Scribe: Cryptography and Network Security (Week 2: Class.3)

Rohit - 20CS60R71

11-Sep-2020

1 Design principles for security

There are some basic principles of security that are followed worldwide and generally, not abiding them laid to some disaster.There are many design principles exist but the most important ones are explained here.

1. **Make defaults safe**: Default means what the system do normally. Users should never change the defaults. So, we need to make the defaults safe. For example using https as default instead of http would possibly defeat many attacks because in http, the integrity, confidentiality and availability properties can easily be broken. However if used https as default then system become more secure.

2. **Make the design open**: We have to make our design open. It means we should ask for feedback from as many people as possible like open source projects. It has been seen that more eyeballs often leads to better security. However in it there is a possibility that some bug might steal our open source code.

3. **Principle of least privilege**: Principle of least privilege is used in practice very commonly. It means that we should give privileges only to users and principles that are required for a particular task. For example never use root account (use sudo), there is timeout that is we cannot login as an administrator for a time greater than timeout. Key point is that we should put some bound on who can access the most critical resources of the system.

4. **Least surprise**: Least surprise means that user should not surprise. So, essentially user mental model that is how a interface or a system work should align with our system design. The interface should do what user thinks it should do. It should not make user confused. So, we have to understand user's mental model.

5. **Never trust the input**: We need to always verify integrity, authentication etc.

6. **Isolation**: It basically involves compartmentalization of resources. Compartmentalization of resources means that there can be multiple users and they can run multiple things on their own. However if their is a shared machine like the machines in a department then we have to compartmentalize. That is if someone is did wrong by running some code from his account then it should not compromise others account, otherwise it would be totally unfare. For example hardware isolation, disk partition, virtualization, sandboxing, firewall etc.

7. **KISS (Keep-It-Simple-Stupid)**: It means that we need to keep designs as simple and small as possible thst has multiple disks. Best example is TPM (Trusted Platform Model).

   (a) **Minimize the trust base**: In this we secure a very small code and hardware base. We have full faith on that part that is that is secure. And using that as a root of trust we try to secure the rest of system.

   (b) **Minimizes attack surface**: In the simplest terms, the "attack surface" is the sum total of resources exposed to exploit within a system. We should minimize the attack surface to minimize the opportunities available to cybercriminals.

2 Tutorial 1 solutions

Q1. Answer the following questions.

1. Let n be a composite number. Then prove that

$$\phi(n) \leq n - \sqrt{n}$$

Ans. n is a composite number. So, we can write $n = ab$ where a and b are coprime numbers, or $n = p^k$ where p is a prime number and k is some arbitrary number.

(a) **Case 1:** $n = ab$, So

$$\phi(n) = \phi(a)\phi(b)$$

And,

$$\phi(a) \leq a - 1$$

$$\phi(b) \leq b - 1$$

Therefore,

$$\phi(n) \leq ab - a - b + 1 \leq ab - \sqrt{ab}$$

$$\phi(n) \leq n - \sqrt{n}$$

(b) **Case 2:** $n = p^k$, So

$$\phi(n) = p^k - p^{k-1} \leq p^k - p^{k/2}$$

$$\phi(n) \leq n - \sqrt{n}$$

Q3. Let the encryption system be as follows:
Each letter of the plain text is replaced with its position in the English alphabet with (A is 1 and Z is 26). To each number, add the value of the polynomial $f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$ either at x_1 or at x_2, which are roots of the polynomial $f(x) = x^2 + 3x + 1 = 0$. Replace the resulting number with the letters.
Decrypt the cryptogram: ECGUCTUJKHV

Ans.

$$f(x) = x^6 + 3x^5 + x^4 + x^3 + 4x^2 + 4x + 3$$

$$f(x) = x^4(x^2 + 3x + 1) + x(x^2 + 3x + 1) + x^2 + 3x + 1 + 2$$

substituting $x^2 + 3x + 1 = 0$ in above equation:

$$f(x) = 2$$

It means that while encryption, the position of english alphabet letter is added by 2. So, for decryption we need to shift back that is by subtracting the position of alphabets by 2.So, the decryption of ECGUCTUJKHV is CAESARSHIFT

Q4.Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.

1. Ankit copies Rohit's homework.
2. Shubham crashes Akash's system.
3. Venu changes the amount of smayan's check from Rs.100 to Rs.1,000.
4. Pravesh forges Ashish's signature on a deed.
5. Suprajit registers the domain name "iitkgp.com" and refuses to let IIT KGP buy or use that domain name.
6. Rashil obtains Rutwik's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
7. Maniteja spoofs Susanth's IP adress to gain access to his computer.

Ans.

1. Confidentiality
2. Integrity
3. Availability
4. Availability
5. Availability
6. Availability, Integrity
7. Integrity

Q5. Argue for or against the following proposition. Ciphers that the government cannot cryptanalyze should be outlawed. How would your argument change if such ciphers could be used provided that the users registered the keys with the government?
Ans. Yes,Ciphers that the government cannot cryptanalyze should be outlawed. Because if it is not outlawed, then those who can cryptanalyze and got keys of cryptosystem would able to get all data. And that data if used in harmfull way then can impact very much.