Bradley Lamitie

Assigned on 9/13/2016

Due on 9/20/2016

Data Communications Thought Questions 3-1 to 3-6

1. A) For unimportant resources I would use a password protection. I would use a password because it’s easy to remember and not as intrusive as biometrics. However, I know that passwords can easily be cracked, but because im using it for unimportant information I believe it’s okay to use a password.

B) For more sensitive resources I would most likely use biometrics as my form of authentication, namely, iris recognition. This form of authentication is hard to replicate, is unique for each person, and is very precise.

2. The promise of newer authentication systems is to have authentication types that are more precise, unique, are nearly impossible to replicate, and are easily accessible.

3. Anti-replay is a sub-protocol of IPsec that is part of IETF. It avoids hackers injecting or making changes in packets that travel from a source to a destination. By sequencing packets if a packet isn’t within an expected range the packet will be dropped (Fortinet, 2016).

4.

|  |  |  |  |
| --- | --- | --- | --- |
| Rule | Destination IP Address or Range | Service | Action |
| 1 | ALL | 25 | Allow Connection |
| 2 | 10.47.122.79 | 80 | Allow Connection |
| 3 | 10.32.67.112 | 21 | Allow Connection |
| 5 | ALL | ALL | Do not allow connection |

5. Private keys are kept secret, and you cannot access the true party’s private key. If somehow, the supplicant could get a hold of the private key, they could ‘prove’ themselves as the true party.

6. Espionage is obtaining access of information secretly, without permission of the party who owns said information. There can be many purposes of espionage, but the biggest one would have to be getting the upper hand, whether it be in business, personal setting, or government.

**Citation**

"Fortinet Knowledge Base - View Document." *Fortinet Knowledge Base - View Document*. Fortinet, n.d. Web. 20 Sept. 2016.