REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
21-02-2023	Final Report	21-Aug-2009 - 20-Aug-2010

4. TITLE AND SUBTITLE
Final Report: ARO Workshop on Trustworthy Social Computing

5a. CONTRACT NUMBER
W911NF-09-1-0445

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES

University of California - Davis
Sponsored Programs
1850 Research Park Drive, Suite 300
Davis, CA 95618 -6153

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)

U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
57004-NC-CF.1

12. DISTRIBUTION AVAILIBILITY STATEMENT

2 Approved for public release; distribution is unlimit

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			S. Wu
UU	UU	UU	UU		19b. TELEPHONE NUMBER: 530-754-7070

RPPR

as of 22-Feb-2023

Agency Code:

Proposal Number: **Agreement Number:**

Organization:
Address: , ,
Country:
DUNS Number: EIN:
Report Date: Date Received:
for Period Beginning and Ending
Title:
Begin Performance Period: **End Performance Period:**
Report Term: -
Submitted By: Email:
Phone:

Distribution Statement: -

STEM Degrees: **STEM Participants:**

Major Goals:

Accomplishments:

Training Opportunities:

Results Dissemination:

Plans Next Period:

Honors and Awards:

Protocol Activity Status:

Technology Transfer:

I certify that the information in the report is complete and accurate:
Signature:
Signature Date:

Research Challenges and Roadmap of Trustworthy Social Computing
Sponsored by Army Research Office (ARO)

This short report is the outcome of the ARO/TSC workshop taking place on July 20~21 of 2009 at University of California at Davis.

Introduction

Social computing concerns the study of social behavior and context based on communication and computing systems. Unparalleled amounts of information are exchanged, among devices or a community of human users, in order to support social-based communication activities. The results from these activities have dramatically changed both the value of the communication and the social relationships among the communicating parties. As an example, online social network services like Facebook with 350+ millions users offer a convenient platform for interactions, friendship formation, and other unprecedented social activities. While numerous online social computing applications/systems are being developed in an unparalleled pace, many issues related to trust management, social computing, trust assessment, and their relationships remain unexplored and unanswered. In particular, the information being shared and exchanged, in a social context explicitly or implicitly, forms the basis of the notion of "***social soft trust***". ***Social soft trust*** can be valuable in detecting anomalous/malicious activities and enhancing the level of situation awareness under critical military missions when the traditional "***harder trust***" is either compromised or unavailable. In this document, we will discuss challenges and roadmaps regarding both how to assess and protect the value of social computing systems and how to leverage such systems to support the notion of soft trust.

A Motivation Example of Social Soft Trust

Traditionally secure communication activities have been supported via mechanisms such as authentication, authorization, access control, integrity, encryption, intrusion detection and prevention. Each of these schemes helps in strengthening at least one perspective of trustworthiness in communication. For instance, soldier X authenticated himself while reporting a critical situation M via an encrypted channel E to an authorized commander C at time T. The commander D or his analysis agent program has to trust the reported information based on the status of all the entities on the information path from X to C, deterministically or probabilistically. However, a number of such entities can be compromised or faulty. X might make a mistake or can be subverted. M's integrity could not be decided due to a revoked certificate. Hence, it is critical that the path from X to C be ensured to be trustworthy. Social computing can help. In the above scenario, the commander C or his program could use some "extra" social-network information to help further determine the trustworthiness of the information M. For instance, C might derive that another soldier Y has a close social relationship with X and, according another friend Z, X and Y might be in the same physical location at time T. This social inference determines that Y would be an excellent verifier/observer to evaluate the correctness of the information M since Y can observe not only the situation described by M but also the reporter X himself. Under this simple example, social computing information such as the

friendships among X, Y, and Z is leveraged to boost the confidence level of the intelligence information we need.

Research Challenges

Protecting the Value of Social Network Infrastructure: As shown in our example, social-network information can be crucial in enhancing the trustworthiness of needed information. However, from a system perspective, this social network system itself could be compromised. For instance, the information about the friendship between X and Y is valuable only if we know that the friendship itself is *bona fide*. In typical commercial social networks like Facebook, a significant portion of friendships is between two social entities that have never met in person. This is still a very open problem as the attackers will utilize not only the traditional software/protocol vulnerabilities but also real-life social channels to penetrate our social network system to reduce its value. For realizing a social soft trust system under a military context, we must first architect the social network infrastructure to prevent problems such as Sybil, collusion, loose and unrealistic relationship. Another critical research challenge is to develop a mathematical model to describe and characterize social network attacks based on both system and social vulnerabilities.

Social Soft Trust, Theoretical Model and Validation: Given a social network infrastructure, it is very interesting to study how this valuable infrastructure can be utilized to characterize quantitatively the trustworthiness between two human users or between a device (and its information content) and a human. To realize such a vision, we must first understand and develop the theories behind how such a notion of soft trust can be specified, built/updated, and analyzed. Furthermore, it is particularly challenging to validate and compare proposed models against both the real-world social network data and the potential attacks against such research models. Finally, it is equally important to study and understand how human social relationships (or the motivation to develop new relationships and form groups) might be changed due to the awareness of the social soft trust system behind these communication activities. As an example, the soldier X might want to form relationships with all other soldiers close to him such that the social network can provide support and protection for his operation/mission.

Social Intelligence Analysis: With a social network infrastructure in place, we will have an enormous amount of, potentially unstructured, social information available. While terabytes of online social network data are being produced daily, we like to investigate how these data sets can be analyzed and correlated, statistically, linguistically, and temporally, for purposes of situation awareness, hidden group detection, and information flow/propagation analysis.

Identity Management for Trustworthy Social Computing. Today we have organizational and software procedures that control the exchange of interpersonal information in social networking sites, text messaging, instant messenger programs, bulletin boards, online role–playing games, computer–supported collaborative work, and online education. All of these applications fit into a larger category of social media such as social software and social networking. *Digital identity* is a fundamental building block of a variety of social and business activities in such a dynamic cyberspace. It generally represents the separateness, existence, and personality of an individual within social media. Also, it provides a mechanism for identification, accountability, and

convenience in various human activities in social networks. To support this, most of these social networks collect and process information regarding their entities, generally individuals, and offer a variety of features such as personalization, affinity sharing, accelerated networking, and novel services. In other words, social networking sites can create a central repository of personal information. These archives are persistent and cumulative. Consequently, marketers, school officials, and online predators can collect data about users through online social networking sites. As the use of personal information in social networks seems manifold, including the representation of an individual's digital persona (or social role) and identification, so does the abuse or misuse of the information. Digital identity concerns not only user authentication but also other important services for virtual communities, and it is believed that digital identity is a set of user information that encompasses authentication information, usage control information, and other user data collected based on a variety of purposes and uses. Therefore, we need to investigate an advanced approach to manage users' personal attributes considering a notion of digital persona (or social role) and associated risks in disclosing such private information over virtual communities such as social networks.

Analyzing Social Dynamics for Countering Net-centric Attacks. While there is some knowledge on the ways that vulnerabilities are exploited, there is little research exploring the ways that attack agents such as bots and malicious codes are distributed across social media or in a social-network infrastructure. Individuals who control existing bot networks also sell access to their infected machines for a variety of attacks including spam and denial of service attacks. As a consequence, these markets enable a great deal of unskilled computer users to engage in cybercrime. Therefore, it is necessary to systematically investigate the creation, distribution, and attack patterns of attack agents circulating social media. This vital information can be used to further investigate specific social communities related to adversarial threats and to further detect and prevent such net-centric threats.

Trust Assessment in a social-networking environment: This is an essential research issue when apps can be easily produced, widely deployed, and effortlessly used, and in the meantime, the entry barriers are so low that a growing number of users join in and make contributions. Their participation in a social networking environment can be tapped as a source of crowd intelligence or wisdom to help trust assessment of various sorts. Using the motivating example presented earlier, commander C faces an obvious decision problem: whether and when or now s/he should raise the suspicion that the information path from X to C might be compromised, and have means to verify (confirm or refute) the suspicion. The social networking information can be used to provide significant help if one can reliably perform trust propagation and trust initialization. Trust propagation is a well-studied topic along with related issues such as rumor spreading, disease diffusion, and information dissemination. Trust initialization is a less explored area. It studies how initial values of trustworthiness of interested parties (or actors, nodes) can be properly determined. Crowdsourcing via social media is one effective means. Finding influential players in a social network can also help trust initialization. With both trust initialization and propagation, one can reasonably carry out trust assessment.