An Overview of Computer Security as Told Through War Stories

By Ronald Seidl

What is Computer Security?

A computer is secure if you can depend upon it and its software to perform, as you would expect. To put it another way, a secure computer ensures that the information that you have saved will be accessible to you when you need it; and this information will remain unread and unaltered by any unauthorized party.

These two statements are like an executive summary of a larger more complex picture. The primary colors of this picture are confidentiality, integrity, and availability. In this case, confidentiality is control over who is supposed to read your information. Integrity is control over who may modify or alter your information. Availability is the accessibility of your information on your time schedule.

There is lot of different kinds of attackers who target these three primary areas of security. They range for the disgruntle employee who has been downsized out of a job, to a terrorist group who sees your company as way to make headlines. Sometimes they are just curious and want to look around. Others just want to try and "show off" their hacking skills.
However, sometimes these attackers are hostile, they come looking for a chance to steal something that belongs to you [A].

There are accidental breaches of security; sometime an inexperienced system administrator will try to fix a problem at the direction a manager who is unaware of security issues. These kind of holes may go undiscovered by the IT staff for weeks or months, but rest assured that someone will trip over them sooner or later.

So how do we highlight some of these weaknesses? If you look over the history of man, we have always had storytellers, or great epics poems or parables from the Bible or fairytales with moral endings. These stories cause people to change their actions.

Awareness training by telling stories shows the problem in way that most people can clearly see. They see others mistakes and faults at a safe distance, and sometimes they can even laugh the mistakes of others. Nevertheless, this is a valuable tool of teaching serious lessons. People will read and remember these war stories and they will change their actions over the long term.

Misplaced Confidence in Encryption

In January of 1917, Europe was at war. Arthur Zimmermann was the German Minister of Foreign Affairs in Berlin. He wanted to keep the US out of the European war. His plan was to entangle the US in a war on its own soil. He proposed to contact the President of Mexico to offer German support to fund a war between Mexico and the US, to regain lost Mexican territory [B].

This message was encrypted and sent from Berlin to Mexico City via Washington DC over US owned cables. Earlier in the war, the British had cut all but one of the German transatlantic cables. The British tapped the remaining transatlantic cable and the cables of other nations, including those owned by the US. That is why the German Minister, Zimmermann, was forced to use a US owned cable. Arthur Zimmermann and the German government fully believed that the code invented by the Germans was unbreakable and therefore safe to be carried over US lines.

The Germans did not foresee that the British, who were monitoring the US lines, would scrutinize this distinctly German message on a US cable. The British knew that this message was invaluable. They invested all their resources into decoding the message. This was accomplished with in one week. In less than three weeks, President Wilson was reading the text of this world-changing message.

With in 45 days of being sent, the text of Arthur Zimmermann's' telegram was printed on the front page of the London and New York newspapers. Germany and Mexico were embarrassed about this leak. Mexico did not go to war with the US and looked for ways to rebuild its relationship with the US. The US entered World War I on the side of the British.

Later during the war, the German government held hearings about the "Zimmermann Telegram". During the investigation Count Von Benstorff, former Ambassador to Washington, stated, "I am no cipher expert, but the cipher experts now state that there is absolutely no cipher which they cannot decipher" [C]. Clearly, the German government had changed their mind about the reliance of unbreakable codes.

We should view this incident as it applies to current day E-mails. This is clearly a loss of confidentiality. The lesson learned here is that the act of encryption and the reliance on the method of encryption does not make the information secure. Encryption makes it more difficult to "read" the message; it does not make it impossible. There will always be someone who may wish to take the time and effort to break the code and "read" the message.

In today's 'net' world, we need to have a scale to help us choose the strength of the encryption products we use. In the science of encryption, the length of the "key" is directly proportional to the strength of the encryption. The longer the key, the harder it is to break open the code. This table shows in general terms the importance of the information verses the lifetime of the information.

How Strong for How Long

This table shows the Security Requirements for different kinds of information. [D]

Type Of Information	Lifetime	Minimum Key Length
Tactical Military Information	Minutes/Hours	56-64 bits

New Product Info, Interest Rates Changes, Mergers	Days/Weeks	64 bits
Trade Secrets	Decades	64 bits
H-Bomb Secrets	>40 Years	112 bits
Identities of Spies	>50 Years	128 bits
Personal Affairs	>50 Years	128 bits
Diplomatic Embarrassments	>65 Years	128 bits

One other note, this lifetime of information should also be reviewed with regards to the table on brute-force attacks. The point being, nothing is ever secret forever.

Who's Really Logged On?

The incident started with a complaint about the "shipping program". It had a bug in it. The customer reported that valuable demo equipment was being shipped to the wrong locations or lost all together. After reviewing the application and the shipping records for the past three-month period, we found that the customer was only having problems with shipments entered by one user account. That account was used by the shipping clerk. This corporation was downsizing and had started a relationship with a national temporary service. This temporary service provided workers for the shipping clerk position. To further complicate the situation, over the three-month period the customer had ten different shipping clerks. All of the incorrectly shipped packages where entered into the system between noon and 1 pm. However, this was the normal lunch hour for the temporary service people.

As we were looking into this problem, the system administrator shared with us several productivity improvements she had implemented. The system administrator determined that she could not spend all her time entering and deleting new accounts for the ever-changing temporary workers. She chose to use the same account login and password for any temporary worker from the same company.

All the pieces had come together, and the big picture began to take shape. The customer realized that it could save money by hiring temporary workers in the shipping department. The system administrator realized that she could save time and money by re-using the same account login and password for all the temporary workers. Last of all, one of the previous temporary workers had realized that with the shipping clerk away at lunch between noon and 1 pm and the unchanged shipping clerk's account login and password, he could send his friends a new laser printer every week.

This is an example of the loss of integrity. Someone who was not supposed to be able to change information was able to do so. It is easy to see that some cost saving programs do not save money, because the do take time to evaluate all the possible complications in implementing the programs. Analysis of a potential cost savings of any downsizing should take into account security.

Availability

Denial of service attacks come in all flavors, sometime from within your own firewall. Moreover, sometimes the tools you choose to monitor of denial of service attacks do not monitor everything. Take for example a cable television provider was building out an infrastructure to start providing Internet access and webpage storage to its cable customers. The build out required a great deal of labor in an already tight labor market. The cable company hired a number of local college students to do the work. The cost of labor was cheap, and it showed that the company was working within the community. This looked like a public relation win for the company.

In the first quarter, it became evident that the data storage space was vastly under estimated. More storage space had to be made available to their growing customer base. Speed was the order of the day. With an eye on cost, the cable provider purchased one terabyte of storage and made provision to "upgrade" as needed. Surely, this was a sign that business was good.

However, at the end of the third quarter the company was again out of storage. This time the company decided to analyze which customers where using the storage space. The idea was to locate the new storage closer to the customers. But to their surprise, the company found that the bulk of the space was used by their internal "build out" group. With a closer look at the type of data being stored, it was revealed that most of the files were MP3 music.

The cable company had provided jobs for the local college kids, as well as a place for them to store their music at work. Because the storage space was in use, the company lost money because their customers could not access the storage space.

This is an example of the loss of availability. The storage space was taken, making it impossible to store the cable customers information when needed. Though this was not an attack from across the Internet, it was a denial of service.

Encryption or Encryption NOT!

There has always been an air of mystery surrounding the hiding of information by cryptology. It seems to be more akin to magic than mathematics in the minds of some people. This air of magic causes people to avoid examining closely what they call encryption.

A number of years ago I was asked by a customer to "improve" their encryption "program". This customer encryted all their text files to keep private company information secret. The customer used a Unix provided utility called "rot13", which was originally used to mask offensive jokes in the transmitting of e-mail. This masking was done by adding the number 13 to the decimal equivalent of the ASCII character being "encrypted". For example, this utility would change the letter "a" to "m" or the letter "b" to "n". This was not a strong method of securing information.

However, this customer was reading an airline business magazine on a recent airline flight and discovered that hackers were using brute-force attack methods to force open files encrypted with weak encryption methods. The article went on to say that industry experts recommend that encryption key length should be changed to “56 bits”. The customer wanted me to convert the utility to shift 56 characters instead of 13.

The lesson here is that knowing the buzzwords of the industry is not a replacement for understanding the technology of the industry. This customer had placed their confidence on something they did not understand. The company’s secrets were secured in nothing but blind faith.

This particular customer did not understand why he needed “56 bits”. He did not understand the types of attacks facing him, nor did he understand the basics of cryptology algorithms.

Cryptology algorithms can be divided into two types, Symmetric and Asymmetric. Symmetric uses one key to encode and decode, whereas Asymmetric requires a pair of keys, one public and the other private [E]. In both cases, the length of the key is directly connected to the strength of the encryption, even against brute-force attacks.

The table below gives an eye-opening look into the problems facing customers like this one. It shows the cost of computer hardware technology used to brute force open encrypted files. Though this data is 6 years old, it puts a “stick in the dirt” to help people see what kind of money is involved in breaking encryption. It therefore enables people to make a better choice about encryption key length.

Brute-Force Attack verses Key Length Table

This is a view of the cost of Hardware Brute-Force Attack in 1995 Dollars: [F]

Cost	**56 Bit Key**	**64 Bit Key**	**128 Bit Key**
$100K	2 Sec	1 year	10^{19} years
$1M	.2 Sec	37 days	10^{18} years
$10M	.02 Sec	4 days	10^{17} years
$100M	2 mSec	9 hours	10^{16} years
$1B	.2 mSec	1 hour	10^{15} years
$10B	.02 mSec	5.4 minutes	10^{14} years
$100B	2 microSec	32 seconds	10^{13} years
$1T	.2 microSec	3 seconds	10^{12} years

The Importance of Training

A large number of authors and computer professional societies have devoted a lot of time and ink to talking about the importance of training. For an example, the SANS Institutes’ “Network Security Roadmap” poster, has been mailed to professionals for the past four years. The results from a 1999 SANS Institutes survey of 1,850 security experts said, “Untrained people cannot maintain security [G]”. The SANS Institutes also has published a list of the mistakes managers make in regard to computer security. “Assigning untrained people to maintain security and providing neither the training nor the time to make it possible to learn and do the job” ranked high on their list [H].

Bob Vilolino, in an article entitled “The Security Façade” from Information Week magazine, summed it up best when he said, “The weakest link in security is often ignorance.” [I]

References

A - Accuite Security and Investigations, Inc. "Information Security" (1997-2000)
URL: http://www.acuite.com/services/informationsecurity.html (26 July 2001)

B – Tuchman, Barbara W. The Zimmermann Telegram, Ballantime Books, New York City, 1958

C – Friedman, William F. and Mendelsohn, Charles J, The Zimmermann Telegram of January 16,1917 and its Cryptographic Background, Aegean Park Press, Laguna Hills CA., 1994, Pg 30

D – Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc New York, 1994, {First Edition}, Pg 140

E - Hardie, Darlene Hill, “PKI: What is this thing, really**?”,** May 21,2001
URL: http://www.sans.org/infosecFAQ/encryption/PKI2.htm (26 July 2001)

F – Schneier, Bruce, Applied Cryptography, John Wiley & Sons, Inc New York, 1996, {Second Edition}, Pg 153

G –Guel, Michele D.,“SANS99 Survey of 1,850 Security Experts”, SANS Network Security Roadmap 2001, Sans Institute, 2001

H – The SANS Institutes, "Mistakes People Make that Lead to Security Breaches" (1997-2000)
URL: http://www.sans.org/mistakes.htm (26 July 2001)

I – Vilolino, Bob, “The Security Façade”, Information Week, October 1966