UIC John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 4 *Journal of Computer & Information Law - Symposium*

Article 2

2008

Convergence at the Boundaries of Information Analysis and Security Technology, 25 J. Marshall J. Computer & Info. L. 599 (2008)

Charisse Castagnoli

CONVERGENCE AT THE BOUNDARIES OF INFORMATION ANALYSIS AND SECURITY TECHNOLOGY

CHARISSE CASTAGNOLI*

I have a background in engineering and thus this talk is predominantly from the technology perspective about how seemingly ordinary changes in technology can have far reaching unintended consequences. I will start with the little disagreement Google had with CNET in about 2005.

CNET is an Internet site focused on technology, thus when Google first came out with its search technology there were some concerns about data privacy. CNET decided to experiment and see what kind of information they could find using Google. They used Google and only Google to look for personally identifiable information about Google's CEO Eric Schmidt. CNET then proceeded to publish their findings in their newspaper and on the Internet. Google was extremely upset about the publication and put a moratorium on meetings with CNET for a year. This story illustrates the point we all have to be concerned with, where and how our information is stored and can it be made available. Think back ten years to medical practitioners, when information only existed in physical form. Information was on a piece of paper, on a film, and maybe with samples in a lab. Today all the information in your doctor's office or the social security office is now entirely digital. Every time someone needs to view or forward that information a permanent exact copy is made.

We also have the GPEA Act ("Government Paperwork Elimination Act") from the Clinton administration. This Act requires government agencies with more than fifty thousand transactions a month to migrate

* Charisse Castagnoli is an independent security consultant and lecturer and an adjunct professor of law at The John Marshall Law School. She has over 15 years of experience in the information technology industry, including 18 years in security product development, marketing and business development. She teaches Information Security and U.S. Policy at John Marshall. She had a J.D. from the University of Texas at Austin and a degree in computer science from the University of California-Berkeley.

to electronic forms of communication with their constituents and to provide and maintain all of the agency's records electronically. This covers most government agencies.

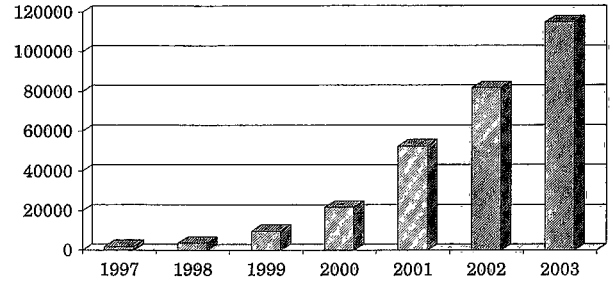
It used to be when you turned sixty-five you would march down to the Social Security Office, talk to a person, register on paper, and soon you would receive your social security checks. Now you perform the same process, but online, over the Web, or from a computer. When you move from a paper process to an electronic process, you not only provide information you intended to provide, but you also include ancillary information that is provided automatically. This information is provided without your consent or knowledge. By way of comparison, when you fill out a piece of paper, the only information that is transferred is what you write down. When you connect over the Internet, there is ancillary information such as: what is your browser, information that is stored and retrieved via cookies, information about where you are connecting from, what type of computer and operating system you are using, etc. This ancillary information is collected as a by-product of that conversation with the government agency and stored on servers in logs and databases. While most organizations do not do anything intentionally or maliciously with this type of information, sometimes changes happen as a natural consequence of evolution of technology and very serious security and privacy consequences. Keep this in mind as in the discussion of some examples and think about how you can be more careful with your own digital information.

First, a little background about the state of computer security, as provided by an organization called Computer Emergency Response Team ("CERT"). CERT was formed after Robert Tappan Morris launched the first Internet worm in 1986. For years and years CERT has tracked how many vulnerabilities are discovered and how many attacks were occurring. A vulnerability is an opportunity to create an attack, not an attack itself. The more vulnerabilities there are, the greater the opportunity for attacks which can be created and launched. The numbers of attacks today are actually increasing at an astonishing rate and I will discuss why that is happening. Actually, it became so onerous to try to keep track of the number of attacks that CERT, threw up their hands and said forget it; it is too difficult, we are not going to keep track of this information anymore.

Fortunately, other organizations have decided that this is interesting information which we should keep track of, and those organizations, including Microsoft, publish attack trends. Microsoft reports on information gathered from their own networks and their malicious software removal tool. They keep track of the types of vulnerabilities they see and, more importantly, the severity. While Microsoft sees the number of

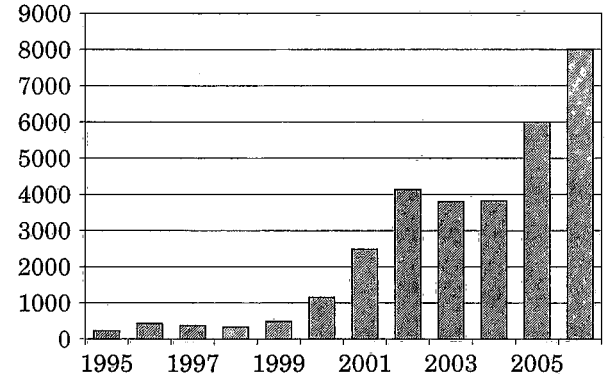
FIGURE 1.

Automation is increasing – resulting in higher incident rate



Source: CERT

FIGURE 2. ATTACK TRENDS



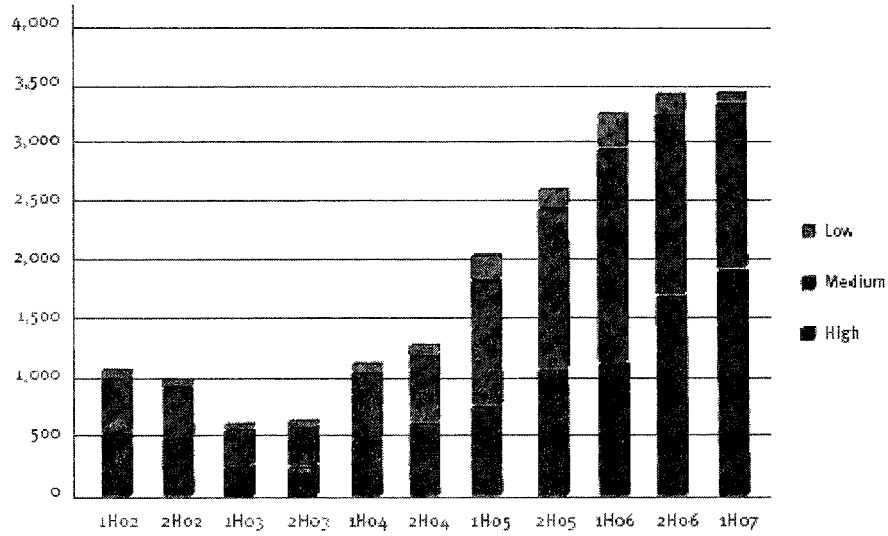
unique vulnerabilities declining, the severity of the new vulnerabilities is increasing.

Another important trend is that more and more attacks are coming in through the application layer. Today, attacks can compromise your desktop through the browser just by surfing a website, by entering data into a form, or even through reading a PDF.[1] As attacks have increased, so has the availability of countermeasures, mostly security programs.

How many people have a firewall in their home? How many people have a firewall in their laptop? If you're running XP or Vista you have a built-in firewall. Most consumer security packages also include a firewall. When I began working in computer security in 1988 nobody knew what a firewall was. Even when they first came out in the early 1990's, nobody knew how to use them. Now you can be driving along interstate 80 listening to the trucker CB channels and they are talking about what you need for anti-virus protection on mobile devices. We really have come

1. Adobe Critical Advisors, Security Bulletin, http://www.adobe.com/support/security/bulletins/apsb08-15.html (last visited Nov. 19, 2008).

FIGURE 3. VULNERABILITIES REPORTED



to the point where security technology is pervasive. Vulnerabilities are increasing and attacks and their severity are still increasing.

One reason for this increase in threats is the technology available for hacking is increasing in sophistication and ease of use. Back in the 1980's, hacking was limited to password guessing. Now a simple Yahoo search will lead to readily available hacking tools that most computer users can effectively operate. One of the latest hacking tools is something called a keyboard loggers. Criminals install them to steal account information. Wives and husbands install them to spy on their partner, and parents install them to keep track of their children. There is a debate about the legality of some hacker tools. On the one hand, the Digital Millennium Copyright Act ("DMCA") provides, "No person shall circumvent a technological measure that effectively controls access to a work protected under this title."[2]

So, if a housewife can download something over the Internet and log all the information about what her husband is doing or the other way around, then technology has advanced to the point where anybody can be a hacker. Unfortunately, those of us who want to protect ourselves from the hackers are in an arms race in which even security vendors who repel hacks for a living cannot keep up. A sad but true fact: if you take an un-patched Windows XP computer (the way you get it out of the box) and you connect it to the Internet it will be compromised within four minutes.[3] There are organizations constantly scanning the Internet looking

2. 17 USC §1201 (A)(1)(a) (2006).

3. Internet Storm Center, *Survival Time on the Internet,* http://isc.sans.org/diary.html?storyid=4721 (last visited Nov. 18, 2008).

for those systems because they want to use them to promulgate further organized attacks such as SPAM and Denial of Service attacks.

Aside from third-party security control software, patching is the main vendor remedy. Everybody should be aware of the little notices from Microsoft Windows saying, "Here's an update for you, download it and trust us it will make you safer." Patching is a reactive approach. In computer security, the reactive approach is never as good as being proactive. Reactive solutions do not scale and are expensive. The estimated cost for a midsize organization of keeping up with their patches is exceeding $250,000 a year. That is a lot of money for a remedy which is unwarranted, and not verified for your particular environment. To put it in perspective, every 99-cent cigar lighter you buy at the grocery store is certified. However, we run hospital medical devices on an operating system which is not even "warranted for a particular purpose". Unfortunately, when computer science began as a discipline, computers were large disconnected devices; no one worried about computer security. It was not until twenty years later that universities started to teach computer security principles. Thus, most programmers do not understand the tools and techniques to make programs secure. The other problem is that most programs are not designed with security and privacy in mind. They are built to do a job, to perform an application, to execute a function. They are not necessarily built to protect the information or the application from malicious attacks.

Finally, users of technology demand low cost, high performance and convenience over security and privacy. Do you have use a free e-mail account, like a Yahoo, Gmail, or Hotmail? Have you ever read the data privacy terms and conditions? These vendors do not promise to protect your data on their servers from eavesdropping, or misappropriation, or infection. Yet, for only ten dollars per year, you can have a personal domain name and an e-mail account, which is private and not subject to scans designed to generate targeted advertising. We voluntarily give up information everyday for convenience or for meager cost savings, and we do not think about the long term consequences. What decision would we make about disclosing information if we really thought through the fact that *any* information put on the Internet is going to be generally available forever?

In the 1970's a disk drive was about the size of a podium, it had ten megabytes on it, and it cost ten million dollars. Now everybody probably has at least three devices with them that have more than 256 megabytes of data on them. Your cell phone, your PDA, your MP3 player, and your laptop all have vast amounts of storage available to them. Effectively today, storage space is free and whether you blog, surf the Web, e-mail, RSS, chat, or text. One consequence of free storage is all of that information can now be permanently stored. When you combine nearly free stor-

age with advanced search capabilities, anything you ever typed, spoke or posted can be found years later.

Not only do we fail to consider where voluntary information may end up, we also do not think carefully about what these changes in technologies can do to our ancillary information or to the security of our data. A recent example of un-anticipated loss of data occurred when a laptop owned by the Veterans Administration ("VA") containing millions of personally identifiable records was misplaced. Ten years ago this would have never happened because all data resided on a mainframe and mainframes do not usually go home with us at the end of the day. But laptops do, and they are small and can be lost. In fact, in Chicago between October of 2004 and February of 2006, 4,700 laptops were left in taxicabs. The VA program office that made the decision to purchase laptops for the personnel probably never considered that any information would be at risk. The program office did not follow the data as applications and processes changed from a monolithic database on a mainframe, to ubiquitous access over the Web, and unlimited copying to local systems like laptop hard drives or intermediate systems like email servers. They did not follow the data usage, they did not think about security and privacy control policies for the data, and they certainly did not consider the risk or cost associated with loss of the data. Now there is a lawsuit pending against the VA alleging violations of the Federal Fair Information Practices Act.[4] Given that statutory damages that are available, the laptop purchase could turn out to be costly for taxpayers. Ironically, there are very good data privacy tools that cost less than twenty dollars per seat which would have prevented disclosure due to accidental loss of the data. The VA has now purchased such a tool, but the Government Accounting Office, recently reported that up to seventy percent of government agencies have yet to deploy similar technology.[5]

In addition to risks to our information created by unintended changes in technology, there are those who use technology maliciously to cause emotional or physical harm. If you don't believe a hacker can cause physical harm, the first such incident was reported in May of 2008,[6] when hackers of an epilepsy information site caused migraines and near seizures. Additionally, more and more medical devices now have external controls which can be manipulated through computers remotely. Hopefully those protocols will be upgraded with security before someone is hurt.

---

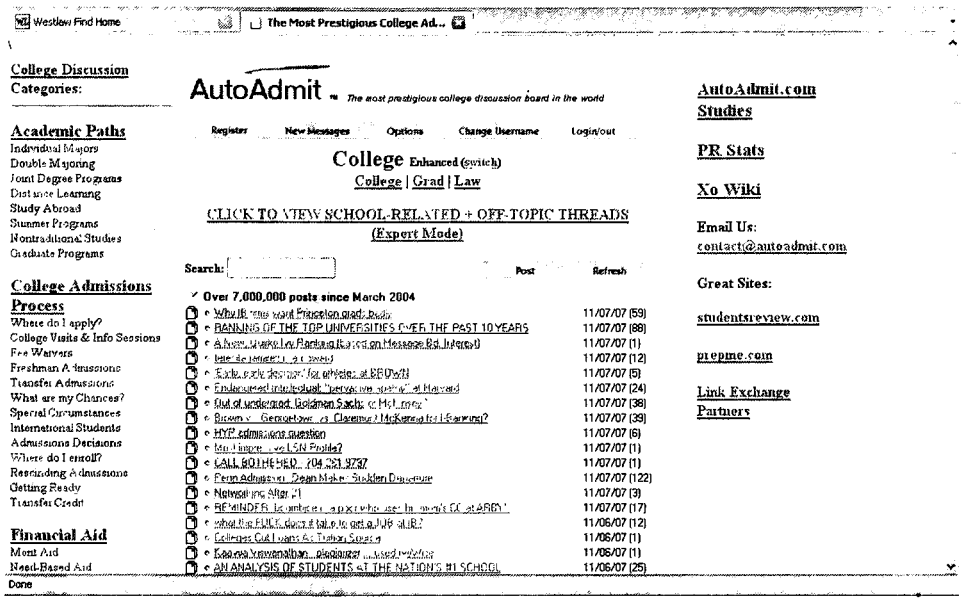
4. In re Dep't of Veteran Affairs Data Theft Litig., 461 F.Supp.2d 1367 (J.P.M.L. 2006).

5. Security Focus, *Federal Agencies Slow to Deploy Crypto*, http://www.securityfocus.com/brief/784 (last visited Nov. 18, 2008).

6. Health 24, *Hackers Incite Epilepsy Seizures*, http://www.health24.com/news/Epilepsy/1-907,46337.asp (last visited Nov. 19, 2008).

On the emotional side, the Internet now makes the high school bathroom stall available to the entire world. I am referring to the practice of cyberbullying. By way of example we're going to talk a little bit about the technology behind the AutoAdmit case. I can't reveal any specifics, but we can talk about the process of computer forensics and how anonymity on the net empowers cyberbullying. If you are not familiar with the case, let's start with the home page of the website where it all began, www.autoadmit.com.

FIGURE 4.



The story begins with an anonymous poster who obtained a private picture of the target, likely from a social networking site.

On a side note, why on earth do we think something on a social networking site is private? There's a little check box up there that says that only your friends can see your stuff, but what about your friends or their friends? Nothing prevents someone from making a copy and passing it on. Furthermore, does anyone really think a determined hacker cannot get onto most websites and extract anything they really want from it? For information you voluntarily post, do not rely and depend on the website to permanently protect the privacy of your information. Try to educate everyone, your family, colleagues, and friends to carefully consider what they post on their MySpace, Facebook or any social networking sites. It's not private, it will be there forever, and anyone determined enough can search and find it.

Back to Autoadmit: a young woman posted her picture on a site for her friends, and some miscreant gets a copy of it. This person then posts

her picture and starts a derogatory, inflammatory, disgusting thread. If this had happened in the past about twenty years ago, it would have been in a locker room, in a bathroom, at a party, but face-to-face where most people knew each other. Eventually, someone would have confronted the malicious person and that would have been the end of the story. However, this conversation was posted on the Internet so anybody could see it, anybody could join in, and no one necessarily knew each other. Unfortunately, the postings specifically identified the individuals who were the targets, yet the posters were using technology to remain anonymous. It is an unintended consequence of technology adoption; now when you really want to be mean to somebody, you can do so without the deterrent of reprisal because you can remain anonymous.

As a forensics consultant, my job is to try and track down this type individual. The first thing to determine is who owns AutoAdmit because they might have log files that would be useful. AutoAdmit was registered behind a proxy, and the mechanism for serving a subpoena was convoluted. However, we were able to obtain some IP addresses (the numbers the Internet uses to connect two computers) and begin the long process. To convert a pseudonym to a real human, you begin with the pseudonym and you look at the post times for that pseudonym. Then you have to find a log file to correlate the post time with an IP address. Often, to obtain a log file you have to file a subpoena. When you get the log file, hopefully you will establish a connect time from that log file. That connect time is then going to give you an IP address from an Internet Service Provider ("ISP"). Now you have to go get another log file so you file another subpoena. Hopefully you will be able to get an authentication match directly at the ISP. If you do not, you have to go through another log file to find another IP address and so on and so on until you finally get to the last hop. The last hop is the authentication from the IP address of the computer that crafted the message you were originally trying to trace.

Once you have an IP address you can hopefully track that down into a MAC address. A MAC address is the unique Media Access Control ("MAC") identifier and used to connect to the network. Then hopefully you can find the physical computer associated with that MAC identifier.

Note, we have only identified the computer; we still do not have a person, but usually, once you get to the computer you can get to a person. There are these wonderful "digital fingerprinting" methods which can prove that this is the computer which sent the message we saw originally on the Internet. This is a lot of work and it takes a lot of time. The relative effort associated with creating the pseudonym and creating the malfeasance in the first place, compared to the amount of effort required to track down the cyberbully very disproportional. Anytime systems become so disproportional we create opportunities for abuse.

There is one further potential twist in tracking down postings. There are a number of websites and tools that are designed to anonymize or obfuscate the real IP address of the computer the poster is using. Sites such as http://proxify.com/, or freethecountry.com offer private surfing or private surfing tools.

What about the people who set up the site itself? Should they be required to help or share the responsibility for the posters? When congress created the safe harbor in the Communications Decency Act of 1996, they created it for "providers of interactive computer services," shielding the provider from liability for the acts of their users.[7] The first question is whether the AutoAdmit website is a protected service under section 230. In *Universal Communications vs. Lycos*, the First Circuit, in a case of first impression, followed the Fourth, Ninth, and Tenth Circuits in holding that a website falls within the scope of a service under 230(c).[8] In an unpublished case, the Third Circuit held that in order to find liability, the bulletin board host must have "solicited and encouraged the actual negative commentary."[9] Finally, in *Zeran v. America Online, Inc.*, the Court, concerned with the chilling effect on the First Amendment, construed the safe harbor protections broadly.[10] The combination of these interpretations makes it unlikely Courts will find liability against bulletin boards regardless of how derogatory or inflammatory the posted content is.

One other technology shift to briefly discuss is the shift from paper money (cash and checks) to electronic money. Credit cards, debit cards, PayPal, and e-gold accounts are all just numeric access codes to our bank accounts and lines of credit. In our digital age, payment systems such as Point of Sale and e-commerce sites are all connected via networks. A by-product of the billions of electronic transactions is that a vast number of copies of electronic money exist across many databases.

One notable incident involved TJX, the parent company of TJ Maxx and other retailers. TJ Maxx's database was compromised sometime in 2005. Lack of forensic data and audit trails make it unlikely the exact initial intrusion date will be uncovered. By early 2007, TJX reported a likely 45 million credit and debit card numbers had been stolen. The data theft was linked to shopping sprees in Southern California and Canada, and Wal-Mart gift card purchases in Florida. How were these numbers spread so far across the country? Through an underground network of websites and bulletin boards that offer such information for sale, complete with guarantees backed up by escrow services.

7. 47 U.S.C. § 230 (2006).

8. 478 F.3d 413 (1st Cir. 2007).

9. Dimeo v. Max, 248 Fed. Appx. 280 (3d Cir. 2007).

10. 129 F.3d 327 (4th Cir. 1997).

We all need to think twice before we put any of our information on the Internet for criminals. Following the advice of Willie Sutton, "go where the money is and go there often."