**CS6823 Network Security**

**Homework 3**

This home work is worth a total of 65 points (6.5% of your total course grade). It is composed of five true/false questions each worth 1 points, two multiple part short answer with points values marked for each part and questions based on reading a research paper. The midterm will follow a similar structure of true/false questions and a few multiple part short answer questions. The midterm will not include any paper summaries or use of openssl.

**True False questions (15 points)**

Circle only one of the choices (3 point each)

1. SSL mitigated protocol version roll back attack by including the version number again in the authenticated and integrity checked messages. True False
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 False
3. Stateless firewalls are more efficient than application firewalls. True False
4. IKEv2 uses diffie-hellman to protect against DoS attacks. True False
5. Signature based IDSs can detect previously unknown attacks. True False

**Short Answer (30 points)**

1. PKI (20 points)
2. 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. [10 points]

This is a hint on how to use openssl for this part: <https://www.zimuel.it/blog/sign-and-verify-a-file-using-openssl>

1. Describe all of the steps and cryptographic algorithms openssl performed to sign your homework and what security properties each provides. [10 points]
2. IDS (10 points)
3. Wolf Security released an intrusion detection system that can detect Syn floods and SQL injection attacks. They boast a low false positive rate and high accuracy rate, rates are in the following table:

How connection is classified

|  |  |  |  |
| --- | --- | --- | --- |
| Type of connection | Syn flood | SQL Injection | Normal |
| Syn flood | 90% | 5% | 5% |
| SQL Injection | 5% | 90% | 5% |
| Normal | 5% | 5% | 90% |

For example, when the IDS observes a Syn flood, it correctly classifies it as a Syn flood with probability 90%, misclassifies it as an SQL Injection attack with probability 5%, and misclassifies it as a normal connection with probability 5%.

For the purposes of this problem, assume that Syn floods are 1% of all connections, and that SQL Injection attacks are 3% of all connections, while 96% of traffic consists of normal connections.

Also assume that a connection cannot be both a Syn flood and an SQL injection attack at the same time.

When the IDS announces that it detected a Syn flood, what is the probability that the connection is, in fact, normal? Give your calculations. [10 points]

**Hint:** This problem is similar to the base rate fallacy problem: <https://en.wikipedia.org/wiki/Base_rate_fallacy>

**Research Paper and Questions (20 points)**

Read Ken Thompson’s Reflections on Trusting Trust [1]

In our day-to-day lives, we implicitly trust countless systems, institutions, people, devices, etc to be trustworthy - to not be faulty, to not be malicious, and so on. When we drink from the water fountain, we have to trust that the last person to use it didn’t spill poison into the mouthpiece, that the municipal water supply has been checked for quality by the city or county, that the pipes in the building are sufficiently new, that the pipe supplier didn’t provide faulty pipes, that the pipe supplier’s metal supplier didn’t supply faulty metal, etc. The list goes on and on. Describe two systems that you use in your daily life that you implicitly trust. For each, describe the trust relationships between that system and the systems on which it relies, the components it uses, etc. Obviously, this could go on forever, so stop once you have a reasonable list (we’ll leave the definition of “reasonable” up to you, so just put in a best-faith effort). How much of a security risk do these trust relationships introduce? Describe two computer systems (software, online services, etc) that you use in your daily life that you implicitly trust. For each, describe the trust relationships between that system and the systems on which it relies, the components it uses, etc. Obviously, this could go on forever, so stop once you have a reasonable list (we’ll leave the definition of “reasonable” up to you, so just put in a best-faith effort). How much of a security risk do these trust relationships introduce?

[1] Attached as part of this assignment