Home Work 3

True False :

1. SSL mitigated protocol version roll back attack by including the version number again in the authenticated and integrity checked messages. **True**
2. The resiliency of X.509 certificates against forgery attacks depends on the cryptographic strength of the hash function used in the signing process : **True**
3. Stateless firewalls are more efficient than application firewalls : **True**
4. IKEv2 uses diffie-hellman to protect against DoS attacks : **False**
5. Signature based IDSs can detect previously unknown attacks. **True**

Short Answer :

1. **PKI**

a) Use openssl to generate a 4096 bit public/private key pair and sign your homework solution using your private key. Include your public key and the signature as separate files in a zip file along with your solutions. Make sure to keep track of your private key, since hw4 will need to be signed with the same key.

Answer :
Install openssl for generating 4096 public/private key pair.

Steps:

1. openssl genrsa -aes128 -passout pass:******* -out private.pem 4096
2. openssl rsa -in private.pem -passin pass:****** -pubout -out public.pem

Private.pem and public.pem are public/private key pairs.

3. Signing the document :

```
 openssl dgst -sha256 -sign /Users/ishitaverma/private.pem -out /tmp/sign.sha256
/Users/ishitaverma/Desktop/iv447_hw3.pdf
```

```
openssl base64 -in /tmp/sign.sha256 -out signed_hw.out
```

b) Describe all of the steps and cryptographic algorithms openssl performed to sign your homework and what security properties each provides.

Answer : We perform the signing of homework in the following steps:

1. First we generate public and private key using openssl.
2. Password is set on the private key file so , it will be encrypted using AES. AES is symmetric key algorithm, meaning same key is used for both encryption and decryption.
3. After this is done homework solution file can be given as an input to secure hash function SHA256 algorithm which is the cryptographic algorithm used for securing our document.
4. The result of the hash function can be signed by using RSA algorithm and private key. RSA is public-key cryptosystem which is used for secure data transmission.

2. **IDS**

Answer **:**

Probability(normal|syn) = Probability(syn|normal) * Probability(normal)/p(syn)
=0.05*0.96/(Probability(syn|normal)*Probability(normal)+Probability(syn|sql)*Probability(sql)+Probability(syn|syn)*Probability(syn))

=5*0.96/(0.05*0.96+0.05*0.03+0.9*0.01)=82.05%

Research Paper and Questions :

In our day to day, there are so many systems and softwares that we implicitly put our trust on. In the paper Reflections on Trusting Trust by Ken Thompson, he has explained That you can not totally trust the application or code that you have not created yourself. But still we depend on so many software and services online and use them with trust.In our day to day life we trust on many things blindly. For example when we drive car for our day to day commute we trust on the mechanical components of the car. There are many things that can go wrong with the internal machinery of the car like break failure etc, but still we trust on it and continue with our commute. The components on which our trust is built on this is the Manufacturer of the car, we trust the brand name and the security feature that they will offer. Another example is using home lock system, trust relationship with lock system is that once we lock our home, no intruder can get in to it. We lock the house with trust and leave. The components in lock system are key and lock. Any lock can be opened with the intended key only.

Just like our daily life we trust on the online software and systems that we use. One such example is Google Docs. Google docs, Google sheets and Google Slides are word processor, spreadsheet and presentation program are part of free web services provided by Google. We completely trust them and write and create our documents and presentation using Google Docs. We share these documents with other people a well so they can work simultaneously on them and edit them accordingly. The trust relationship that we have with Google Docs is that our documents are secure with Google and no intruder can access them. The key component that Google Docs use is Encryption. Encryption brings a higher level of security and privacy to Google services. When we share our documents we move them across our devices, Google services and their data centers. It is important to protect the data using multiple layer of security, including techniques like HTTPS and Transport layer security. Another online service that we use is online transaction services. We enter our credit card information with these third party system for processing with full faith. There are many threats involved with using online transaction systems like theft of credit card information. For a secure online payment system, the transaction flow must be end-to-end encryption. Technology (Software and Hardware) solution are paramount to safeguard the payment ecosystems, industry collaboration is also integral component against cybercrime.