Global Information Assurance Certification Paper

An Overview of Information Security and Privacy Threats

Mickey Elam
GSEC Practical Version 1.3
9 April 2002

Summary

The purpose of this paper is to provide an overview of some of the threats to personal privacy and security that exist in today's world. Some of the threats covered include voluntary surrender of information, active data collection, online data collection, and information theft. The importance of awareness, attitude, and education for the individual is stressed.

Developing threats to security and privacy are also covered. The developing threats covered are smart cards, biometric identification, and biochips. Once again, the importance of awareness, attitude, and education for the individual are illustrated. The role of the information security professional is also briefly discussed.

Introduction

The capability to gather and assimilate personal, private information has become both pervasive and highly advanced. Databases exist, both public and private, that track an individual's purchases, movements, and preferences. These databases also contain very personal and private data such as names, social security numbers, addresses, telephone numbers, sex, clothing sizes, and any other piece of personal data, no matter how trivial, that an individual, company or government might want to pay for.

There has been a growing awareness in society of these databases and their effects upon the individual. Telemarketers call, often during dinner. Junk mail fills snail-mail boxes and email inboxes. "Special offers" fill credit card and utility bill envelopes. These databases give marketing companies the information they need to determine who may be susceptible to their offers.

Laws exist to regulate the gathering and usage of this information, but limiting the digital forms of these activities is problematic. The ascendancy of information technology has enabled relationships to be established between separate pieces of information, thus leveraging the available data and allowing more intensive processing to be performed. This results in a more complete "picture" of an individual than was previously possible.

Finally, the vast amount of information available facilitates espionage, both governmental and industrial. With such huge volumes of information being collected and shared, the possibility that some small part of it is sensitive or valuable to a competitor or enemy is certainly not insignificant. In today's world, competition is so keen, and margins are so thin, that the loss or revelation of any sensitive data can mean the difference between profitability and bankruptcy. International security issues are such that information security can literally mean life or death.

This paper will discuss some of the methods, both current and in development, of digitally gathering and utilization of this information and some of the social and legal methods of controlling such data collection and use. It will focus on the importance of awareness, education, attitude and policies in information security, not just for corporations or governments, but also, perhaps especially, for individuals.

Voluntary Surrender of Information

Perhaps the most prevalent form of information collection, especially for individuals, is voluntary surrender. There are many varieties of this. A few are online purchasing, applications for credit and jobs, and surveys.

Online purchasing is a tremendous tool for the collection of personal data. An individual willingly gives up his name, address, credit card information, telephone number, and other valuable data for the privilege of purchasing a good or service online. Most persons don't even read the posted privacy policies, and if these policies are read, they are often not understood. The personal data submitted is transmitted over the public network. The data is often encrypted, but this isn't a requirement, and there is no good, simple way to determine that the server being communicated with is the one that is thought to be communicating with [10]. This personal data is also often stored on public servers. For example, online stores offer to store personal shipping and payment information for their customers' convenience.

The World Wide Web has become more useful for such activities as applying for credit or jobs in recent years. This improvement in utility has driven the perception that it is acceptable to submit personal information online. For the most part, this is an accurate perception; however, the Web is not completely safe for such activities. All of the possible breaches of security that apply for online purchasing apply to online credit and job applications as well. There is also other very sensitive information exchanged in these types of transactions such as credit reports and bank account balances and numbers. The potential for abuse of this information is tremendous.

One of the most innocuous methods of collecting information online is through the use of surveys. Often, there is a reward for the completion of a survey, such as the opportunity to win money or discounts on merchandise. These surveys are also often presented as opportunities for the consumer to assist a corporation in determining the needs and desires of the consumer. The data gathered through these surveys is most useful when it can be associated with an email address or name, information that most consumers are more than happy to give out. The fact that must be remembered about this method of information gathering is that it facilitates the creation of a profile of the consumer for marketing or other purposes.

All of the methods of information collection listed above are useful and desirable in the proper circumstances. However, there should be limits to their implementation. The limits most often thought of today are legal, but there are other, more effective ones available. Individuals should determine how much information they want to make available about themselves and take steps to prevent private data from becoming available. The most important components of consumers becoming more responsible for their privacy and security are education and awareness.

Companies and governments also have a responsibility to be good custodians of the information entrusted to them. One example of sensitive information falling into the wrong hands occurred in December of 2000, when the credit card database of online retailer Egghead was hacked into. The company did a good job of informing the credit card industry and its customers of the security breach, but the fallout of the incident potentially cost banks and consumers millions of dollars [7]. This incident could not have occurred without the complicity of the individuals who allowed their personal information to be stored by Egghead.

Active Data Collection

One of the most subtle methods of data compilation is done by actively collecting information through the sharing and review of sales data and other data a consumer may not even know he is submitting. Data on clothing preferences and sizes, food bought, clubs frequented and reading material purchased can be gathered in this manner. If a credit card or check is used for a purchase, all of the information on the sales receipt can be correlated to the identity of the purchaser. Many stores request the address or other identifying information of the consumer at the time of purchase.

Most people do not think twice about the information they give up in this manner. They do not think about the use to which this data can be put. This data can be

used to develop telemarketing lists and bulk mailing lists. Different, seemingly unrelated, bits of information can be analyzed for relationships. All of the information gained in the above manner is potentially valuable to someone.

Once again, attitude and education are the keys to the control of this type of information collection. Consumers should always be aware of what information they are giving up and the uses to which it can be put. Laws can be enacted to provide protection, but the potential for abuse still exists. It's much better to remove the temptation than to legislate against it. There are legitimate uses for the information collected in this manner such as fraud prevention, but prevention of abuse is difficult.

The type of data collection mentioned above occurs not only at brick and mortar stores, but also online. Knowledge of privacy policies is vital to knowing what is done with collected information. An excerpt from the Yahoo!™ privacy policy stating how information may be collected and combined is shown below.

> Yahoo! collects personal information when you register with Yahoo!, when you use Yahoo! products or services, when you visit Yahoo! pages or the pages of certain Yahoo! partners, and when you enter promotions or sweepstakes. Yahoo! may combine information about you that we have with information we obtain from business partners or other companies [13].

The privacy policy goes on to state that Yahoo!™ may confidentially share data with trusted partners. They do not define what entities are trusted partners. This is an example of a comprehensive privacy policy, but how many Yahoo!™ users have read or understand the policy? Once again, education is the key to maintaining personal privacy.

Online Data Collection

The method of information collection that has perhaps most captured the attention of the public is online data collection by companies such as DoubleClick™, Avenue A™, and 24/7 Media™. These companies collect data through the use of cookies and clickstream data. This has traditionally been viewed as relatively innocuous, but early in the year 2000, DoubleClick™ caused a great deal of controversy when it was revealed that the company had techniques whereby clickstream data could be related to personal user data like names and IP addresses. The company eventually stated that it would not utilize this capability until industry and government guidelines were developed to regulate such activity [8]. Online stores also have the capability to place cookies

on user's machines and monitor where the user may go to after leaving a site. These capabilities are much less well publicized, but they do exist.

The decision by DoubleClick™ not to participate in such information gathering was well received, but other companies with similar data availability exist and such companies could also develop the capability to correlate clickstream data with user information. Consumers have to be aware of these capabilities and the legal and social environments need to keep pace with technological developments. Once again, individual awareness and education drive the development of suitable privacy standards.

Information Theft

Perhaps the most damaging mode of information collection is information theft. Huge volumes of personal information are stored by credit reporting agencies, credit card companies, insurance companies and medical services providers. A significant portion of this information is stored digitally. There are laws and regulations such as the Health Insurance Portability and Accountability Act of 1996 [11] dictating that this data be stored securely, but there is great profit in acquiring it.

Secure storage of this data is of vast importance. Firewalls, intrusion detection systems, and network monitoring are vital tools in securing this stored information, but consumers need to be aware of what information about them is being stored and how it is shared. Once again, the example of the Egghead™ credit card database hack comes up. It is believed by many experts that Egghead™ did not use many of the tools available to secure their servers [7]. The company did a good job of informing the public of the problem, but perhaps the problem should not have happened in the first place.

A potentially much more damaging security breach was the responsibility of the United States Internal Revenue Service recently. The U.S. General Accounting Office released a report entitled "Information Security: IRS Electronic Filing Systems" on 16 February 2002 detailing the failure of the IRS' security systems in protecting taxpayer data contained in electronic tax filing servers [6]. This is an example of individuals (taxpayers) assuming that data would be safe under the control of an entity (the IRS). The GAO report outlined the failure of the IRS to use all tools reasonably at its disposal to protect taxpayer data in its hands.

Both the Egghead database hack and the Internal Revenue Service security failure are examples of organizations not using all tools and information at their disposal to protect the data entrusted to them. It is believed that the Egghead intrusion was interrupted before any significant damage was done and the IRS

security vulnerability was discovered by another government agency. Both of these events were well publicized and documented. The question remains, however, of how many such intrusions and hacks remain unpublicized or undocumented.

Future Threats

There are conflicting requirements and desires when talking about protecting privacy. On the one hand, there are few things more personally valuable for most people than their privacy. Just ask any celebrity how much he values his privacy. The main difference between the celebrity and the average individual is that the individual has his privacy, while the celebrity does not. Often, individuals do not realize just how much of value they are giving up on the privacy front until it is too late to stop the loss or to recover what has been lost.

On the other hand, it is possible to gain a great deal of convenience by giving up a little bit of privacy. Websites that store cookies on computers so that users are recognized when they visit again, user profiles stored on online retailers' servers so that the consumer does not have to re-enter personal information, and many of the other topics discussed above are just plain convenient. Each individual has to decide for himself just how much personal information to give up for convenience, but these decisions should be based on knowledge of the issues and awareness of the trade-offs inherent in them. This section of the paper will discuss two currently developing technologies that could have a tremendous impact on privacy in the coming years.

The first technology that will be discussed is smart card technology and the second is biometric identification and biochips. Both of these technologies could contribute tremendously to convenience, and even safety, but individuals should be very aware of the possible privacy issues involved with them.

Smart Cards

Smart cards have been in use in Europe for several years, mostly for prepaid phone calling cards and to prevent credit card fraud, but also for other uses. Smart cards consist of a plastic card in the credit card form factor with an integrated circuit microchip implanted into the plastic. The chip can consist of non-volatile memory only or can have limited processing capabilities [10].

Significant volumes of information can be stored on these cards. Most commonly, at least in the consumer market, the information consists of number of minutes of call time remaining or of bank account balances. Smart cards are

also an integral component of the Global System for Mobile Communication (GSM) standard for mobile phones and communication [10]. Many companies are also using these cards for physical and logical access to facilities and computing resources. Smart card uses also include electronic cash, medical records storage, mass transit access, and identification.

As the cost of microprocessors drops, the amount of information that can be carried on a smart card will rise. The convenience of smart cards implies that the volume of stored information that is sensitive will also increase. It is extremely convenient to have one's medical information on a credit card sized card, but is it a good idea? Identification using smart cards also seems like a good idea on the surface, but there are possible conflicts that arise when many functions are combined on the same card.

In the United States, there has been a push for some form of national identification card in the months since 11 September 2001. A number of individuals and entities ranging from Congress to Larry Ellison of Oracle have advocated such a card. Mr. Ellison advocates a card that facilitates the integration of many of the databases that are currently maintained by government and the commercial sector [13]. This might be a good idea if there were some guarantee that the processing power this would enable would never be misused, but there exists no such guarantee. Many feel that laws could provide a prohibition against misuse, but laws can change. A national ID card would allow virtually all known information about an individual to be collected into one easy to access interface. As pointed out earlier, disparate bits of information are not necessarily dangerous to privacy. The true danger to privacy comes when these bits of data are correlated and cross-referenced. The existence of the ability to analyze the data that currently exists virtually ensures that the ability will be used, perhaps in ways that were never planned for and therefore could not be legislated against.

Public awareness of many of the pitfalls of a national ID card is currently high [9], but steps are being taken to implement many of the preliminary steps without such public awareness. Many financial services companies are discussing how to use the data that they already possess to assist the government with the pursuit and apprehension of terrorism suspects [11]. This seems to be fraught with the potential for abuse and error. There is currently no way to ensure the accuracy of the financial and personal data these companies are the custodians of. Larry Ellison and Oracle have offered to provide the software for creating a national database with the information already contained in many individual databases for free and have challenged other technology companies to contribute as well [13].

Biometric Identification/Biochips

One of the most reliable methods of identifying a person involves biometrics. Biometrics involves identifying an individual through physical characteristics possessed only by that individual. These characteristics include fingerprints, retinal patterns, hand shape and size, facial features, and DNA, among others. It is possible, given sufficient resources, to falsify any of these characteristics; however, this is extremely difficult to do. A national database of these characteristics associated with the names and other personal data of individuals presents great potential for abuse. If this technology is fully utilized, the possibility exists for anonymity to become a thing of the past. No person could go anywhere without being recognized and tracked.

One of the major driving forces for the deployment of biometric systems is the perceived security benefit of these systems. These systems allow what is believed to be a positive method of identification of individuals. In the social climate of the day, this is seen as beneficial. However, biometric systems rely on the collection of all of the necessary physical data. This is a difficult process and could result in many abuses.

Another method of identifying a person based on individual characteristics involves the implantation of a microchip under the skin of the subject. This is referred to as a biochip. The uses of a biochip are similar to those of a smart card combined with a biometric system. These chips seem innocuous on the surface, but, as with many other security technologies, have the potential for incredible abuse. The main problem with these chips is that although they seem very convenient now, there exists the potential for "function creep [7]." For example, the company currently applying for government approval for such a chip is also working on developing the ability to implant a device that would allow satellite tracking of individuals [7]. Once again, anonymity and privacy become casualties of the drive for better security. Such technology removes the infrastructure requirements of the other biometric systems and allows truly borderless tracking of individuals.

The Big Picture

This paper has attempted to give an overview of some of the most serious threats to privacy and security. As stated earlier, the most important tools in preserving security and privacy are awareness, attitude, and education.

All individuals must take responsibility for their own security and privacy. Relying on laws or regulations to preserve security and privacy is not a good idea. Laws and regulations can only go so far, and cannot protect against unscrupulous

individuals and companies determined to use private information in an unlawful or unethical manner. Laws can also change, and if private information is already recorded in a database, it will be difficult, if not impossible, to remove it from such databases.

Companies and governments also have a responsibility to use the information entrusted to them in an honest and informed manner. These entities have resources much greater than any individual and so have a much greater requirement for responsible use of private data.

It's difficult for anyone who doesn't make a living in the security and privacy field to keep up with all of the new developments in the field. Security professionals have a responsibility to make decisions for the good of their organization and community [8]. Privacy is one of the fundamental rights set out in Article 12 of the Universal Declaration of Human Rights [12]. Privacy is fundamental to freedom. Ultimately, we are responsible for our own privacy, but we are also responsible for not interfering with another individual's privacy. Personal decisions allow us to fulfill these responsibilities, not laws or regulations.

Bibliography

1. Cagliostro, Charles. "Primer on Smart Cards." Smart Card Industry Association. URL: http://www.scia.org/knowledgebase/aboutSmartCards /primer.htm.

2. "Computer chip implanted in humans? Government to weigh security idea." SiliconValley.com. 27 February 2002. URL: http://www.siliconvalley.com/ mld/siliconvalley/business/special_packages/security/2756631.htm.

3. Ellison, Larry. "Digital IDs Can Help Prevent Terrorism." *The Wall Street Journal*. 8 October 2001. URL: http://www.oracle.com/corporate/index.html?digitalid.html.

4. "Financial companies to discuss how to use consumer databases to profile terrorists." SiliconValley.com. 3 April 2002. URL: http://www.siliconvalley.com/ mld/siliconvalley/business/special_packages/security/2989812.htm.

5. Global Information Assurance Certification. "GIAC Code of Ethics." URL: http://www.giac.org/COE.php.

6. "Information Security: IRS Electronic Filing Systems." Government Accounting Office. 16 February 2001. URL: http://frwebgate.access.gpo.gov/ cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=d01306.txt&directory= /diskb/wais/data/gao.

7. Lemos, Robert. "Lengthy Egghead investigation costs banks millions." CNET News.com. 9 January 2001. URL: http://news.com.com/2009-1017-250745.html?legacy=cnet.

8. O'Connor, Kevin. Press release. DoubleClick Corporation. 2 March 2000. URL: http://www.cdt.org/privacy/000302doubleclick.shtml.

9. "Privacy Under Pressure." SiliconValley.com. 19 October 2001. URL: http://www.siliconvalley.com/mld/siliconvalley/business/special_packages/securit y/2579675.htm.

10. Stein, Lincoln D. "The World Wide Web Security FAQ." The University of Houston. 2 January 1995. URL: http://www.telecomm.uh.edu/links/www-security-faq.html.

11. "The Health Insurance Portability and Accountability Act of 1996." United States Government. 1996. URL: http://www.hcfa.gov/hipaa/hipaahm.htm.

12. United Nations. "Universal Declaration of Human Rights." URL: http://www.unhchr.ch/udhr/lang/eng.htm (21 Jan 2002).

13. “Yahoo! Privacy Policy.” Yahoo!. 2002. URL: http://privacy.yahoo.com/privacy/us/.