline measures, and the other two provide treatment measures. Findings indicate that signs of potential betrayal can be collectively identified by team members through text and behavioral patterns – to uncover social intent that is not explicitly stated.

Keywords: Insider threats, information systems security, socio-technical system, online game simulation, human-computer interactions

1 Introduction

Organizations rely on their employees' access to organizational information for productivity and accountability. However, allowing such access has potential negative consequences too. *Insider threats* are defined as situations in which a critical member of an organization with authorized access, high social power and holding a critical job position, inflicts damage to her own organization by behaving against the interests of the organization, generally in an illegal and/or unethical manner [15]. This typically refers to an individual who holds a key position, which grants him or her access and authority, but any employees with access could cause significant damage to an organization's internal information.

According to 2009 Computer Security Institute Survey, financial losses caused by computer crime averaged $234,000 per responding company, significantly above 2005 and 2006 figures. Twenty-five percent of the respondents felt that 66% of their financial losses were due to *insider activities*, and that 43% were from malicious *insiders' actions* [33]. Forty-six percent of the respondents experienced the damage caused by insider attacks as being more severe than outsider attacks, and 33% viewed the insider attacks as not only more costly, but more sophisticated [6]. Moreover, 70% of insider incidents were handled internally without legal action [6].

In a world where security professionals have been traditionally focused on protecting the *perimeter* of network architecture, cloud computing presents new and unique challenges similar to insider threat and identity theft scenarios. Bolstering against this weakest link - the human factor - becomes critical in the chain of an organization's security defense [25].

Parker [27] was the first to propose a general model for describing insider threats called SKRAM – which identifies five logical dimensions of detection: skill, knowledge, resource, authority and motive. Its utility as a guide to the study of *cyber* insider threats, though, is limited because it does not take into account how these are technologically expressed. The technological domain is tricky precisely because it must allow for nuances in the framework for classification of accidental and intentional breaches in information security as well as concealment. Moreover, it is retrospective, and we are concerned primarily with a predictive model. Schultz's model introduces predictive measures, defining behavioral benchmarks that combine verbal and technological patterns [36]. Similarly, Ray develops algorithms based on an attack tree, as input for a quantitative model [32]. What all of these models lack or neglect is the opportunity to leverage the uncanny ability of humans to detect deception – to address insider threats in the same way that intrusion detection systems work; analyzing information in real-time, and identifying anomalies as early warning signs.

Normally we observe human behavior in the physical world through facial expression, appearance, and social interaction with others. It is a challenging security issue when the motivation of an individual is obscured by regular, patterned external behavior. Take, for example, the case of the so-called traitor Robert Hanssen as an instance of betrayal. It took nearly 15 years for the FBI to realize his conspiracy [9]. Hanssen appears to have maintained consistent enough behavior to have successfully eluded detection for over a decade. Motivation or "basic motives" can be easier to identify once human behavior becomes unusual or abnormal [22]. These challenges are amplified in the virtual world of cyberspace.

In most circumstances in cyberspace, we may only understand human intention through virtual behavior and language—communicated through text and written words. Ajzen [1] posits that interpreting intention falls somewhere between a person's intrinsic motives and a resulting action. Since human intention is typically reflected in their behavior [1] as realized through words they speak, we may be able to hypothesize that human emotions reflect intention as well as behavioral change. By observing human behavior and words, we can understand the motivation and conversational intent of a target individual. Nevertheless, benchmarking consistency in human behavior presents a challenge, and certainly personality disorders may lead to behavior fluctuations that confound these observations. While information behavior through words and conversations is hard to detect, hidden behavioral changes are even harder to identify when one's true intent is unknown. This explains why the FBI had difficulty in detecting Robert Hanssen's case [9].

Hanssen's case causes us to question how an organization may identify precursors of a critical member's betrayal through the aggregative views of the target's virtual team members in close relationship. As we adopt the analogy of humans as sensors on the network, we aim our study at the human's sensors' emotional states as a reflection of interactions with the target individual. Due to the difficulty of understanding uncertain human behavior, we framed our research question thusly:

> "*How can insider betrayal, a dispositional state, be predicted through changes of emotional states among virtual team members*?"

In insider threat situations, the potential perpetrators are embedded in communities of coworkers who might ostensibly be able to detect anomalous changes in each perpetrators' patterns of behavior. Unusual or unexpected changes in an individual's behavior as detected by human observers may provide potential clues to the imminence of insider threat activity. One way to characterize and assess the reliability of an insider is to consider "trustworthiness" [15].

In this paper we present our theoretical framework, in the second section, based on *Attribution Theory*. We approach the problem by building several experiments to simulate insider threat situations. We explain our research method, design rationale and data collection in the third section. We discuss our methods for processing and analyzing data in the fourth section. Using basic human conversation, we demonstrate how to extrapolate and analyze conversational intent, and we seek to understand how emotional conditions of the team members might correlate and reflect dispositional states of target's trustworthiness, using the Finite State Machine approach. In the fifth section, we discuss our findings of this experiment. Emotional data from four sets of experiments are visualized and compared. We conclude our study in the sixth section.

2 Theoretical Framework

Our research framework is based on how groups attribute the behavior of a focal individual when his or her trustworthiness in terms of integrity towards his/her teammates becomes questionable. *Attribution Theory* helps us to understand how people observe deceptive behavior over time (or interpret any behavior that is suspect), how people make inferences about changes in behavior that signify something abnormal, and consequently, possibly predictive of the likelihood of a shift in that individual's intentions. For this reason, we have adopted *Attribution Theory* to examine the insider threat phenomenon in computer-mediated communications.

2.1 Attribution Theory

Attribution Theory - introduced and developed to model how a typical person answers questions - also helps to frame the response to potentially unfamiliar stimulus. According to Kelley et al [20], a person believes that his/her reaction to a stimulus is correct when the reaction meets three criteria. One's response to any stimulus is considered valid if:

1) the response is associated uniquely with the stimulus,
2) the response is similar to others' responses to the same stimulus, and
3) the response is constant over time when exposed to the stimulus.

More succinctly, the response must be distinct, there must be a perceived consensus, and it must be consistent for an individual to consider it valid. By consensus, we mean agreement among one's close social network with regards to an individual's behavior, not agreement with another's behavior across situations.

These three factors make up part of the *Person* × *Entity* × *Time* model formulated by Kelley et al. [19], which states that persons, entities, and time comprise the three possible causes in attribution problems. Kelley et al [20] provided the following example to further illustrate the model. In the example below, Alice is an actor being observed by others.

> Alice laughed at the comedian she heard the other night. Almost everyone who hears the comedian laughs at him (referring to the comedian). Alice does not laugh at almost any other comedian. In the past, Alice has almost always laughed at the same comedian. [19]

This example mentions each of the above facets from the model. One begins to question which of the three factors leads to the laughter ensuing from watching the comedian. Is there something about Alice (the person; an internal causal factor) that causes her to laugh at this comedian? Is the comedian himself (the entity; an external causal factor) responsible for the laughter? Is there something special about the time and circumstances (situated context) that causes the laughter? This example offers a scenario where the entity (the comedian himself) has sole responsibility for the outcome. The above scenario removes the possibility that Alice's laughter transpires only from one of her characteristics (an internal cause). The fact that Alice has not had the same response in the past to other comedians - or rather has only laughed at the same comedian consistently - eliminates doubt that Alice's laughter comes from something other than the comedian (an external cause). Thus, we would likely label the cause of Alice's laughter as an external attribution.

The factors of *distinctness*, *consensus*, and *consistency* describe the situation above, where an entity is responsible for one's judgment [19,21]. To continue with the example, Alice's laughter is *distinctive* behavior because "Alice does not laugh at almost any other comedian," and Alice's laughter is *consistent* since "Alice has always laughed at the same comedian" based on everyone's historical observations in *consensus*. These factors are the driving force behind the "phenomenology of attribution validity." An observer is more likely to believe that his or her perceptions are true when the above three factors are met.

3 Methods

We have developed and implemented a series of online games to help explore our research question [38]. These games involve a controlled activity with a series of experimental situations, aggregated into an exercise where team members are able to observe and attribute a leader's behavior over time [15]. The rationale for using this game is that it is, by definition, a simulation of an insider threat scenario. This allows us to collect perceptions about a supervisor from a group of subordinates over time, and especially after a supervisor's behavior has been influenced or manipulated through intervention.

3.1 Predicting Observed Downward Shifts in Trustworthiness

The research goal here is not to determine whether or not someone will betray, but rather, whether or not teammates will be able to detect the betrayal. This study simulates a virtual betrayal situation which provides interpretive participant observation research data - and adopts a positivist view toward identifying indicators of abnormal behaviors based on specific criteria of trustworthiness assessment. We designed experimental situations to answer our research question, and we adopted attribution theory to represent how people attribute (or assign) the causes of others' behaviors [12,13]. Of course, observers' perceptions vary depending on different interpretations, the target individual studied, and different situational settings [11,12,40]. The attribution of the target's (A) behavior by observers (B) is determined by Bs' judgment that A intentionally or unintentionally [12] behaves in a way attributable to either external (situational) causality or internal (dispositional) causality. As such, Ho [14,16] set up a group of individuals as observers (B) and collected their daily perceptions about a target's (A) behavior. A's behavior and the types of tasks involved were controlled, so that Bs' perceptions could be measured. A questionnaire was designed to collect any changes in Bs' judgments about A's behavior [12] that might be attributable to either external (situational) causes or internal (dispositional) causes. The principle of distinctiveness was also applied to A's behavior. In other words, behavioral change must be noticeable for others to perceive it.

3.2 Socio-technical Research Design

To set the stage for betrayal, the game used a micro-payment system to compensate the winners. "MerryBux tokens" were offered as the winning prize for each team [39]. A Game-Master used additional MerryBux tokens as the bait to lure the Team-Leader (as Target A) in an effort to alter her/his behavior. In this threat simulation, we observe participants (as Observer B_n) as they observe the Team-Leader's betrayal taking place. The climax of this contest was controlled. At the end of the entire experiment, the tokens could be exchanged for gift certificates.

Each participant's role in the online game is clearly defined to the participants. The role of a Game-Master is to influence the dynamics of the virtual competition. The Game-Master has both the knowledge of the game's expected outcome, as well as control over the micro-currencies so as to compensate the winners. The Game-Master also reports to the team on the progress of the other (fictitious) teams. In this scenario, the primary responsibility of the Game-Master is to manipulate the competition and inject the bait for the Team-Leader at the appropriate moment. The purpose of the bait is to create a conflict of interest between the leader and the team members.

The Team-Leader is appointed from among the team participants by the Game-Maser. One role of the Team-Leader is to obtain all game-related information, including both the in-progress data as well as final scores from the Game-Master. Note that the information regarding the performance of each team and the larger competition is only released to the Team-Leader, not to the team participants. The Team-Leader is the only person authorized to have direct contact with the Game-Master, and imparts the team's (winning or losing) status at the end of each game. The Team-Leader should feel in total control of managing and rewarding the team. In order to create the feeling of fairness and reduce suspicions, the Team-Leader is required to fill out a daily report just like team participants do.

Team members are volunteer research participants. The role of the team member is to cooperate with the Team-Leader [A] and achieve the highest score as a team on the assigned tasks. The rewards program (MerryBux tokens paid as micro-currency) is announced at the beginning of the game. Team members [B_n] are told that their rewards will be handed out directly by the Team-Leader.

There is a "mole" player embedded in each of four teams. The role of the mole player is to influence team discussions. Specifically, two types of moles are designed into the games - to either increase or decrease group suspicion (sensitivity) about the target's behavior. One mole type is charged with enhancing group sensitivity and instructed to question the target [A], Team-Leader. The other mole type is charged with decreasing group sensitivity - instructed to smooth out any questioning about the target. Both types of mole are chosen after groups are formed. They have no knowledge of the experiment, and their role is only to insert text into the conversations at the request of the experimenter.

Communications from the Game-Master to the Team-Leader is scripted as much as possible. The behavior of the team participants, of course, is not controlled.

The experiment was designed with careful consideration for the representativeness of the sample frame that matches the unit of analysis [30]. The experiment was designed in such a way to as to simulate real world group dynamics. This experiment was designed to recruit one real team, while sharing fictitious scores of three other teams. In fact, four teams were recruited, but each played in their own game framework. Two of the four teams received bait, and the other two did not.

3.3 Virtual Betrayal Simulation

This experiment consists of four situations to study varying degrees of two group-related phenomena: *group sensitivity* and *target influence* [15]. We define group sensitivity in this context as the degree to which group members recognize a behavioral change in their designated Team-Leader. Target influence in this context refers to how easily a particular Team-Leader can be persuaded to betray his respective team members. We refer targeted individuals, as Team-Leaders for Alligator, Buffalo, Crocodile, and Dragon. Teams with corresponding names are referred to as Teams Alligator, Buffalo, Crocodile, and Drag. The following paragraphs elaborate further on the overall experiment, as well as group sensitivity, target influence, and other related terminology.

Before the experiment started, researchers appointed Team-Leaders - and the organizational makeup of each team - at random. During the course of each simulation, each team received verbal and math-based logic puzzles to solve under the direction of the Team-Leader. The Team-Leader had the responsibility to direct and motivate the other team members, and to enter the solution into a web-based interface for automatic scoring. If a Team-Leader was not attentive to the group's efforts, the group suffered by not earning the day's maximum number of points for that day. At the end of each day, an announcement detailed the relative achievements of each group. The Game Master (an authority figure) announced that each group would earn a gift certificate according to the position of the team's relative positioning to the other (fictional) teams. Teams that finished first in the daily competition would earn more MerryBux. Team members then had to fill out surveys to rate their Team-Leaders.

Treatment in this case refers to the introduction of verbal persuasion via emails from the Game Master, encouraging the Team-Leader on the third day of the experiment to let his/her team lose and pocket (not distribute) reward tokens. Team-Leaders Crocodile and Dragon received specific communications to persuade them to take the "bait" and betray their respective teams, while Teams- Leaders Alligator and Buffalo did not.

In addition, "moles" were inserted covertly into all teams. These moles were given exact phrases - in the form of predefined scripts - to infuse during the chat sessions in an effort to influence the groups' dialogue. Teams Alligator and Crocodile each had a mole character inserted into their respective groups. These moles were given a script designed to encourage disparaging remarks about the Team-Leader. Teams Buffalo and Dragon included mole characters as well, but these members had predefined scripts that would discourage talk about the group's Team-Leader. In other words, by design, group sensitivity for Groups Alligator and Crocodile was relatively enhanced, and group sensitivity for Groups Buffalo and Dragon was relatively reduced. In addition, Alligator's and Buffalo's Team-Leaders were not tempted with any bait, while Crocodile's and Dragon's Team-Leaders were tempted with bait.

Triangulation was adopted through multi-level data collection. Data from the four different experiments was collected in several different formats. Chats, blogs and emails became records of how team players interacted with one another. This experiment recorded not only how a virtual organization might operate, but also how target players were influenced by both authoritative and peer figures as part of back-end shadow information. A face-to-face interview was conducted and transcribed as a repetition and reinforcement of the qualitative surveys. The real purpose of the online leadership and group dynamic game was debriefed[1] to all players during the final face-to-face interview. Participant observations were provided by all four Game-Masters throughout the game.

4 Data Analysis

In this section, we report on the analysis by three annotators' (indirect observers') etic[2] aspects [28,29] of the conversations between the targets as the Team-Leaders and the observers as the Team Members. Three annotators read through all the conversation transcripts of four teams and identified emotion-related text.

[1] Syracuse University IRB #07-276.

[2] This parallels the linguistic terms *phonemic* and *phonetic,* from which the words *emic* and *etic,* are derived. A phonemic sound is not a sound at all. It is a representation of the sound before it is spoken. Only the person about to speak a phoneme can truly hear it. The phonetic sound is that actual sound produced after a noise is made—third parties can observe this. Likewise, emic perspectives can only be obtained by the subjects directly involved in the study. They will never be able to provide etic perspectives, as their involvement makes them subjective to the entire matter. The reverse holds true for etic observations.

4.1 Data Processing

Data was obtained by giving each of the three annotators a list of possible emotions and their definitions (Appendix A – Coding Scheme). Each annotator then read through the transcripts (scenarios Alligator, Buffalo, Crocodile, and Dragon) and chose the lines of dialogue that contained emotion. When a line of dialogue was chosen, the annotators documented the medium of the communication (email message, forum post, chat room message), the name of the speaker, the date and time of the utterance, the full quote as written, the emotion portrayed in the quote, and to whom the quote was directed. Special cases of a Team Member speaking about a Team-Leader - and a Team-Leader speaking about him/herself - have deeper relevance in the analysis.

We provided several channels of communications, e.g., chat, email and forum posts. Chats in real-time lend themselves to the instantaneous expression of emotions. Emails allow members to engage in private exchanges. Forum posts are slow and thus did not facilitate emotion sharing. We always noted the speaker to identify trends in how vocal certain individuals were. Naturally, some voiced their opinions more than others. The time was always recorded to see how emotions evolved through the five-day experiment. The intended recipient of each quote is vital in defining whether the emotions are about trust for the Team-Leader - or unrelated.

Kaiser et al [18] has noted the difficulties of translating online game results obtained in a laboratory setting into the real emotional experiences of a typical situation. The efforts in creating a controlled environment with replicable results can often interfere with natural spontaneous emotional expression. To address these issues, Kaiser et al [18] created a multi-level game scenario that included elements designed to invoke emotional reactions. In Kaiser's games, a helper agent was included to offer assistance to the players at different turns in the game. Some subjects reported anger at having the helper agent, due to feeling condescended to, and some subjects reported a degree of comfort and relief from the presence of the agent, as reflected in degrees of sadness reported at the agent's removal from the game toward the end of the scenario.

We adopt Scherer's [35] view that different emotions result from different kinds of stimuli. The stimuli delineated in Scherer's work range from novelty to the ability to cope with unexpected situations. The stimuli we focus on in this study have more to do with the aspects of the game that involve a team-oriented goal and group-related social interactions. With these insights in mind, we created a coding scheme (Appendix A – Coding Scheme) as a guideline for determining if and when a particular player experienced a specific emotion. In addition, Ekman and Friesen's [8] study differentiated among three different kinds of happiness:

1) a relief happiness that occurs after a negative emotion has ended,
2) a pride happiness that occurs after reaching an achievement, and
3) a general, pleasure happiness.

We adopt the first two realizations of happiness for our study. For generating the rest of the emotions listed, we adopted insights from Ochs et al. [26]. The coding schemes include seven different categories: *excitement, happiness, tenderness, apologetic-ness, sadness, distressfulness, and angriness.* Appendix A – Coding Scheme lists the stimuli for each emotion; we made inferences about what emotion a game subject experienced based on the context of a particular phrase in the transcript.

4.2 Emotional Patterns in the Virtual Betrayal Simulation

4.2.1 Finite State Machine (FSM)

Various studies have used Deterministic Finite Automata (DFA) to describe states of dialogues, emotion, and personality [4,7,41]. Zhu et al [41] define each state of the DFA by an exchange of information in a dialogue. In this study, the researchers examined the quality of the information exchange during a dialogue with an automated operator. Dialogues that had certain state patterns of a great deal of information exchange were judged as more valuable than dialogues that include less or no exchange of information. Egges' [7] study contains a simulation of an emotionally charged agent with the goal being to have an agent judged as empathic. That analysis viewed states as containing both a personality variable and an emotion variable to capture the fact that different personalities can respond to the same event with different emotions. Lastly, Bosma and Andre [4] offer an analysis of a set of dialogues in terms of what actions, for example, acceptance or rejection, can lead to different emotional states. These studies have large datasets in common—each study collected thousands of utterances, or dialogue turns.

To determine general patterns of emotions over time, this study adapted the DFA model [41]. A change in state was used to model when an exchange of information occurred. Similarly, we adopted the approach that a change of state can indicate a change in emotion. FSM models the emotional states that members of a group experience when detecting trustworthiness changes in their leader. FSM's can account for variability in a generalized way. Variation can occur among groups because their reactions can depend on their external circumstances and the makeup of the individuals in the group. These variations can be captured with FSM. Once we detect patterns among the different FSM models, we can possibly make a generative model of human behavior.

4.2.2 Emotional Patterns

We use FSM expressions to represent emotional patterns in the virtual betrayal simulation. Due to the nature of online communication, an emotional state of each individual is captured from a dialogue. Thus we represent an emotional state as a dialogue in our study. The emotional patterns are defined by the following quintuple:

$$M = (Q, \sum, \delta, q_0, F)$$

where

Q: $\{s_{ij} : i = 0, 1, 2, \ldots, n, j = 0, 1, 2, \ldots, m\}$ is a finite set of **states**

$\sum$: $\{a_{jkl} : j = 0,1,2, \ldots, m, k = 0,1,2 \ldots, r,\ l = 0,1,2, \ldots, s\}$ is a set of symbols called the **input**

δ: $Q \times \sum \rightarrow Q$ *is* a **transition function**

$q_0 \in Q$ is the **initial state**

F: $\{f_b, f_l\}$ is a set of **final states**, where f_b denotes betrayal and f_l denotes loyalty.

A state attribute value matrix (AVM) model was designed to determine the relationship between team members' observations of Team-Leaders behavior and Team-Leaders actual betrayal. A state s_{ij} and an input a_{jkl} can be represented using the feature structure with a notation of AVM as shown in the following:

$$s_{ij} = \begin{bmatrix} \text{emotion} & \mathrm{e_i} \\ \text{person} & \mathrm{p_j} \end{bmatrix} \text{ for } i=0,1,2,\ldots,n,\ j=0,1,2,\ldots,m$$

The above emotion-person pair, is derived by the following model based on Kelley's attribution model: person × entity × time [19].

$$a_{jkl} = \begin{bmatrix} \text{person} & \mathrm{p_j} \\ \text{dialogue} & \mathrm{d_k} \\ \text{time} & \mathrm{t_l} \end{bmatrix} \text{ for } j=0,1,2,\ldots,m,\ k=0,1,2,\ldots,r,\ l=0,1,2,\ldots,s$$

The AVM input is represented as the triplet person × dialogue × time. The person in this model is always the Team-Leader. Dialogues, represented in the model as $D = \{d_1, d_2, d_3, \ldots, d_r\}$, represent the coded content of conversations between (1) team members and (2) team members and their Team-Leaders. These dialogues are captured at times before, during, and after the betrayal has been initiated against team members.

Because this simulation is done in an online environment, reactions to the system can influence a person's emotion, as in real life. There is no way to control for outside influences. For instance, if a participant cannot log in as expected, the participant may become confused or show other emotions. Thus, for our purposes, we consider the system capable of triggering emotions.

The transition function shows a shift from one state to another upon receiving an input. Starting from the initial state, the transition function leads the state change eventually toward one of the final states. Final states f_b and f_l indicate betrayal and loyalty, respectively. Loyalty means that no betrayal occurs until possibly the end of the virtual betrayal simulation.

Since we deem predicting human behavior as being no trivial act, we insert a person p_j in the FSM to carefully consider the human factor. In addition, since the virtual betrayal simulation has a reasonable number of participants such that each person is a personality component, the FSM uses a person in the state AVM $\{s_{ij}\}$ and in the input AVM $\{a_{jkl}\}$. However, it is also possible that this FSM encompasses any personality classification or any other classifications with respect to predicting human behavior such as person types [3], personal traits [10], and five-factor models [2,5,23,24,31,34,37]. Thus, we can replace the person field p_j in the FSM by the other classification, as follows:

$$s_{ij} = \begin{bmatrix} \text{emotion} & e_i \\ \text{personality or human behavior factor} & p_j \end{bmatrix} \text{ for } i=0,1,2,\ldots,n, \quad j=0,1,2,\ldots,m$$

$$a_{jkl} = \begin{bmatrix} personality\ or\ human\ behavior\ factor & p_j \\ dialogue & d_k \\ time & t_l \end{bmatrix} \text{ for } j=0,1,2,\ldots,m, \quad k=0,1,2,\ldots,r, \quad l=0,1,2,\ldots,s$$

The FSM state diagram can be represented as a directed graph $G = (V, E)$, where V denotes a set of states, E denotes a set of transition functions, and a weight on each directed arrow denotes the input, as shown in Figure 1-2.

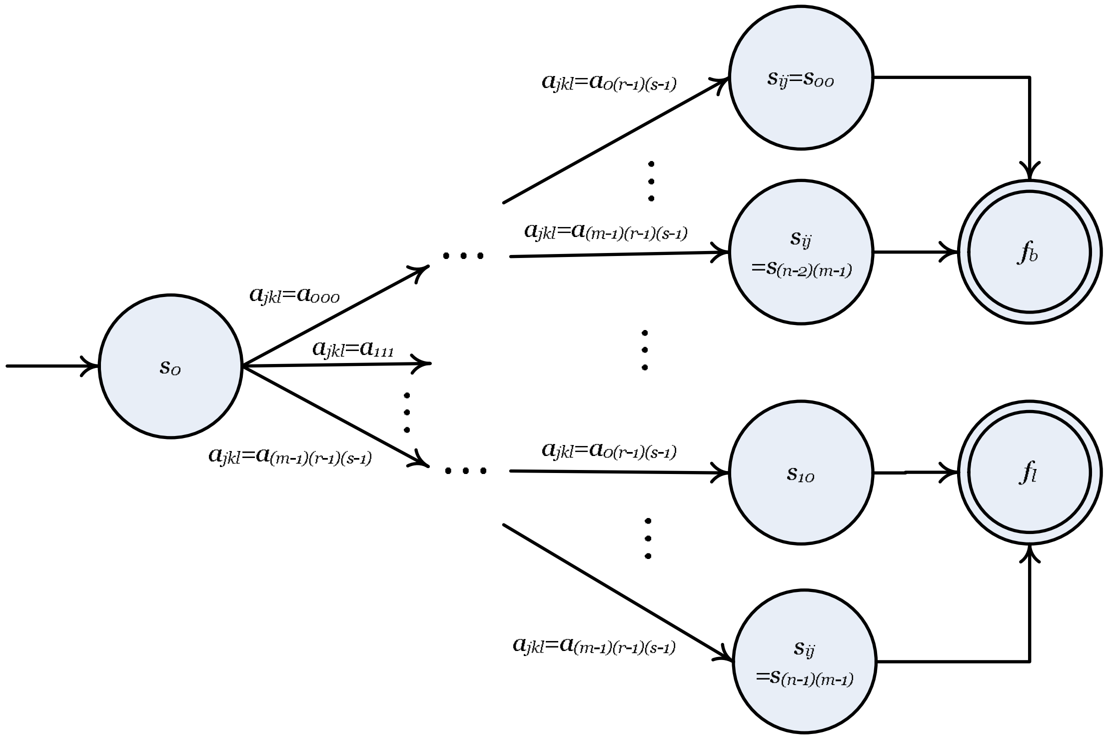

Figure 1: State diagram depicting the possibility of any team member betraying the team.

The state diagram in Figure 1 depicts the FSM scenarios in which any member can betray the team. This includes group sensitivity and target influence, explained in the section entitled Virtual Betrayal Simulation.

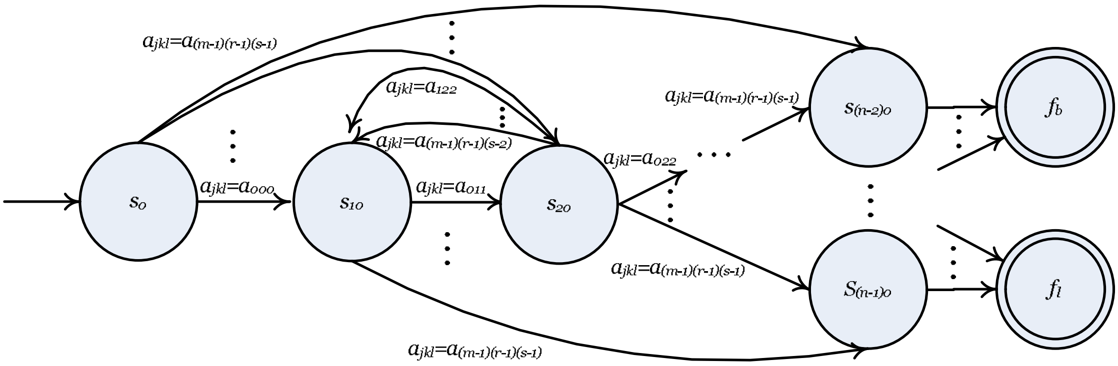

Figure 2: State diagram depicting the possibility of a critical member betraying the team.

In the virtual betrayal simulation, group sensitivity shows no visible impact on the observations of the Team-Leader's emotional state, but the target influence does show such an impact. In addition, the simulation is designed to determine how we may correlate mood with Team-Leader's betrayal if the Team-Leader betrays the team. Thus, the state diagram Figure 2 depicts the scenarios in which only a Team-Leader can betray the team, with a focus on target influence.

5 Results

Team-Leaders Crocodile and Dragon ended up betraying their teams, while Team-Leaders Alligator and Buffalo remained loyal to their teams. We then analyzed whether emotions and language could have predicted the betrayal. We labeled each scenario from an etic perspective, first identifying which utterances appeared to be emotionally charged, and then - for each of these utterances - we ascribed an emotion from a pre-defined list of emotions. Appendix A – Coding Scheme lists emotions and justifications for associating the emotions with a person's utterance. We selected the various emotions listed in the table to include the main emotions listed in the results of Ochs et al. [26], Kaiser and Wehrle [17], which relate to emotionally-charged online games. We based justifications in Appendix A – Coding Scheme on rationales provided by Scherer [35].

After annotation of the transcript for each scenario, including the text of emails, chats, and blogs by three labelers, we made a comparison to determine 1) which utterances were consistently labeled as expressing an emotion and 2) for these utterances, which ones were consistently labeled with the same emotion. In addition, we determined how many times an emotionally charged utterance about the Team-Leader occurred - from the perspective of the group - and from the Team-Leader. The results are presented in **Table 1**.

The use of language in expressing one's emotions plays a large role in online communication. We found emotionally-laden utterances in the attribution of Team-Leaders' Crocodile and Dragon. We also identified that emotional changes in Teams Crocodile and Dragon occur more often than in Teams Alligator and Buffalo (**Table 1**).

Table 1. Emotionally Changed Utterances in Four Simulated Case Studies by Three Annotators.

Scenario	Total Emotional Phrases			Group Speaking About Leader			Leader Speaking About Self		
Annotator	1	2	3	1	2	3	1	2	3
Alligator	495	866	367	132	64	95	42	14	17
Buffalo	214	695	173	27	35	16	27	14	12
Crocodile	286	691	502	43	68	51	38	9	14
Dragon	290	689	425	80	88	90	40	27	31

These emotions range from excitement (in anticipation of the next game) to anger (resulting from arguments with each other). The results indicate that unintentional repetition of errors is not a strong indicator for predicting betrayal; it refers to the fact that a particular individual may be incompetent by nature. On the contrary, a person may be very competent in leadership and management - and yet be influenced to betray the team. Furthermore, scenarios with more negative emotions (ones where the team performed poorly) generate more utterances wherein the group questions the leader. In scenarios where the group performs to the team members' expectations, participants have no need to probe the leader's intentions or competence.

5.1 Sample Data and FSM State Diagrams

Appendix B – Sample Dialogue shows raw data of online conversations between Crocodile team members and their Team-Leader. Since it is a raw data, it includes typos, which intentionally were not corrected to show the original data. But, strong negative words which are not suitable to show in this paper were changed to multiple x letters. In order to protect the participants' privacy, we change the participants' names to Member One, Member Two, Member Three, Member Four, Member Five and Member Six, etc.

These conversations were color-coded with their emotional states according to the Appendix A – Coding Scheme. The changes of emotional is represented in a digested form using FSM state diagrams as shown in Figure 3 and Figure 4. Both figures show a part of important emotional state changes.

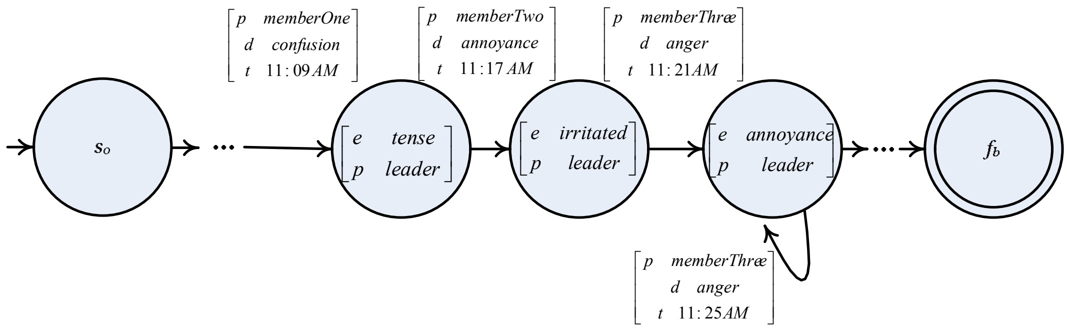

Figure 3. Sample of the changes of a Team-Leader's emotional states.

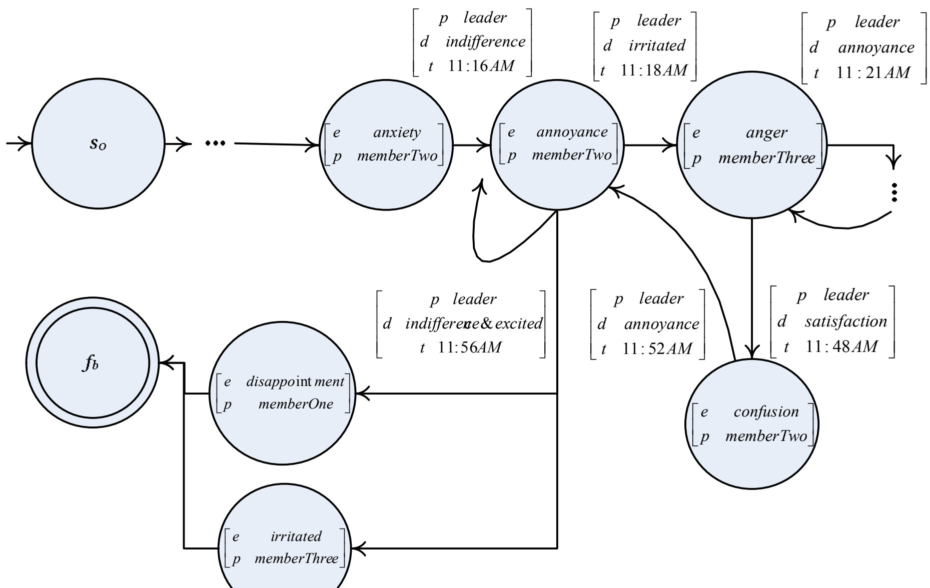

Figure 4: Sample of the changes of Team Members' emotional states.

In the virtual betrayal simulation, group sensitivity shows no visible impact on the results, but the target influence does show such an impact. In addition, the simulation is designed to determine whether the Team-Leader betrays the team. Thus, the state diagram Figure 2 depicts the scenarios in which only a Team-Leader can betray the team, with a focus on target influence. The state diagram Figure 3 shows a sample of the Team-Leader's emotion changes. The state diagram Figure 4 shows a sample of team members' emotional changes in response to the Team-

Leader's input in dialogues. In the figure, Team-Leader's emotion and team members' emotion is not consistent. For instance, when team member two expresses anxiety, the Team-Leader shows indifference at 11:16am. When team member two expresses annoyance, the Team-Leader shows indifference and excitement. Although the emotional disconnection between the leader and the members is not always a positive alarm to detect the Team-Leader's betrayal, it can be observed. This happens because when the Team-Leader decides to betray the team members, the Team-Leader's emotional change is triggered by a different goal than the team members' goal.

5.2 Group's Emotional Ties to the Target in Virtual Team

We captured the analysis of the emotional states of all team members in four experiments based on **Table 1**. Figure 5 shows the data in a network format comparing each player's emotions toward the Team-Leader (depicted as the crown) by the connecting lines to the respective emotions. The emotional states of the Team-Leader refer to his or her emotions toward him/herself or in defending his/her position. The bigger the emotion nodes, the more the states were applied in the group, as compared to the other listed emotions. The thickness of the edges corresponds to the repeated times said player expressed the referred emotional states.

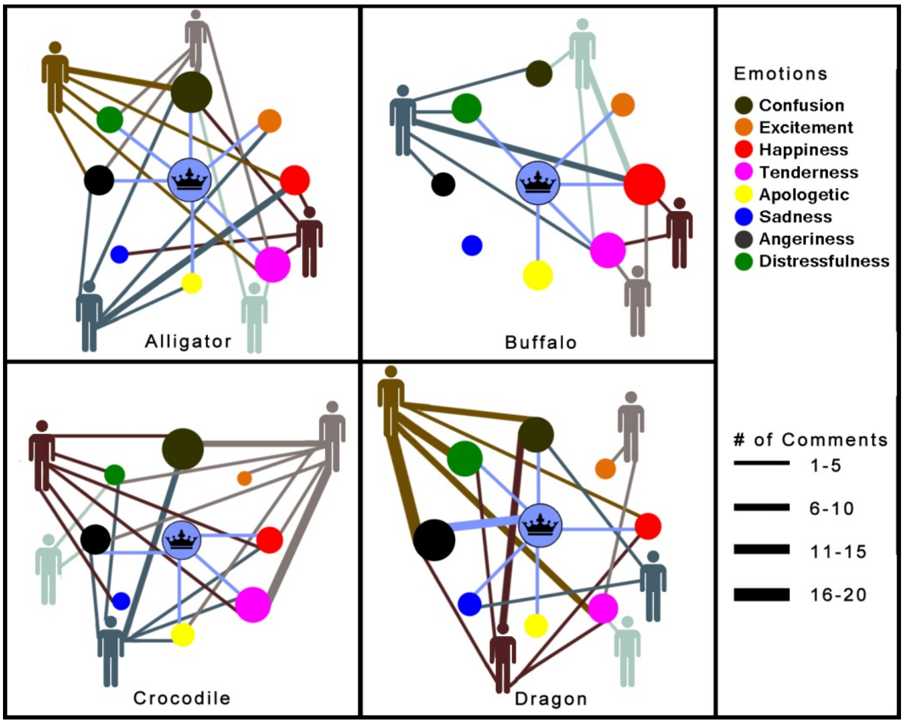

Figure 5. Group members' emotional states toward the target.

Let's consider Team Alligator. The node with brown color indicates that this player was filled with anger. The thickness of the edges connecting this brown player to her immediate nodes indicates the frequency with which this brown player had expressed this feeling to her teammates toward their Team-Leader. At the end of the game, most of the team members have colors related to negative emotions such as anger, victimization, confusion, sadness, etc. towards the target, Team-Leader, and Leader's emotions towards their team is also negative.

The overall analysis shows that both Teams Crocodile and Dragon - which performed poorly on the game and in which both Team-Leaders' ultimately betray their team - have more members with negative emotions (e.g., distressfulness, angriness, and confusion, etc.) towards the Team-Leader and vice versa. While Team Alligator shows more emotional connection to confusion due to the incompetence of Team-Leader Alligator, Teams Alligator and Buffalo in general show positive emotions such as happiness, excitement, and tenderness. Team-Leaders Alligator and Buffalo were not presented with the opportunity to betray their teams in the game.

6 Conclusions and Future Work

Our research design is based on trustworthiness attribution theoretical framework. Since humans are an important factor in countering insider threat, we simulated cyber insider threat scenarios using the analogy of humans as sensors on a social network detecting behavioral changes of a focal individual. This threat simulation was conducted in virtual team settings, where members of each team volunteer to collaborate to achieve a pre-determined team goal. This socio-technical research design enabled us to collect and analyze a full spectrum of insider threat data using deterministic finite-state machines.

In conclusion, note that language use in chat rooms includes many subtle cues. Hypotheses about language used in virtual teams - especially in insider threat simulations - can present challenges in formulating and testing. The use of finite state machines aids our understanding of group dynamics in cloud communication environment.

Groups demonstrated emotionally-laden utterances such as “angriness,” “distressfulness,” and “confusion” toward the target at the point where the target individual acts to betray. At the same time, groups also demonstrated a significant amount of emotionally-related utterances such as “confusion” and “tenderness” toward the target individual when the target did not live up to the group’s expectations, implying that team members’ sensed incompetency and a lack of leadership. We plan to further investigate our theoretical framework in Figure 1-4 when we can look at patterns of speech acts and levels of trust. How often do people make requests of people they consider not trustworthy? We also plan to identify patterns of emotional communication from these utterances.

In addition, as we analyzed a mere hundreds of utterances in all, it would prove difficult to determine a comparison between this study and other studies that look at DFAs for use in modeling emotion. We can derive commonalities from the similarities of the emotions studied and the variables used to determine when an emotion is triggered, but the creation of an automatic analysis is not possible due to the relatively small amount of data available. Making an attempt to divide the data between training and test data would be very difficult. Training data for such mechanisms require thousands of instances. Therefore, when the different patterns are reported, they are based on manual analyses. Future work will include a larger sample size and more automated analyses.

Furthermore, this study used each state of a DFA to capture a particular emotion labeled at a given time. As language triggers emotions, it would be impossible to put the edge trigger on the arc between states, as this study has so many possible triggers. Future work could consolidate the possible language triggers for further analysis. At this time, the authors hope to determine significantly different emotional patterns, if any - over time - that appear when the target is trusted, and also when the target is viewed under suspicion.

Acknowledgement

The authors thank Kathleen Murray, Roberto Salome, Issam Ahmed, Nazha Elhasnaoui, Nora McDonald, and Dhanesh Neela Mana at Drexel University for their participation of data analysis. The first author wishes to thank Conrad Metcalfe for his editing assistance.

References

[1] I. Ajzen, Attitudes, Personality, and Behavior, The Dorsey Press, 1988.
[2] J. B. Asendorpf, "Head-to-head comparison of hte predictive validity of personality types and dimensions," *European Journal of Personality*, vol. 17, no., pp. 327-346, 2003.
[3] Bernstein, Penner, Clarke-Stewart and Roy, Psychology (8th Ed.), Houghton Mifflin Company, 2008.
[4] W. Bosma and E. Andre, "Exploiting Emotions to Disambiguate Dialogue Acts," in *Proc. of the 9th International Conference on Intelligent User Interfaces (IUI'04)*, *Funchal, Portugal*, ACM, January 2004, pp. 85-92.
[5] H. E. Cattell, "The original big five: a historical perspective," *European Review of Applied Psychology*, vol. 46, no. 5-14, 1996.
[6] Software Engineering Institute, Carnegie Mellon University, "CyberSecurity Watch Survey: How Bad is the Insider Threat?," www.cert.org/archive/pdf/CyberSecuritySurvey2011Data.pdf, 2011.
[7] A. Egges, S. Kshirsagar and N. Magnenat-Thalmann, "Generic Personality and Emotion Simulation for Conversational Agents," Computer Animation and Virtual Worlds, vol. 15, no. 1, pp. 1-13, January 2004.

[8] P. Ekman and W. V. Friesen, Unmasking the Face, Prentice Hall, 1975.
[9] F.B.I. Press Release, "FBI History Famous Cases: Robert Philip Hanssen Espionage Case," 2001.
[10] A. Furnham and J. Crump, "Personality Traits, Types, and Disorders: An examination of the relationship between three self-report measures," *European Journal of Personality*, vol. 199, no., pp. 167-184, 2005.
[11] R. Hardin, "Gaming Trust," in: E. Ostrom and J. Walker (Eds.), *Trust and Reciprocity: Interdisciplinary Lessons From Experimental Research, Russell Sage Foundation*, New York, pp. 80-101, 2003.
[12] F. Heider, The Psychology of Interpersonal Relations, John Wiley & Sons, 1958.
[13] F. Heider, "Social Perception and Phenomenal Causality," *Psychological Review*, vol. 51, no. 6, pp. 358-374, November 1944.
[14] S. M. Ho, "Attribution-Based Anomaly Detection: Trustworthiness in an Online Community," in: H. Liu, J. J. Salerno and M. J. Young (Eds.), *Social Computing, Behavioral Modeling, and Prediction*, Springer-Verlag, pp. 129-140, 2008.
[15] S. M. Ho, "Behavioral Anomaly Detection: A Socio-Technical Study of Trustworthiness in Virtual Organizations," Ph.D. Thesis, Syracuse University, 2009, from http://surface.syr.edu/it_etd/47/.
[16] S. M. Ho, "A Socio-Technical Approach to Understanding Perceptions of Trustworthiness in Virtual Organizations," in: H. Liu, J. J. Salerno and M. J. Young (Eds.), *Social Computing, Behavioral Modeling, and Prediction*, Springer-Verlag, pp. 113-122, 2009.
[17] S. Kaiser and T. Wehrle, "Situated Emotional Problem Solving in Interactive Computer Games," in *Proc. of the Proceedings of the VIXth Conference of the International Society for Research on Emotions (ISRE'96)*, Storrs, Connecticut, USA, ISRE Publications, 1996, pp. 276-280.
[18] S. Kaiser and T. Wehrle, "Situated Emotional Problem Solving in Interactive Computer Games," in *Proc. of the VIXth Conference of the International Society for Research on Emotions (ISRE'96)*, Storrs, Connecticut, USA, ISRE Publications, 1996, pp. 276-280.
[19] H. H. Kelley, "The Process of Causal Attribution," *American Psychologist*, vol. 28, no. 2, pp. 107-128, February 1973.
[20] H. H. Kelley, J. G. Holmes, N. L. Kerr, H. T. Reis, C. E. Rusbult and P. a. M. Van Lange, "The Process of Causal Attribution," *American Psychology*, vol. 28, no. 2, pp. 107-128, 1973.
[21] H. H. Kelley, J. G. Holmes, N. L. Kerr, H. T. Reis, C. E. Rusbult and P. a. M. Van Lange, "An Atlas of Interpersonal Situations," Cambridge University Press, 2003.
[22] D. C. Mcclelland, "Human Motivation," Cambridge University Press, 1987.
[23] R. R. Mccrae and P. T. Costa Jr., "Validation of the five-factor model of personality across instruments and observers," *Journal of Personality and Social Psychology*, vol. 52, no. 1, pp. 327-346, 1987.
[24] R. R. Mccrae, A. Terracciano, P. T. Costa Jr. and D. J. Ozer, "Person-factors in the California adult Q-set: Closing the door on personality types?," *European Journal of Personality*, vol. 20, no., pp. 29-44, 2006.
[25] K. D. Mitnick and W. L. Simon, "The Art of Deception: Controlling the Human Element of Security," Wiley, 2002.
[26] M. Ochs, N. Sabouret and V. Corruble, "Modeling the Dynamics of Non-Player Characters' Social Relations in Video Games," in *Proc. of the 4th Artificial Intelligence and Interactive Digital Entertainment Conference Stanford, California, USA,* Association for the Advancement of Artificial Intelligence, October 2008, pp. 90-95.
[27] D. B. Parker, "Fighting computer crime: a new framework for protecting information," John Wiley & Sons, 1998.
[28] K. L. Pike, "Language in Relation to a Unified Theory of the Strucure of Human Behavior," Summer Institute of Linguistics, 1954.
[29] K. L. Pike, "Discourse Analysis and Tagmeme Matrices," *Oceanic Linguistics*, vol. 3, no. 1, pp. 5-25, Summer 1964.
[30] A. Pinsonneault and K. L. Kraemer, "Survey Research Methodology in Management Information System: An Assessment," *Journal of Management Information Systems*, vol. 10, no. 2, pp. 75-105, 1993.
[31] D. J. Pittenger, "The limitations of extracting typologies from trait measures of personality," *Personality and Individual Differences*, vol. 37, no., pp. 779-787, 2004.
[32] I. Ray and N. Poolsapassit, "Using Attack Trees to Identify Malicious Attacks from Authorized Insiders," in *Proc. of the 10th European conference on Research in Computer Security (ESORICS'05)*, *Milan, Italy*, *LNCS*, vol. 3679, Springer-Verlag, September 2005, pp. 231-246.
[33] R. Richardson, "14th Annual CSI Computer Crime and Security Survey Executive Summary," *CSI Computer Crime and Security Survey*, 2009.
[34] G. Saucier and L. R. Goldberg, "The language of personality: Lexical perspectives on the five-factor model," in: J. S. W. (Ed.) (Eds.), "*The five-factor model of personality: Theoretical perspectives*," Guilford, New York, 1996.

[35] K. R. Scherer, "Criteria for Emotion-Antecedent Appraisal: A Review," in: G. H. B. V. Hamilton, & N.H. Frijda (Eds.), "*Cognitive Perspectives on Emotion and Motivation*," Kluwer, pp. 89-126, 1988.
[36] E. E. Schultz, "A framework for understanding and predicting insider attacks," *Computers & Security*, vol. 21, no. 6, pp. 526-531, 2002.
[37] E. C. Tupes and R. E. Christal, "Recurrent Personality Factors Based on Trait Rating.," 1961.
[38] L. Von Ahn, "Games with a Purpose," *IEEE Computer Magazine*, vol. 39, no. 6, pp. 96-98, 2006.
[39] L. Von Ahn, B. Maurer, C. Mcmillen, D. Abraham and M. Blum, "reCAPTCHA: Human-based Character Recognition via Web Security Measures," *Science*, vol., no., pp. 1465-1468, 2008.
[40] B. Weiner, "Social Motivation, Justice and the Moral Emotions: An Attributional Approach," Lawrence Erlbaum Associates, Inc., 2006.
[41] Y. Zhu, Z. Yang, H. Meng, L. Baichuan, G. Levow and I. King, "Using Finite State Machines for Evaluating Spoken Dialog Systems," in *Proc. of the 2010 IEEE Spoken Language Technology Workshop (SLT'10), Berkeley, California, USA*, IEEE, December 2010, pp. 478-483.

Shuyuan Mary Ho, Ph.D. is Assistant Professor in the iSchool, College of Communication and Information at Florida State University. Shuyuan's research focuses on trusted human-computer interactions, insider threats, identity theft, using games for research analytics, natural language processing, and computational modeling. Shuyuan received her Doctoral of Philosophy Degree in Information Science and Technology from iSchool at Syracuse University in 2009.

Hwajung Lee, D.Sc. is an associate professor in the department of Information Technology at Radford University, Virginia, USA. She received the Doctor of Science degree in Computer Science from George Washington University in 2003. Her research interests include network algorithm and security in optical networks, ubiquitous computing networks, grid computing networks, and wireless sensor networks.

Appendix A – Coding Scheme

Category	Color Scheme	Possible Emotions	Description
Excitement	Excited	excitement (ecstasy)	great enthusiasm, anticipation
		energetic	operating with vigor
		aroused	stimulated, awakened
		bouncy	animated
		perky	briskly self-assured, cheerful
Happiness	Happy	fulfilled	to meet the requirements
		satisfaction	a sense of completion, reaching the desired result
		pride	expressing happiness from achievement
		happiness (joy)	happy, but not relief or pride
		surprise	A state of astonishment
		gratitude	being thankful
		confidence	consciousness of one's power or of self-reliance
		pleased	to afford pleasure
		relief	feeling after a negative emotion has resolved
Tenderness	Tender	intimate	warm or familiar communication
		affection	tender attachment
		loving	Affectionate
		warm hearted	marked by ready affection, cordiality, generosity, or sympathy
		hope	to desire with expectation of obtainment belief in positive outcome?
		empathy	capable of understanding, and to some extent, sharing the feeling of others
		kind	of a sympathetic or helpful nature
		soft	agreeable to the senses
		shyness	easily frightened; hesitant in committing oneself
		loneliness	being without company
		worry	to afflict with mental distress or agitation
		envy	resentful awareness of an advantage enjoyed by another joined with a desire to possess the same advantage
		disgust	to provoke to loathing or aversion; be offensive to
		hatred	prejudiced hostility or animosity
Apologetic	apologetic	apologetic	uses the word "sorry," apologizes
		weakness	the quality or state of being weak
		helplessness	lacking support from expected resources
		doubt	input is too uncertain to believe
		confusion	input is unclear
Sadness	Sad	down	to a lesser degree; in a lower or worse condition
		blue	low in spirits
		indifference	of no importance or value one way or the other; marked by a lack of interest or enthusiasm
		sadness/grief	experiencing a loss of something valuable
		rejected	to refuse to accept, consider, submit to
		fear	anticipating a negative event
		depression	being below the standard; low in spirits
Distressfulness	Scared	tense	state of mental or nervous strain
		nervousness	timid, easily irritated; feeling nervous
		anxiety	painful or apprehensive uneasiness of mind, fearful concern
		jittery	a sense of panic, or extreme nervousness
		frightened	to make afraid
		terrified	to impel by menacing, scare; a state of intense fear
		suffering	to submit to or be forced to endure, experience of unpleasantness
		despair	to lose all hope or confidence
Angriness	Angry	irritated	to provoke impatience, anger, or displeasure in
		resentful	to feel or express annoyance or ill will at someone or something other(s) have obtained
		annoyance	not happy with current situation
		disappointment	not reaching a goal
		annoyance	to disturb or irritate especially by repeated acts
		anger/frustration	to balk or defeat in an endeavor
		furious	goaded by anger
		raging	violent and uncontrolled anger

Appendix B – Sample Dialogues

Day	Time	Role	Dialogue	Emotional State
Day 5	11:09 AM	Member One	I have no idea what that means, though	confusion
Day 5	11:09 AM	Member One	so what's the next?	frightened
Day 5	11:10 AM	Team-Leader Crocodile	im putting it	tense
Day 5	11:10 AM	Team-Leader Crocodile	times about to run out	tense
Day 5	11:11 AM	Member Two	team-leader: can you see our performance so far?	anxiety
Day 5	11:15 AM	Member Two	to our team leader: could you post our performance after each question?	hope
Day 5	11:16 AM	Team-Leader Crocodile	it doesnt come up that quick but when i find out i will post it	indifference
Day 5	11:17 AM	Member Two	please make it asap	annoyance
Day 5	11:18 AM	Team-Leader Crocodile	ya were struggling too	irritated
Day 5	11:18 AM	Team-Leader Crocodile	i can only post it when it comes out so theres only so much i can do	irritated
Day 5	11:20 AM	Member Five	you wouldnt believe where i found the answer	surprise
Day 5	11:20 AM	Member Five	the bakerview elementary website	surprise
Day 5	11:21 AM	Member Two	I can read the xxxxing chat logs, but not log in, d you know how FRUSTRATING THIS IS????	anger/frustration
Day 5	11:21 AM	Team-Leader Crocodile	thats really strange.	annoyance
Day 5	11:22 AM	Member Two	great, thanks. how do you know that?	relief
Day 5	11:22 AM	Team-Leader Crocodile	becasue when they post our score sometimes they post the answers	indifference
Day 5	11:24 AM	Member One	oh! i get it.	relief
Day 5	11:25 AM	Member Two	No one is posting on the message boards to talk to me, and I am really annoyed b/c i want a gift certificate!!!	anger/frustration
Day 5	11:27 AM	Team-Leader Crocodile	try not to post answers already said to keep things simple	annoyance
Day 5	11:27 AM	Member One	sorryy.they literally didn't show up until I'd already posted	apologetic
Day 5	11:28 AM	Team-Leader Crocodile	oh ok no worries	empathy (sympathetic)
Day 5	11:30 AM	Member Two	I am reading the chat log behind you guys. - The girls in my office are SCREAMING and arguing over the ball question, its ANNOYING ME!	anger/frustration
Day 5	11:34 AM	Team-Leader Crocodile	1 min left	tense
Day 5	11:38 AM	Member One	wow. that does work.	surprise
Day 5	11:38 AM	Team-Leader Crocodile	i think Member Five is right	pride
Day 5	11:39 AM	Member Two	HEY HELLO I am trying to read the quetions and you didn't even post it!	anger/frustration
Day 5	11:40 AM	Member Four	sorry sorry sorry team leader You saw me not that active 2day,right? coz I have a urgent presentation to prepare just in this morning since I have to present it at noon. really sorry about.	apologetic
Day 5	11:40 AM	Member Two	Next time post the question to the board please - how do you think I knew the question?	irritated
Day 5	11:43 AM	Team-Leader Crocodile	Member Five why werent you doing this all week	perky
Day 5	11:43 AM	Team-Leader Crocodile	we wouldve gotten every question right!	perky
Day 5	11:44 AM	Member One	That was the most frustrating session yet	anger/frustration
Day 5	11:45 AM	Member Five	but hey its over and friday	relief
Day 5	11:45 AM	Member Two	WITH LAG TIME! I can't watch it LIVE as it happens - I keep trying to refresh and it takes forever and it is VERY delayed.	anger/frustration
Day 5	11:47 AM	Member Two	Hey guys,Glad its over, but today really sucked hard for me! I coudln't read what you were saying, and they stopped posting the questions for me on the forum after question 6!! I could	anger/frustration

Day	Time	Role	Dialogue	Emotional State
			check the chat log, but with only serious lag time...so fairly frustrating - I needed a bit more communication on the boards :(	
Day 5	11:48 AM	Team-Leader Crocodile	i think we should be in the top 2	satisfaction
Day 5	11:49 AM	Member Two	then how to they assess our answers?	confusion
Day 5	11:52 AM	Member Two	wait, you didn't give me merrybux on Wed	confusion
Day 5	11:52 AM	Team-Leader Crocodile	i sent them out this morning	annoyance
Day 5	11:53 AM	Team-Leader Crocodile	1st place today	happiness (joy)
Day 5	11:53 AM	Member Two	woo hoo!	happiness (joy)
Day 5	11:53 AM	Member Six	cooL!!!	happiness (joy)
Day 5	11:54 AM	Member Two	we finally got the 1st palce!!	relief
Day 5	11:55 AM	Member Two	and I'm also wondering how much merrybux to get today!!	anxiety
Day 5	11:55 AM	Member Two	but how come I didn't get much for the previous days?	annoyance
Day 5	11:56 AM	Team-Leader Crocodile	well they were limited the last few days since i only had 40 to distribute	indifference
Day 5	11:56 AM	Team-Leader Crocodile	but now i have 120 to share	excitement (ecstasy)
Day 5	11:59 AM	Member One	That sucks. I think we got first today, despite the fact that the answers were rid. hard. We also only had six or seven questions total, I think. The game ended quite early for some reason.	dissapointment
Day 5	12:07 PM	Member Two	Crocodile is not emailing the merry bux and nor is this person answering any of the emails I am sending them, and I really have other things to do now rather than wait for him and fill out surveys, could you please tell them to hurry?	irritated
Day 5	12:37 PM	Member Two	eXperimenter, Ok I filled everything out :-). I have to admit, I was getting suspicious that you game masters and stuff were screwing with me a little bit in me not getting into the chat- or like...that maybe you were the team leader. Like that experiment where they had people deliver electric shocks and stuff :-p. Anyway - good game	annoyance
Day 5	3:32 PM	Member Two	I wonder if the MerryBux is fairly assigned to us. Can you let me know how much you got from the team leader? I only got 18 MerryBux however he/she said there are 120 MerryBux in totally for today (this was told in the chat room)!I feel there are extra money gone...Any idea on this?	annoyance
Day 5	3:34 PM	Member Two	Nothing though...The MerryBux doesn't seem to be fairly assigned among us. Can you let me know how much you got from the team leader? I only got 18 MerryBux however he/she said there are 120 MerryBux in totally for today (this was told in the chat room)!I feel there are extra money gone...Any idea on this?	annoyance
Day 5	7:59 AM	Member Two	Yeah I only got 15 Merry Bux - and the leader screwed me becuase he stopped posting the questions on the message board.	irritated