6.915 Computer and Network Security	Fall Term, 1995

Lecture 3 : September 14th

Lecturer: Ron Rivest *Scribe: Andrew M. Sarkar*

Going back to address an issue from last class: there was a denial of service attack last night on the "theory" file server. Somehow the main disk /u had permissions set to 770 instead of 775. Some of the issues we dealt with last time are treated in the *Computer Security Reference Book*. Fire in computer rooms: read pages 266, 267 and 324. Also from the same book the following quote (page 325)

> At least 80% of computer fraud, theft, sabotage, and accidents are caused by company staff. A further probable 15% comes from the contractors and consultants who are given access to your buildings, equipments, and codes, so only about 5% is external crime of all forms. ...

Topics covered today:

- Communication Security and Phone Systems
- Risk Analysis
- Introduction to Cryptography

1 Communication Security and Phone Systems

The phone system is the biggest communication system around; it is a large, interesting system that needs to be understood and made secure. It is an information-processing system itself, providing services that people may wish to use. It is an integral part of many other companies' information systems. Watching how security on the phones has changed, in adaptation to the different attacks on the system, is a good way to study the evolution of security, in general. Phone booths, and pay phones have evolved into highly impenetrable fortresses. They are designed against physical attacks and attempts to make money off of them as well as being difficult to vandalize.

Rivest indicated a book called *The Hacker Crackdown* (1992, Bantam; also available online), about law and order in the computer cyberspace zone. Some terminology brought up: phone freaks, computer hackers, and phracks. A phone freak is someone who uses phones illegally, computer hacker is someone who breaks into computer systems illegally; the combination of the two is called a phrack. A little bit before our times, in the mid 70s, devices called blueboxes were used to get free long distance. In the early 80s modems were tried to be made to get free calls so that hackers could call up favorite remote sites for free. The 2600 Hz signal used for blueboxes became an acronym for phreaks. There is a news group alt.2600, a FAQ, that discusses vboxes, redboxes, blueboxes and has code for Ethernet sniffers.

Besides the phone book, there are some other services related to the phone industry... some of which smack of inverse phone listings. x9400 will tell you what MIT extension number you are calling from. 1-800-692-6447 will tell you what phone number you are calling from, on regular phones. 1-900-933-3330 is a pay service that will tell you the customer name and address of any given phone number. Compuserve is also reputed to offer this last service. Does the fact that these services exist bother us? Should it? Who owns your address, phone number, social security number? These questions and other social policy issues are talked about in a book called *Who Owns Information?*, by Anne Branscomb.

In general, we should not rely on the phone system for security or authenticity, when we lay other responsibilities on it, such as the interactions between computer systems. We can see from the phone freaks' use, or misuse, of the system that the phone system is not particularly secure.

2 Risk Analysis

Risk Analysis is about analyzing a situation, and the risks that apply to it, as well as the security measures being taken currently and the measures that could be taken (more or less measures). It is a standard approach for deciding the seriousness of a risk. It is done to show the validity of an expensive system that appears to do nothing useful. It is a validation for security budgets. In class we discussed the simple example of a gym locker, that has the ability to be locked.

1. Identify assests and determine value

clothes	50
wallet	100
glasses	100
sports eq.	30

drivers liscense	5
car keys	2000
house keys	5000
tapes and walkman	70

2. Find vulnerability
   - theft
   - accidental loss
   - disclosure of information (eg. read wallet)
   - vandalism
3. Estimate likelihood of exploitation

10	more than once a day
9	once a day
8	once every three days
7	once a week
6	once every two weeks
5	once a month
4	once every four months
3	once a year
2	once every three years
1	less than once every three years

   For example for theft a 7 could be estimated.
4. Figure annual loss

   Approximately 7400 dollars worth of expected loss each time, occuring every week. This works out to about 370,000 dollars per year.
5. Determine cost of added security

   To get a lock would cost 5 dollars. If it would be broken, it would cost another 5 dollars to replace.
6. Estimate likelihood of exploitation under added security

   The new likelihood of theft could be estimated at a 4.

7. Form conclusion

   The lock would give a yearly loss of about 20,000 dollars. This saves us 350,000 dollars, yearly, and so should be done.

Notice how silly this can be, since the numbers are all such rough estimates. It is very unlikely that gym users lose 370,000 dollars a year to theft, and certainly not 20,000 a year when they lock their locker daily. Even though it may seem silly here, especially with our soft numbers and no research done into the problem, in big systems, where a computer company has a vested interest in finding out whether or not to protect themselves, risk analysis is useful. This example was more meant to show the method of the procedure, rather than its usefulness. The homework will make us go through another example of risk analysis, to give a good idea for it, as well.

Rivest also discussed a book *Hackers*, by Steven Levy. Speculation followed on whether the movie (which he came back during lecture 4 to tell us that it is not worth seeing) was based on that book. There was a computer person at MIT when passwords were first introduced, that objected to the password system: Stallman. He would even say to a user, when logging in, "I see that you have chosen password x. May I suggest you use the null string password. It is much easier to type and conforms to the correct philosophy, namely that passwords shouldn't exist."

This may seem silly to us, as we are used to passwords and they fulfill an important security objective. But we can see why he might object if we consider the following scenario. MIT says that its rooms are too insecure. A system will be set up so that there is a retinal scanner at the door of each room, and only authorized personel may enter, after giving a retinal scan. Just imagine how annoying all the students and faculty would find this.

3 Cryptography

Despite this not being a crypto course, we shall get into some of its basics and discuss its relevance to security. Recommended book: *Cryptography: Theory and Practice*, (Stinson, CRC Press, 1995). What is cryptography about? Communication in the presence of adversaries. What are the worries? Confidentiality (or secrecy, or privacy): keeping messages secret. Also Authenticity (or integrity): making sure the recipient of a message knows who originated it.

Lets introduce our classic characters: Alice, Bob, and Lucifer. Alice is sending messages to Bob, and Lucifer controls their communications medium. He can change the message, can block messages, can send his own messages. Bob wants to know that Alice is sending the message and that it is unmodified and that it is secret.

Alice sends an encoding of a message: ciphertext. Alice has an encoder to accomplish this. She then sends it out on the communications line, where Lucifer can get at it. Bob has a decoder. If Bob receives a message, he decodes it with his decoder and if it makes sense, he will accept it as coming from Alice.

We can distinguish between two forms of cryptography depending on what it is used to protect the data: either information theory or computational complexity.

Information-theoretically protected data is proven to be safe. There is a proof of the unbreakability of the encrypting algorithm, so it is impossible for Lucifer to read the messages being sent. To do this, however, a key has to be known to both parties, as long as the message; as more messages are sent, more key is used up. Since we like to share a fixed length of a secret key, the majority of encryption uses computational complexity. In this case we are using the fact that it would take too long and it would be too hard for the enemy to decrypt the messages we are sending. In these cases a proof of security of the cryptosystem hinges on some unproven computational assumption which is however generally known to be true (for example factoring large integers is hard.) By this very definition, we are on shakier ground when we are sending information; however, since it is easier, it is the more common practice.

3.1 Information-theoretic secrecy

The encryption is provable as being unbreakable. An example of an encryption scheme is the **one time pad**. It requires Alice and Bob to share a key, k (example: $k = 0101001110011\ldots$), where k is at least as long as the message to be sent. It is very important that this pad has not been used before.

To prepare the message, Alice puts her message and the key (one time pad) together, in a bitwise XOR function.

$$c = m \oplus k$$

c is the ciphertext sent over the line. If Bob gets a message, he takes that ciphertext and XORs it, in a bitwise fashion, with his copy of the (same) key, to recover the original message.

$$c \oplus k = (m \oplus k) \oplus k = m$$

This technique provides perfect secrecy. If the pad is never used again, then the ciphertext does not increase Lucifer's knowledge about the message (he may know something beforehand, like that it is likely about the design project that Alice and

Bob are partners on, that is due tomorrow.) Indeed it is easy to prove that given a ciphertext c any message m could have been sent using the key $k = c \oplus m$

Why is it important to only use the pad once? If you let it be a two time pad, and somehow Lucifer knows or guesses that you are using the same pad, he can gain some knowledge. If m_1 and m_2 are encrypted using the same pad k to get c_1 and c_2 then Lucifer can compute

$$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

This may not seem very important, but statistical analysis shows that it can be very easy to get the two origonal messages from this, due to the redundancy of the english language. One thing to note is that if m_1 and m_2 are compressed before the encryption, then it is much harder to get the origonal messages from the XOR of the two compressed messages.

3.2 More Cryptography

We ran out of time in today's class to go on with Cryptography. Next time we will discuss how to achieve authenticity in an information-theoretic way. Then we will discuss algorithms that use computational complexity in order to achieve privacy and authentication. Then we will get into DES, the Digital Encryption Standard (1977).

4 Handouts and Readings

There were three handouts. Problem set one, the scribe notes from the first class, and an article from the New York Times Consumer's World section, called "Web of Cellular Phone Fraud Widens".

Chapter 11 of the textbook deals with Communication Security. Chapter 13 talks about Risk Analysis. Chapters 2 and 3 cover Cryptography.

The FAQ file of the newsgroup alt.2600 is available online from the class Web page and in the Athena class locker.