

COGNITIVE HACKING: TECHNOLOGICAL AND LEGAL ISSUES

George Cybenko, Annarita Giani, Carey Heckman, Paul Thompson
Dartmouth College
Hanover, NH 03755
US

{george.cybenko, annarita.giani, carey.heckman, paul.thompson}@dartmouth.edu

ABSTRACT

In this paper, we define a category of computer security exploits called "cognitive hacks." Loosely speaking, cognitive hacking refers to a computer or information system attack that relies on changing human users' perceptions and corresponding behaviors in order to be successful. This is in contrast to denial of service (DOS) and other kinds of well-known attacks that operate solely within the computer and network infrastructure. In this paper several cognitive hacking techniques are illustrated by example, legal issues related to cognitive hacking are discussed, and technologies for preventing and mitigating the effects of cognitive hacking attacks are proposed.

Ultimately each individual is responsible for his or her use of technology and for decisions taken based on information gathered from the web. The primary concern here is with misinformation that cannot be easily detected. Who is responsible for a large loss incurred resulting from misinformation posted on the Web? Is this simply a matter of "buyer beware," or can users be protected by technology or policy?

KEY WORDS

Cognitive Attacks, Competition, Information Technology, Internet, Stock Markets.

1. INTRODUCTION

Cognitive hacking refers to a computer or information system attack that relies on changing human users' perceptions and corresponding behaviors in order to be successful. This is in contrast to denial of service (DOS) and other kinds of well-known attacks that operate solely within the computer and network infrastructure. With cognitive attacks neither hardware nor software is necessarily corrupted. There may be no unauthorized access to the computer system or data. Rather the computer system is used to influence people's perceptions and behavior through misinformation. The traditional definition of security is protection of the computer system

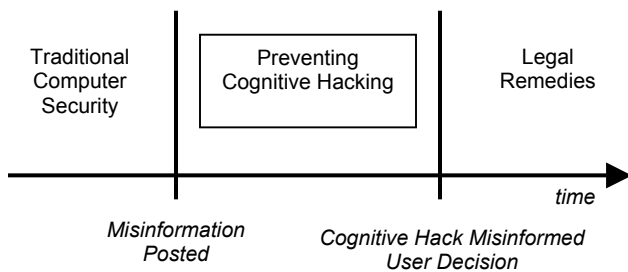
from three kinds of threats: unauthorized disclosure of information, unauthorized modification of information, and unauthorized withholding of information (denial of service). Cognitive attacks, which represent serious breaches of security with significant economic implications, are not well covered by this definition. Social engineering via a computer system, i.e., a hacker's psychological tricking of legitimate computer system users to gain information, e.g., passwords, in order to launch an autonomous attack on the system, is a special case of cognitive hacking.

In face to face interaction with other people, there is normally some context in which to evaluate information being conveyed. We associate certain reliability to information depending on who the speaker is and on what we know of the person. This type of evaluation cannot be transferred to the Web. Anyone can post anything on a Web page with very few limitations. The Internet's open nature makes it an ideal arena for dissemination of misinformation. The issue is how to deal with false information on the Web and how to decide whether a source is reliable. People use Web technology for personal and economic reasons, e.g., buying shares or finding a job. What happens if a user makes a decision based on information found on the Web that turns out to be misinformation?

Computer and network security present great challenges to our evolving information society and economy. The variety and complexity of cyber security attacks that have been developed parallel the variety and complexity of the information technologies that have been deployed, with no end in sight for either. We delineate between two classes of information systems attacks: *autonomous* attacks and *cognitive* attacks. Autonomous attacks operate totally within the fabric of the computing and networking infrastructures. For example, files containing private information such as credit card numbers can be downloaded and used by an attacker. Such an attack does not require any intervention by users of the attacked system, hence we call it an "autonomous" attack. By contrast, a *cognitive* attack requires some change in users'

behavior, affected by manipulating their perception of reality. The attack's desired outcome cannot be achieved unless human users change their behaviors in some way. Users' modified actions are a critical link in a cognitive attack's sequencing.

Consider the graph below. Most analyses of computer security focus on the time before misinformation is posted, i.e., on preventing unauthorized use of the system. A cognitive hack takes place when a user's behavior is influenced by misinformation. At that point the focus is on detecting that a cognitive hack has occurred and on possible legal action. Our concern is with developing tools to prevent cognitive hacking, that is, tools that can recognize and respond to misinformation before a user acts based on the misinformation.



As discussed in section 4, legal perspectives related to cognitive hacking, as is the case with many areas of Internet law, are still evolving. The purposes of this paper are: a) to define cognitive hacking, b) to bring up related legal issues, c) to present a few example instances, and d) to propose counter-measures. As discussed in section 2, most research in computer security has not focused on cognitive attacks. In our earlier work we have presented economic [1] and general security aspects of this new model [2]. The main contribution of this paper is a consideration of the legal issues related to cognitive hacking.

2. DEFINITION OF COGNITIVE HACKING

Cognitive hacking is defined in this paper as gaining access to, or breaking into, a computer information system for the purpose of modifying certain behaviors of a human user in a way that violates the integrity of the overall user-information system.

A definition of semantic attacks closely related to our discussion of cognitive hacking has been described by Schneier [3], who attributes the earliest conceptualization of computer system attacks as physical, syntactic, and semantic to Martin Libicki, who describes semantic attacks in terms of misinformation being inserted into interactions among intelligent agents on the Internet [4]. Schneier, by contrast, characterizes semantic attacks as "... attacks that target the way we, as humans, assign

meaning to content." He goes on to note, "Semantic attacks directly target the human/computer interface, the most insecure interface on the Internet" [3].

Denning's discussion of information warfare [5] overlaps our concept of cognitive hacking. Denning describes information warfare as a struggle over an information resource by an offensive and a defensive player. The resource has an exchange and an operational value. The value of the resource to each player can differ depending on factors related to each player's circumstances. The outcomes of offensive information warfare are: increased availability of the resource to the offense, decreased availability to the defense, and decreased integrity of the resource. Applied to the Emulex example, described below, Jakob is the offensive player and Internet Wire and the other newswire services are the defensive players. The outcome is decreased integrity of the newswires' content. From the perspective of cognitive hacking, while the above analysis would still hold, the main victims of the cognitive hacking would be the investors who were misled. In addition to the decreased integrity of the information, an additional outcome would be the money the investors lost.

3. EXAMPLES

Emulex

Mark S. Jakob, after having sold 3,000 shares of Emulex Corporation in a "short sale" at prices of \$72 and \$92, realized that, since the price rose to \$100, he lost almost \$100,000. This kind of speculation is realized by borrowing shares from a broker and selling them in hope that the price will fall. Once this happens, the shares are purchased back and the stock is returned to the broker with the short seller keeping the difference.

On August 25th 2000, when he realized the loss, he decided to do something against the company. The easiest and most effective action was to send a false press release to Internet Wire Inc. with the goal of influencing the stock price. He claimed that Emulex Corporation was being investigated by the Security and Exchange Commission (SEC) and that the company was forced to restate 1998 and 1999 earnings. The story quickly spread, and half an hour later other news services such as Dow Jones, Bloomberg and CBS Marketwatch picked up the hoax. Due to this false information, in a few hours Emulex Corporation lost over \$2 billion dollars. After sending misinformation about the company, Jakob executed trades so that he earned \$236,000. Jakob was arrested and charged with disseminating a false press release and with security fraud. He is subject to a maximum of 25 years in prison, a maximum fine of \$220 million, two times investor losses, and an order of restitution up to \$110 million to the victims of his action [6].

Jonathan Lebed

A 15 years old student using only AOL accounts with several fictitious names was able to change the behavior of many people around the world making them act to his advantage. In six months he gained between \$12,000 and \$74,000 daily each time he posted his messages and, according to the US Security Exchange Commission, he did that 11 times increasing the daily trading volume from 60,000 shares to more than a million.

He sent this kind of message after having bought a block of stocks. The purpose was to influence people and let them behave to pump up the price by recommending the stock. The messages looked credible and people did not even think to investigate the source of the messages before making decisions about their money. Jonathan gained \$800,000 in six months. Initially the SEC forced him to give up everything, but he fought the ruling and was able to keep part of what he gained. The question is whether he did something wrong, in which case the SEC should have kept everything. The fact that the SEC allowed Jonathan to keep a certain amount of money shows that it is not clear whether or not the teenager is guilty from a legal perspective. Certainly, he made people believe that the same message was post by 200 different people.

Richard Walker, the SEC's director of enforcement, referring to similar cases, stated that on the Internet there is no clearly defined border between reliable and unreliable information, investors must exercise extreme caution when they receive investment pitches online [7].

NEI Webworld

In November 1999 two UCLA graduates students and one of their associates purchased almost all of the shares of the bankrupt company NEI Webworld at a price ranging from 0.05 to 0.17 per share. They opened many Internet message board accounts using a computer at the UCLA BioMedical Library and posted more than 500 messages on hot web sites to pump up the stock of the company, stating false information about the company with the purpose of convincing others to buy stock in the company. They claimed that the company was being taken over and that the target price per share was between 5 and 10 dollars. Using other accounts they also pretended to be an imaginary third party, a wireless telecommunications company, interested in acquiring NEI Webworld. What the three men did not post was the fact that NEI was bankrupt and had liquidated assets in May 1999. The stock price rose from \$0.13 to \$15 in less than one day, and they realized about \$364,000 in profits. The men were accused of selling their shares incrementally, setting target prices along the way as the stock rose. On one day the stock opened at \$8 and soared to \$15 5/16 a share by 9:45 a.m. ET and by 10:14 a.m. ET, when the

men no longer had any shares, the stock was worth a mere 25 cents a share.

On Wednesday, December 15, 1999, the U.S. Securities and Exchange Commission (SEC) and the United States Attorney for the Central District of California charged the three men with manipulating the price of NEI Webworld, Inc. In late January 2001, two of them, agreed to gave up their illegal trading profits (approximately \$211,000). The Commission also filed a new action naming a fourth individual, as participating in the NEI Webworld and other Internet manipulations. Two of the men were sentenced on January 22, 2001 to 15 months incarceration and 10 months in a community corrections center. In addition to the incarcerations, Judge Feess ordered the men to pay restitution of between \$566,000 and \$724,000. The judge was to hold a hearing on Feb. 26 to set a specific figure. Anyone with access to a computer can use as many screen names as desired to spread rumors in an effort to pump up stock prices by posting false information about a particular company so that they can dump their own shares and give the impression that their own action has been above board [8].

Britney Spears

On 7 October 2001, the day that the military campaign against Afghanistan began, the top-ranked news story on CNN's most popular list was a hoax, "Singer Britney Spears Killed in Car Accident" [9]. Allegedly this hoax was started by a researcher who sent a specially crafted URL, beginning with the characters <http://www.cnn.com> followed by "@" and the IP address of his Web site, to three users of AOL's Instant Messenger chat software. Web browsers ignore the characters to the left of "@," so clicking on this url led users to the spoofed article. Then, due to a bug in CNN's software, when people at the spoofed site clicked on the "E-mail This" link, the real CNN system distributed a real CNN e-mail to recipients with a link to the spoofed page. At the same time with each click on "E-mail This" at the bogus site, the real site's tally of most popular stories was incremented for the bogus story. Within 12 hours more than 150,000 people had viewed the spoofed page.

PayPal.com

"We regret to inform you that your username and password have been lost in our database. To help resolve this matter, we request that you supply your login information at the following website."

Many customers of PayPal received this kind of email and subsequently gave personal information about their PayPal account to the site linked by the message (<http://paypalsecure.com> not <http://www.paypal.com>) [10]. The alleged perpetrators apparently used their access to PayPal accounts in order to purchase items on eBay.

4. LEGAL ISSUES RELATED TO COGNITIVE HACKING

If cognitive hacking challenges security experts because it aims at the vulnerable human/computer interface, it challenges legal experts because it both targets and exploits information, the very lifeblood of free speech and democracy. Criminal prosecution and civil lawsuits may help combat cognitive hacking, but this will be possible only in compliance with free speech protection. Laws already exist that can fight disinformation without violating fundamental rights. But cognitive hacking introduces new characteristics requiring revised legal doctrines. Ultimately, confronting cognitive hacking will require integrating legal and technological anti-hacking tools.

Within the United States, where the U.S. Constitution prevails, legal action seeking to regulate cognitive hacking can conflict with First Amendment free speech protection. The First Amendment prohibits government punishment of “false” ideas or opinions. The competition of ideas, not legislatures or courts, determines what ideas and opinions society accepts. And while false *facts* lack constitutional protection, the U.S. Supreme Court has ruled that the news media as well as non-news media discussion of public issues or persons require some margin of factual error to prevent chilling legitimate debate. “The First Amendment requires that we protect some falsehood in order to protect speech that matters.” [11]

Punishing web defacement should present no First Amendment concerns. As with graffiti in the physical world [12], the First Amendment does not shield unauthorized damage to property of others. Distribution of false information with an intent to defraud or manipulate should also require little First Amendment consideration.

However, a regulatory measure aimed at the content of the cognitive hacking, on what the hacking *says*, would likely fail constitutionally unless the state interest were compelling and no content-neutral alternative were available. Attempts within the United States to stop a web site or metatags or list server postings from expressing unpopular views would also struggle to pass First Amendment muster [13].

Indeed, many legal avenues already exist for attacking cognitive hacking consistent with First Amendment rights.

Some forms of cognitive hacking are tightly coupled with conduct that has legal consequences. Web defacement requires breaking into another’s web site, and therefore could be characterized as vandalism, destruction of property, trespassing, or, under the right circumstances, a

violation of the Electronic Communications Privacy Act of 1986. As described above, manipulating securities markets through cognitive hacking can trigger prosecution under the securities laws. If unauthorized use of a software robot to harvest information from another’s web site can be trespassing [14], perhaps so is feeding false data into another’s software robot that is harvesting web information.

Other forms of cognitive hacking involve incendiary or factually false statements beyond First Amendment protection. Disseminating false information to secure an agreement could be the basis of legal actions for fraud or misrepresentation. Disseminating false information that damages the reputation of a person, business, or product could lead to a libel, defamation, or commercial disparagement suit. Incorporating trademarks of others as metatags that mislead consumers about the origin of goods or services or reduce the goodwill associated with a mark could be reached through the legal remedies provided by trademark and trademark antidilution statutes.

The special persuasive powers of computer output create an extra dimension of legal concern. Humans are quick to believe what they read and see on their computer screen. Even today, it is common to hear someone say a fact must be true because they read it on the web. A web site’s anthropomorphic software agent is likely to enjoy greater credibility than a human, yet no conscience will prevent an anthropomorphic agent from saying whatever it has been programmed to say [15]. Cognitive hackers may therefore require new legal doctrines because their mechanisms apparently bypass normal human critical thinking.

Still more elusive will be identifying and taking meaningful legal action against the perpetrator. The speed and lack of human intervention that is typically associated with cognitive hacking, combined with the lack of definitive identification information generally inherent in the Internet’s present architecture, complicate legal proof of who is the correct culprit. Privacy protection makes the task more difficult. Even if identified, the individual or entity may disappear or lack the assets to pay fines or damages.

Attention may therefore focus instead on third-party intermediaries, such as Internet service providers, web sites, search engines, and so forth, just as it has for Internet libel, copyright infringement, and pornography. Intermediaries are likely to have greater visibility and more assets, making legal action easier and more productive. A cognitive hacking victim might contend that an intermediary or the producer of web-related software failed to take reasonable measures to defend against cognitive hacking. An intermediary’s legal responsibility will grow as the technological means for blocking cognitive hacking become more effective and

affordable. Rapid technological advances with respect to anti-hacking tools would empower raising the bar for what is considered reasonable care.

The actual application of the law to cognitive hacking is still in formation. It is to be expected that case law with respect to cognitive hacking will continue to evolve over the coming years. Enactment of specific legislation is also possible.

5. COGNITIVE HACKING COUNTERMEASURES

Given the wide variety of cognitive hacking approaches, *preventing* cognitive hacking reduces either to preventing unauthorized access to information assets (such as in web defacements) in the first place or detecting posted misinformation before user behavior is affected (that is, before behavior is changed but possibly after the misinformation has been disseminated). The latter may not involve unauthorized access to information, as for instance in "pump and dump" schemes that use newsgroups and chat rooms. By definition, *detecting* a successful cognitive hack would involve detecting that the user behavior has already been changed. We are not considering detection in that sense at this time.

Our discussion of methods for preventing cognitive hacking will be restricted to approaches that could automatically alert users of problems with their information source or sources (information on a web page, newsgroup, chat room and so on). Techniques for preventing unauthorized access to information assets fall under the general category of computer and network security and will not be considered here. Similarly, detecting that users have already modified their behaviors as a result of the misinformation, namely that a cognitive hack has been successful, can be reduced to detecting misinformation and correlating it with user behavior.

5.1 SINGLE SOURCE COGNITIVE HACKING

In this section, we develop a few possible approaches for the single source problem. By single source, we mean situations in which redundant, independent sources of information about the same topic are not available. An authoritative corporate personnel database would be an example.

5.1.1 AUTHENTICATION AND TRUST RATINGS OF SOURCE

This technique involves due diligence in authenticating the information source and ascertaining its reliability. Various relatively mature certification and Public Key Infrastructures technologies can be used to detect

spoofing of an information server. Additionally, reliability metrics can be established for an information server or service by scoring its accuracy over repeated trials and different users. In this spirit, Lynch [16] describes a framework in which trust can be established on an individual user basis based on both the identity of a source of information, through PKI techniques for example, and in the behavior of the source, such as could be determined through rating systems. Such an approach will take time and social or corporate consensus to evolve.

5.1.2 INFORMATION "TRAJECTORY" MODELING

This approach requires building a model of a source based on statistical, historical data or some sort of analytic understanding of how the information relates to the real world. For example, weather data coming from a single source (website or environmental sensor) could be calibrated against historical database (from previous years) or predictive model (extrapolating from previous measurements). A large deviation would give reason for hesitation before committing to a behavior or response. Modeling information sources is something that can be done on a case-by-case basis as determined by the availability of historical data and the suitability of analytic modeling.

5.1.3 ULAM GAMES

Stanislaw Ulam in his autobiography "*Adventure of a Mathematician*" posed a problem that can be understood in terms of the "20 Questions" game. In playing such a game, some number of answers can be incorrect. What is the questioner's optimal strategy for asking questions knowing that some answers will be lies? Of course, if an unbounded number of lies are allowed, no finite number of questions can determine the truth. On the other hand, if say k lies are allowed, each binary search question can be repeatedly asked $2k + 1$ times which is easily seen to be extremely inefficient. Several researchers have investigated this problem, using ideas from error-correcting codes and other areas [17].

We suspect that this kind of model and solution approach may not be useful in dealing with the kinds of cognitive hacking we have documented, although it will clearly be useful in cognitive hacking applications that involve a sequence of interactions between a user and an information service, as in a negotiation or multi-stage handshake protocol.

5.2 MULTIPLE SOURCE COGNITIVE HACKING

In this section, we discuss possible approaches to preventing cognitive hacking when multiple, presumably redundant, sources of information are available about the same subject of interest. This is clearly the case with financial, political, and other types of current event news coverage. Automated software tools could in principle help people make decisions about the veracity of information they obtain from multiple networked information systems. A discussion of such tools, which could operate at high speeds compared with human analysis, follows.

5.2.1 SOURCE RELIABILITY VIA COLLABORATIVE FILTERING AND RELIABILITY REPORTING

The problem of detecting misinformation on the Internet is much like that of detecting other forms of misinformation, for example in newsprint or verbal discussion. Reliability, redundancy, pedigree, and authenticity of the information being considered are key indicators of the overall "trustworthiness" of the information. The technologies of collaborative filtering and reputation reporting mechanisms have been receiving more attention recently, especially in the area of on-line retail sales [18]. This is commonly used by the many on-line price comparison services to inform potential customers about vendor reliability. The reliability rating is computed from customer reports.

5.2.2 BYZANTINE GENERALS MODELS

Byzantine General's Problem models a group of generals plotting a coup. Some generals are reliable and intend to go through with the conspiracy while others are feigning support and in fact will support the incumbent ruler when the action starts. The problem is to determine which generals are reliable and which are not. Just as with the Ulam game model for a single information source, this model assumes a sequence of interactions according to a protocol, something that is not presently applicable to the cognitive hacking examples we have considered, although this model is clearly relevant to the more sophisticated information sources that might arise in the future.

5.2.3 DETECTION OF COLLUSION BY INFORMATION SOURCES

Collusion between multiple information sources can take several forms. In pump and dump schemes, a group may hatch a scheme and agree to post misleading stories on several websites and newsgroups. In this case, several people are posting information that will have common

facts or opinions, typically in contradiction to the consensus.

Automated tools for preventing this form of cognitive hack would require natural language processing to extract the meaning of the various available information sources and then compare their statistical distributions in some way. For example, in stock market discussion groups, a tool would try to estimate the "position" of a poster, from "strong buy" to "strong sell" and a variety of gradations in between. Some sort of averaging or weighting could be applied to the various positions to determine a "mean" or expected value, flagging large deviations from that expected value as suspicious.

Similarly, the tool could look for tightly clustered groups of messages, which would suggest some form of collusion. Such a group might be posted by the one person or by a group in collusion, having agreed to the form of a cognitive hack beforehand.

Interestingly, there are many statistical tests for detecting outliers but much less is known about detecting collusion which may not be manifest in outliers but unlikely clusters that may not be outliers at all. For example, if too many eyewitnesses agree to very specific details of a suspect's appearance (height, weight, and so on), this might suggest collusion to an investigator. For some interesting technology dealing with corporate insider threats due to collusion, see [19].

5.2.4 LINGUISTIC ANALYSIS

Stylistic techniques from linguistic are also potential tools for determining the likelihood of authenticity of multiple documents being analyzed. Suppose we are given a set of documents authored by one or more people hiding themselves under possibly multiple pseudonyms. It would be desirable to group the documents according to the real author; that is, to partition the documents into subsets of papers all belonging to the same author.

The main idea is to embed the given document into a finite dimensional linear feature space of stylistic language usage with some notion of stylistic distance in that space. By performing cluster and other types of analyses on the writing and linguistic style of the whole document or sections thereof, it might be possible to establish which sections of documents are stylistically similar and so, presumably, authored by the same writer.

This kind of detection cannot be applied to short messages, but for a consistent length and enough words, it could determine, with high confidence the stylistic characteristic of the author, or source.

6. CONCLUSION

Cognitive hacking represents a new kind of threat. It requires new kinds of tools to prevent it and a deep understanding of the problem to be able to identify how the law should be applied to these activities. Meeting the technical and legal challenges presented by cognitive hacking will require a multidisciplinary approach.

7. ACKNOWLEDGEMENT

Support for this research came from the Department of Defense Critical Infrastructure Protection Fellowship grant with the Air Force Office of Scientific Research, F49620-01-1-0272; Defense Advanced Research Projects Agency projects F30602-00-2-0585 and F30602-98-2-0107; and the Office of Justice Programs, National Institute of Justice, Department of Justice award 2000-DT-CX-K001 (S-1).

The views in this document are those of the authors and do not necessarily represent the official position of the sponsoring agencies or of the U.S. Government.

REFERENCES

- [1] G. Cybenko, A. Giani, & P. Thompson, Cognitive Hacking and the Value of Information *Workshop on Economics and Information Security*, May 16-17, 2002, Berkeley, California.
- [2] G. Cybenko, A. Giani, & P. Thompson, Cognitive Hacking: A Battle for the Mind *IEEE Computer*, 35(8), 2002, 50-56.
- [3] B. Schneier, Semantic attacks: The third wave of network attacks *Crypto-gram Newsletter* October 15, 2000. <http://www.counterpane.com/crypto-gram-0010.htm>.
- [4] M. Libicki, *The mesh and the Net: Speculations on armed conflict in an age of free silicon* National Defense University McNair Paper 28, 1994. <http://www.ndu.edu/inss/macnair/mcnair28/m028cont.html>
- [5] D. Denning, *Information warfare and security* (Reading, Mass.: Addison-Wesley, 1999).
- [6] B. Mann, Emulex fraud hurts all *The Motley Fool*, 2000. <http://www.fool.com/news/foolplate/2000/foolplate000828.htm>
- [7] M. Lewis, Jonathan Lebed: Stock Manipulator, S.E.C. Nemesis – and 15 *New York Times Magazine* 25 February 2001.
- [8] A.K. Smith, Trading in False Tips Exacts a Price, *U.S. News & World Report*, February 5, 2001, p.40
- [9] Pop singer's death a hoax a top story at CNN Newsbytes, 2001. <http://www.newsbytes.com/cgi-bin/udt/im.display.printable?client.id=newsbytes&story.id=170973>
- [10] B. Krebs, E-Mail Scam Sought To Defraud PayPal Customers *Newsbytes* 19 December 2001, <http://www.newsbytes.com/news/01/173120.html>
- [11] Gertz v. Robert Welch, Inc., 428 U.S. 323, 94 S.Ct. 2997, 41 L.Ed.2d 789 (1974).
- [12] See, e.g., New York v. Vinolas, 667 N.Y.S.2d 198 (N.Y. Crim. Ct. 1997).
- [13] See R.A.V. v. City of St. Paul, 505 U.S. 377, 112 S.Ct. 2538, 120 L.Ed.2d 305 (1992)
- [14] Ebay Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal., 2000)
- [15] C. Heckman & J. Wobbrock Put Your Best Face Forward: Anthropomorphic Agents, E-Commerce Consumers, and the Law, *Fourth International Conference on Autonomous Agents*, June 3-7, Barcelona, Spain, 2000.
- [16] C. Lynch, When Documents Deceive: Trust and Provenance as New Factors for Information Retrieval in a Tangled Web, *Journal of the American Society for Information Science & Technology*, 52(1), 2001, 12-17.
- [17] D. Mundici & A. Trombetta, 1997. Optimal Comparison Strategies in Ulam's Searching Game with Two Errors, *Theoretical Computer Science*, 182(1-2) 1997, 217-232.
- [18] C. Dellarocas, Building trust on-line: The design of reliable reputation reporting mechanisms for online trading communities *Center for eBusiness@MIT* paper 101.
- [19] 3D Corporation, see <http://www.the3dcorp.com/ddd/index2.html>.