Small Steps and Giant Leaps toward Homeland Security

Leona F. Fass

P.O. Box 2914
Carmel CA 93921
lff4 [AT] cornell [DOT] edu

Abstract

AI Technologies are applicable to Homeland Security, particularly in problems of analysis, discovery and prediction. We describe relevant AI techniques including Link Analysis, dynamic Decision Support and Agent Organization modeling, whereby anomalous activities may be detected and threats deterred. We also discuss application of techniques in local government and to security matters close to home. We conclude that AI Technologies are immensely useful for improving security of citizens and the homeland, especially in conjunction with skilled human experts. But our position is that privacy cannot be fully protected if security is to be substantially enhanced.

Introduction

We consider issues of Homeland Security from both professional and personal perspectives: as a computer scientist and researcher, and as a citizen who often participates in local governmental matters. Furthermore, our AI-related experience with relevant areas of privacy, trust and security has been both observational and hands-on. As a result *we believe strongly that AI Technologies have been and can be immensely useful for improving security of citizens and the homeland, particularly in conjunction with sufficiently-skilled human experts. But we also believe* that *privacy cannot be fully protected if security is to be substantially enhanced.*

As a computer scientist we are aware of the very positive aspects of almost-universal Web access, but of negative aspects as well. We realize that "hit-and-run", essentially anonymous, access to public machines can have dire consequences nowadays, raising issues of privacy, trust and security that may not have been imagined when the Internet and Web came to be. We are aware of the complexities of Web and Semantic Web development, and the possibility that future Web-navigating software agents, originally intended to facilitate honest human access, may themselves compound and present security threats. We see user interface issues and scheduling and planning issues that can enhance or impede security, depending on how they are resolved. But mostly, we see problems of analysis, discovery and prediction, where anomalous behaviors may be detected and possible threats deterred. These are all areas where AI Technologies have an important role to play, to facilitate the work of human analysts and decision-making experts.

Security Begins at Home

As a long-term resident of a small village, we periodically become aware, and are amazed to learn, of security threats that become evident even at *our* local level. Who could anticipate that in an area with just a few thousand full-time residents, and an aging population of median age 54+, there could be: voter fraud grounded in identity deception; bomb scares necessitating robot deployment; spyware installed in citizen-accessible machines; or attempted purchase of illicit weapons *via* computers in the village library? But such things have happened, and more.

As someone originally born and raised in New York City, with family and friends directly affected by the events of the September 11, 2001 attacks and subsequent terrorist-related acts, we fully understand that security must be taken seriously. Now we must be able to anticipate and deter events that previously could hardly have been imagined. The activities described above, discovered in our current small-town environment, might be occurring throughout the country and the world, magnified by a factor of many thousand-fold. So here we discuss our own observations and discoveries, in our profession and as a citizen, that can result in small steps toward security locally, and can also lead to greater levels of security throughout the homeland.

Modeling and Prediction for Security

In our initial computer science research we devised inductive inference techniques whereby observed behaviors were analyzed to determine patterns of what *had* occurred, in order to predict what could occur in future. We also developed testing techniques to detect relatively anomalous behaviors, for purposes of adapting or correcting potential behavioral models. Although this work was first developed within the theoretical research area of Computational Learning, we found its applications had a broader, practical scope. We participated in an AI & Link Analysis symposium (Jensen and Goldberg 1998) where our own examples (Fass 1998) included some non-threat-related analyses and models of financial markets, and identity verification to protect the validity of the local

election process. At that time we were introduced to similar approaches to Behavioral Analysis, Data Mining and Prediction on a much greater scale, for detection of possible criminal acts and transnational threats. Thus, years before September 11, 2001, we learned that Organizational Theory, Network Analysis and tracing of Web hits could determine unusual activity indicative of bio-terrorist threats (Picarelli 1998). We learned that by integrating information extraction techniques with a relational database, criminal and terrorist associations and activities could be discovered (Lee 1998). We also learned that analysis of financial market transactions could reveal money laundering indicating criminal, and perhaps terrorist, acts (Goldberg and Senator 1998, Goldberg and Wong 1998). Numerous intelligence and law enforcement agencies had been looking into these processes for years; then came September 11, 2001, so that a multitude of technically astute researchers now think about these problems.

Many AI Technologies approaches currently deployed, or under development, to protect citizens and the homeland are discussed in (Yen 2004). These include the use of information technology for pattern analysis and predictive modeling, facilitating collaboration among counter-terror agencies and providing Decision Support. Such work is described by (Popp *et al* 2004). Their aim is to assist agencies in "sharing, analyzing and acting on the right information". Proactive decision support is discussed by (Kogut *et al* 2004), including the potential of Personal Assistant agents to aid in decision-making of first responders, anticipating their information needs and effecting coordination.

An application of the Organizational Theory approach to discovering transnational threats [that we first learned of from (Picarelli 1998)] is the more current work by (Berry *et al* 2004), employing the model of Agent Organizations to discover formation of terrorist cliques. Updated views of Data Mining to determine money laundering appear in (Zdanowicz 2004) and in (Kingdon 2004). The former shows us that analysis of import/export data reveals terrorist financing nowadays, and suggests anticipatory action that can provide some deterrence. The latter shows that by determining "usual behavior" in a financial market or banking environment, *un*usual behavior will become apparent and worthy of a second, investigatory, look. This approach provides adaptive, dynamic Decision Support. It can also protect privacy of an entity behaving "as usual", unless and until an anomalous act, necessitating investigation by a qualified expert, may occur.

Security and Privacy, on the Web and Locally

As we have expanded our behavioral modeling research, we have investigated Adaptive User Interfaces and the potential of the Semantic Web (Fass 2002, 2004). Such AI application areas have been developed with the goal of making machine, Internet and Web access easier for all citizens, not just those technically grounded. But these areas bring with them important considerations relating to privacy, and to security of citizens and the homeland. Two instances of particular interest to us have been the public's use of machines in our local library, and the possibility of our voting processes becoming fully electronic, at local polling places and, perhaps, online.

As a citizen involved with local government, we have made suggestions to the city administration, with respect to library access and security matters. We are concerned with issues of spyware, system integrity, Internet integrity, and the ramifications of universal access, including the potential of misuse. The library has made several iterative attempts to create a policy to balance privacy and security concerns, with a satisfactory balance yet to be achieved. E.g., now, on the one hand, access is given to *anyone* coming in off the street, raising some significant security questions in a village where anonymous tourists and visitors substantially outnumber the resident locals. On the other hand, the user interface spyware tracks behaviors, so that users are monitored and network attacks, from within, or other misuses and breaches might be detected after the fact. We have suggested access restrictions, eliminating what is now, essentially, total user privacy at the front end, to facilitate matters of security. (Thus far the library staff has responded by charging an access fee, using the funds to defray the costs of misuse.) By observing library user behaviors, we have begun to understand the complexities of the Semantic Web (Fass 2002, 2004). Aiming to facilitate users' access to information and services, the Semantic Web's security issues are compounded by service compositions and access, not just by human users, but also by software agents navigating the Web. The possibility of malicious or destructive activity, deliberately or due to inadvertent lapses in compositions of security protocols, is enormous. Some current relevant research pertaining to authorization, certification, privacy and security aspects of the Semantic Web is described in (Kagal *et al* 2004).

Involved with local governmental processes, we also have served as a county election officer at various times throughout the past decade. Thus we have familiarity with election codes and processes, and security concerns that existed even before today's proposals for voting electronically. Election tampering is always a threat to security of the homeland. Voting systems developed for potential use by our citizens, as discussed in (Neumann 2004), were suggested to make balloting easier for voters, and determination of results more accurate. But we know they raise numerous privacy and security issues, such as those described throughout (Neumann 2004) and by (Schmidt 2004) and (Cherry 2004). Like the library's universal access problems, these too involve matters of system integrity, perhaps spyware and Internet integrity, privacy and potential machine misuse. We support the ACM position on the matter (ACM 2004) and are pleased

that, at least in our state, the governor made provision of alternative paper ballots mandatory. (In our county of residence, we will now only use paper.) But even without the electronic aspects of voting considered by the researchers cited above, there are still areas where AI Technologies can aid in election security. The concoction of bogus voter identities and their "documentation", first reported locally by (Miller and Wilde 1998), can be countered by Data Mining techniques indicated in (Fass 1998) and, perhaps, by the more current use of record linkage and matching algorithms described by (Wang, Chen and Atabakhsh 2004) for detecting deceptive *criminal* identities. Here to, when warranted, security trumps privacy. We encourage human expert safeguards, such as auditing practices described in (Neumann 2004).

As a citizen just being a citizen, we have seen that AI Technologies have been protecting us in our everyday life. Adaptive User Interface research is assisting the development of communication systems used by first responders whose concern is information accuracy even more than speed. Such AI developments are described by (Sawyer *et al* 2004). We see their deployment as our local safety officers access the city network and interact *via* their laptops, cells and other devices that are state-of-the-art. We see that officers and emergency vehicles are geographically distributed throughout the village, and realize that planning and optimization of transportation networks, such as the Markov Process research described by (Hauskrecht 2004) has, most likely, been applied. We reap the benefits of robotics research for our security (Murphy 2004) when local bomb scares necessitate the deployment of Rescue Robots. This was first publicized in our area by (Guthrie 2003), but has now become so commonplace it hardly receives public notice.

Conclusions: Security Trumps Privacy

The many applications of AI Technologies described above have enhanced our security and that of our homeland. But as we have noted we believe security must take precedence over privacy when necessitated by the state of the world in which we live today.

As an example we review a security problem detected in our library some years ago when computer usage there was monitored more *actively* than it is now. As reported in (Brownfield 1999) a library staffer was watching a user behaving "furtively" while accessing a library terminal. She suspected the user was sending email which, in those days, was disabled on most library equipment due to "policy". Approaching the user, she could see his unusual behavior actually revealed his attempt to use library equipment for online purchase of a pellet gun. His privacy violated, the user fled. But by monitoring the system and tracking his hits, the library provided police with evidence indicating the user had attempted the purchase with a stolen credit card. The police identified the culprit and the gun company assured them that the sale would not go through. "Unusual behavior" cost the user his privacy, but our security was enhanced.

Determination of "unusual behavior" may reveal criminal or terrorist homeland threats, but we must know what is "usual" to distinguish such behavior from the rest. Human analysts and intelligence experts may make hypotheses about behavioral acts and patterns; AI Technologies may assist by sifting through data to discover persons and events to be "red tagged". Further investigation, by knowledgeable experts, can pursue potential problems once the AI system has applied the "red tag". Thus a satisfactory ratio between privacy and security may be achieved.

Acknowledgments

The Carmel Foundation provided technical support for the initial submittal of this paper. Helpful comments from the anonymous referees facilitated this final version.

References

ACM Statement on Voting Systems, 2004, *Comm. of the ACM* , Vol. 47, No. 10 (October 2004): 70.

Berry, N., Ko, T., Moy, T., Smrcka, J., Turnley, J. and B. Wu, 2004, "Emergent Clique Formation in Terrorist Recruitment", in *AAAI Workshop on Agent Organizations: Theory and Practice*, San Jose, CA, July 2004, AAAI Press, W04-02: 31-38.

Brownfield, M, 1999, "Librarian Stops Look-alike Gun Buy", *The Carmel Pine Cone*, Carmel CA, Vol. 85, No. 32 (August 6 -12, 1999): 1A ff.

Cherry, S., 2004, "The Perils of Polling", *IEEE Spectrum*, Vol. 41, No. 10 (October 2004): 34-40.

Fass, L.F., 1998, "Inductive Inference and Link Analysis", in (Jensen and Goldberg 1998): 35-37.

Fass, L.F., 2002, "Can We Improve Web Access in the Real World?", appears as Statement of Interest in *AAAI Workshop on Ontologies and the Semantic Web*, Edmonton AB, July 2002, AAAI Press WS02-11: xv-xvi.

Fass, L.F., 2004, "The 'Digital Divide' Just Isn't What It Used to Be", in *Proc. 26th International Conf. on Software Engineering, Workshop on Bridging the Gaps between Software Engineering and Human-Computer Interaction*, Edinburgh Scotland, May 2004, The IEE W1L: 83-87.

Goldberg, H.G. and T. E. Senator, "Restructuring Databases for Knowledge Discovery by Consolidation and Link Formation", in (Jensen and Goldberg 1998): 47-52.

Goldberg, H.G. and R.W.H. Wong, 1998, "Restructuring Transactional Data for Link Analysis in the FinCen AI System", in (Jensen and Goldberg 1998): 38-46.

Guthrie, J., 2003, "Carmel Hit by Bomb Hoax", *Monterey County Post*, Monterey County. CA, August 21, 2003: 1-2.

Hauskrecht, M., 2004, "Solving Factored MDPs with Continuous and Discrete Variables", Invited Talk, AAAI Workshop on Learning and Planning in Markov Processes--- Advances and Challenges, San Jose CA , July 27, 2004.

Jensen, D. and H.G. Goldberg (Editors),1998, *AAAI Fall Symposium on Artificial Intelligence & Link Analysis*, Orlando FL , October 1998, AAAI Press FS98-01.

Kagal, L., Finin,T, Paolucci, M., Srinivasan, N., Sycara, K and G. Denker, 2004, "Authorization and Privacy for Semantic Web Services", *IEEE Intell. Sys.*, Vol. 19, No. 4, (July/August 2004): 50-56.

Kingdon, J., 2004, "AI Fights Money-Laundering", in *IEEE Intell. Sys.*, Vol. 19, No. 3 (May/June 2004): 87-89.

Kogut, P., Yen, J., Leung, Y., Sun, S., Wang, R., Mielczarek, T., and B. Hellar, 2004, "Proactive Information Gathering for Homeland Security Teams", in (Yen, 2004): 48-50.

Lee, R. , 1998, "Automatic Information Extraction from Documents: a Tool for Intelligence and Law Enforcement Analysts", in (Jensen and Goldberg 1998): 63-67.

Miller, P., and K. Wilde, 1998, "Voter Fraud: Simple as 1-2-3", *The Carmel Pine Cone*, Carmel CA, Vol. 83, No. 15 (April 10-16, 1998): 1A ff.

Murphy, R. 2004, "Rescue Robotics for Homeland Security", in (Yen 2004): 66-68.

Neumann, P.G. (Editor), 2004, Special Section on the Problems and Potentials of Voting Systems, *Comm. of the ACM*, Vol. 47, No. 10 (October 2004): 28-70.

Picarelli, J.T., 1998, "Transnational Threat Indications and Warning: The Utility of Network Analysis", in (Jensen and Goldberg 1998): 88-93.

Popp, R., Armour, T., Senator, T. and K. Numrych, 2004, "Countering Terrorism through Information Technology", in (Yen 2004): 36-43.

Sawyer, S., Tapia, A., Pesheck, L. and J. Davenport, "Mobility and the First Responder", in (Yen 2004): 62-65.

Schmidt, P. 2004, "Wary of E-voting, Some Professors Sound the Alarm", *The Chronicle of Higher Education*, April 23, 2004: A18- A20.

Wang, G., Chen, H. and A. Atabakhsh, 2004, "Automatically Detecting Deceptive Criminal Identities" in *Comm. of the ACM*, Vol. 47, No. 3, (March 2004): 71-76.

Yen, J. (Editor), 2004, Special Section on Emerging Technologies for Homeland Security, *Comm. of the ACM*, Vol. 47, No. 3, (March 2004): 32-68.

Zdanowicz, J.S., 2004, "Detecting Money Laundering and Terrorist Financing via Data Mining", *Comm. of the ACM*, Vol. 47, No. 5, (May 2004): 53-55.