The Necessity Of Computer Security Essay, Research Paper

The Necessity Of Computer Security

When the first electronic computers emerged from university and military

laboratories in the late 1940s and early 1950s, visionaries proclaimed them the

harbingers of a second industrial revolution that would transform business,

government and industry. But few laymen, even if they were aware of the

machines, could see the connection. Experts too, were sceptical. Not only were

computers huge, expensive, one-of-a-kind devices designed for performing

abstruse scientific and military calculations, such as cracking codes and

calculations missile trajectories, they were also extremely difficult to handle.

Now, it is clear that computers are not only here to stay, but they have a

profound effect on society as well. As John McCarthy, Professor of Computer

Science at Stanford University, speculated in 1966: “The computer gives signs of

becoming the contemporary counterpart of the steam engine that brought on the

industrial revolution – one that is still gathering momentum and whose true

nature had yet to be seen.”

Today’s applications of computers are vast. They are used to run ordinary

household appliances such as televisions and microwaves, to being tools in the

workplaces through word processing, spreadsheets, and graphics software, to

running monumental tasks such as being the heart and soul of the nations tax

processing department, and managing the project timetables of the Space Shuttle.

It is obvious that the computer is now and always will be inexorably linked to

our lives, and we have no choice but to accept this technology and learn how to

harness its total potential.

With any progressing technology, an unauthorized application can almost be

found for it. A computer could and has been used for theft and fraud – for

example, as a database and manager of illegal activities such as drug

trafficking and pornography. However, we must not just consider the harmful

applications of the computer, but also take into account the good that they have

caused.

When society embraced the computer technology, we have to treat this as an

extension of what we already have at hand. This means that some problems that

we had before the computer era may also arise now, in the form where computers

are an accessory to a crime.

One of the problems that society has faced ever since the dawn of

civilization is privacy. The issue of privacy on the Internet has risen many

arguments for and against having it. The issue of privacy has gotten to the

point where the government of the United States has placed a bill promoting a

single chip to encrypt all private material on the Internet.

Why is privacy so important? Hiding confidential material from intruders

does not necessarily mean that what we keep secret it illegal. Since ancient

times, people have trusted couriers to carry their messages. We seal out

messages in a envelope when sending mail through the postal service. Using

computer and encrypting programs to transfer electronic messages securely is not

different from sending a letter the old-fashioned way. This paper will examine

the modern methods of encrypting messages and analyse why Phil Zimmerman created

an extremely powerful civilian encipherment program, called the PGP, for “Pretty

Good Privacy.” In particular, by focusing on cryptography, which was originally

intended for military use, this paper will examine just how easy it is to

conclude why giving civilians a military-grade encrypting program such as the

PGP may be dangerous to national security. Therefore, with any type of new

technology, this paper will argue that the application of cryptography for

civilian purposes is not just a right, but is also a necessity.

Increasingly in today’s era of computer technology, not only banks but also

businesses and government agencies are turning to encryption. Computer security

experts consider it best and most practical way to protect computer data from

unauthorized disclosure when transmitted and even when stored on a disk, tape,

of the magnetic strip of a credit card.

Two encryption systems have led the way in the modern era. One is the

single-key system, in which data is both encrypted and decrypted with the same

key, a sequence of eight numbers, each between 0 and 127. The other is a 2-key

system; in this approach to cryptography, a pair of mathematically complementary

keys, each containing as many as 200 digits, are used for encryptions and

decryption. In contrast with ciphers of earlier generations, where security

depended in part on concealing the algorithm, confidentiality of a computer

encrypted message hinges solely on the secrecy of the keys. Each system is

thought to encrypt a message so inscrutably that the step-by-step mathematical

algorithms can be made public without compromising security.

The single key system, named the Data Encryption Standard – DES for short -

was designed in 1977 as the official method for protecting unclassified computer

data in agencies of the American Federal government. Its evolution began in

1973 when the US National Bureau of Standards, responding to public concern

about the confidentiality of computerized information outside military and

diplomatic channels, invited the submission of data-encryption techniques as the

first step towards an encryption scheme intended for public use.

The method selected by the bureau as the DES was developed by IBM

researchers. During encryption, the DES algorithm divides a message into blocks

of eight characters, then enciphers them one after another. Under control of

the key, the letters and numbers of each block are scrambled no fewer than 16

times, resulting in eight characters of ciphertext.

As good as the DES is, obsolescence will almost certainly overtake it. The

life span of encryption systems tends to be short; the older and more widely

used a cipher is, the higher the potential payoff if it is cracked, and the

greater the likelihood that someone has succeeded.

An entirely different approach to encryption, called the 2-key or public-

key system, simplifies the problem of key distribution and management. The

approach to cryptography eliminates the need for subscribers to share keys that

must be kept confidential. In a public-key system, each subscriber has a pair

of keys. One of them is the so-called public key, which is freely available to

anyone who wishes to communicate with its owner. The other is a secret key,

known only to its owner. Though either key can be used to encipher or to

decipher data encrypted with its mate, in most instances, the public key is

employed for encoding, and the private key for decoding. Thus, anyone can send

a secret message to anyone else by using the addressee’s public key to encrypt

its contents. But only the recipient of the message can make sense of it, since

only that person has the private key.

A public key cryptosystem is called the PGP, for Pretty Good Privacy.

Designed by Phil Zimmerman, this program is freely distributed for the purpose

of giving the public the knowledge that whatever communications they pass, they

can be sure that it is practically unbreakable.

PGP generates a public and private key for the user using the RSA technique.

The data is then encrypted and decrypted with the IDEA algorithm – which is

similar to the DES, but the work factor to decode the encrypted message by brute

force is much higher than what the DES could provide. The reason why the RSA is

used only when generating the keys is that the RSA takes a very long time to

encrypt an entire document, where using the RSA on the keys takes a mere

fraction of the time.

At this time, Zimmerman is bing charged by the US government for his effort

in developing the PGP. The government considers encryption as a weapon, and

they have established regulations controlling or prohibiting the export of

munitions. Since the PGP is a powerful encryption program, it is considered and

can be used as a powerful weapon and may be a threat to national security.

On the Internet, it is clear that many people all over the world are

against the US government’s effort on limiting the PGP’s encryption capabilities,

and their reason is that the ban infringes on the people’s right to privacy.

The PGP must not be treated only as a weapon, for it contains analogies

that are not used in wartime. One of them is authentication. The two-key

cryptosystem is designed with authentication in mind: Using someone’s public key

to encrypt enables only the owner of the private key to decrypt the same message.

In the real world, we use our own signature to prove out identity in signing

cheques or contracts. There exists retina scanners that check the blood vessels

in out eyes, as well as fingerprint analysis devices. These use our physical

characteristics to prove our identity. A digital signature generated by a

public key cryptosystem is much harder to counterfeit because of the mathematics

of factoring – which is an advantage over conventional methods of tests for out

identity.

Another analogy the PGP has with the real world is the need for security.

Banks and corporations employ a trusted courier – in the form of an armoured

truck or a guard – to transfer sensitive documents or valuables. However, this

is expensive for civilian purposes, and the PGP provides the same or better

security when securing civilian information.

While many argue that limiting the PGP’s abilities are against the people’s

right to privacy, the PGP must also be seen as a necessity as we enter the

Information Age. There is currently little or no practical and inexpensive way

to secure digital information for civilians, and the PGP is an answer to this

problem.

Computer privacy must not be treated differently than any other method to

make private any documents. Rather, we must consider the computer as a tool and

use it as an extension of society’s evolution. Clearly the techniques we employ

for computer privacy such as encryption, secure transfers and authentication

closely mirrors past efforts at privacy and non-criminal efforts.

The government is putting more pressure against the distribution of PGP

outside of the United States. One of their main reasons was that since it is

freely distributed and thus can be modified in such a way that even the vast

computational resources of the US government cannot break the PGP’s secured

message. The government could now reason that the PGP can provide criminal

organizations a means of secure communications and storage of their activities,

and thus make the law enforcement’s job much harder in tracking criminals down

and proving them guilty.

Also, we must never forget one of out basic human rights – one that many

laid their lives for, is freedom. We have the freedom to do anything we wish

that is within the law. The government is now attempting to pass a bill

promoting a single algorithm to encrypt and decrypt all data that belongs to its

citizens. A multitude of people around the world are opposed to this concept,

arguing that it is against their freedom and their privacy.

34b