CS6823 Network Security
Homework 2

True False questions (20 points undergrads) (10 points grads)

Circle only one of the choices (4 points each undergrads) (2 points each grads)

1. RSA used to encrypt a message provides message integrity.
   True
2. Risk-based two-factor authentication systems can cause account lockout issues.
   True
3. TCP sequence numbers mitigate spoofing attacks from onpath attackers who can eavesdrop. **False**
4. Any symmetric-encryption algorithm with a 128-bit key size would be computationally infeasible for any attacker to decrypt the cyphertext. **False**
5. Disabling auto-trunking mitigates VLAN hopping attacks. **True**

Short Answer (30 points undergrads) (20 points grads)

1. Authentication (18 points undergrads) (12 points grads)
   Note for this question: Identification is the claiming of an identity. Authentication is the act of verifying or proving the claimed identity.
   Your NYU ID card contains many different factors which may be used for identification, authentication, or authorization. Describe three scenarios in which your NYU ID card is used for each of these. For each scenario, answering the following: (6 points undergrads) (4 points grads) for each scenario

- Scenario 1: NYU IDs are used to tap into school buildings, restricted to students and staff only.
  a) Which of identification, authentication, and authorization is involved?
  Tapping an ID on the card reader is used as identification. Even if you are not the person on the ID, by tapping and attempting to enter, you are claiming to identify as someone with privileges.
  b) What factors are involved (something you have/are/know/can do)?
  Magnetic stripe sends information electronically to a scanner that is linked to a computer physically.
  c) How secure is the security in this scenario? How bad would it be if the security were to be compromised? How likely is it that such an attack would occur? Given these, do you consider the security in place to be sufficient, or do you think the costs of increased security (in terms of money, hassle, etc) would be justified?
  Someone could easily pose as a student if they have similar physical features because security staff may not recognize any differences. In this way, someone could enter the building to intend physical harm to

students, or possibly to gain access to information or spaces they are not supposed to. In terms of buildings with large access to students and staff, I do not think that an attack like this would be very likely, I think they might just force their way in or sneak in through an open door if they were intending to do some harm, which would not be solved by increasing ID security. I think our current security is sufficient for proving students are students and faculty are faculty, although it does not do much more than that, such as authentication if a security officer cannot distinctly analyze a person.

- Scenario 2: School ID cards can be used as an identifying or additional document for professional applications/privileges.
    a) Professionals, such as someone at the DMV or passport processing center could use picture, name, and school information in conjunction with other identification to verify a person. This serves as authentication for security purposes.
    b) Personal photo and legal name on ID. An ID must show signs of being directly issued by the school.
    c) Considering school IDs are not used as primary sources of identification most of the time, its use as a secondary form does not pose much harm. Although school IDs can be easily replicated via photoshop, especially if they are not being electronically scanned, this can pose some identity theft risks. The risks require far too much planning and resources, therefore they would probably only be done with significant intent. I do not think changing the ID card in any way would help in this instance. The use of holographic detailing already deters some fake ID attempts because it signifies the ID origin.
- Scenario 3: Dorm building access by tap is restricted to only students registered to that dorm.
    a) The sticker containing dorm name, and even further magnetic strip access allows students into their dorms. If you are not given explicit permission to access a dorm at the beginning of the year via their issue of such stickers, you are not authorized to enter, and must speak to the resource officer.
    b) Additional holographic stickers supplied by dorm authority on ID. Information updated and connected to ID that specifies dorm occupation.
    c) Someone attempting to gain access to a dorm may use the dorm of a verified student that looks similar to them to get in. In this case, much like scenario 1, it would be hard to detect. Although, for the most part students attempting this are trying to see their friends, physical harm is still a threat. Perhaps, if students had to scan ID to exit as they do to enter, the

resource offer could be provided additional information as to if someone has entered twice without exiting and prompt them to ask the visitor more questions. This would not be too costly, as the existing scanner could be used for exit as well, if not, then an exit scanner would have to be installed, which are not too costly considering other security technologies available.

2. Attacks (12 points undergrads) (8 points grads)
    a) Describe one attack that availability mitigates and one attack that authenticity mitigates? (3 points undergrads) (2 points grads)
    Availability can mitigate DDoS attacks on a server overwhelmed by packets by filtering and restricting content from IP addresses. Authentication mitigates phishing attacks, as a person would have to verify their identity perhaps through multi factor authentication sources in emails or logins.
    b) Describe a cryptographic method for achieving authentication and one for achieving confidentiality. (9 points undergrads) (6 points grads)
    U2F authentication mitgates user end comprimision. The token is paired to an account (for example google), and provides a physical form of second factor authentication. AES provides confidentiality for messages to prevent eavesdropping. It uses a symmetric key system with linear and non-linear components to ensure optimal encryption.