

CS 461 / ECE 422 Information Assurance
HW #2
Due submitted to Compass by 3:00 p.m. Feb. 5

The questions below prefaced by T/F are true-false questions. For these you must select one or the other, but may clarify your answer with more text if you wish.

1. **T/F** Security concerns are separate from software engineering concerns, so that an efficient way to design and implement software is to get its functionality right first, and later add security mechanisms.
2. Describe the difference between a constraint, a requirement, and a control in a security policy.
3. **T/F** Once a security policy has been established, one needs to review it and its effect on the system periodically but infrequently.
4. **T/F** The only people who are needed to develop a security policy are security experts and application experts. Since management doesn't understand either, it's only role is to adopt the plan developed by the experts.
5. Describe the difference between a business continuity plan, and an incident response plan
6. **T/F** If one symmetric cryptographic method uses a longer key than another, it is more secure.
7. **T/F** An important principle of symmetric cryptography is that keys and the data being encrypted are completely separate---in no way does a key depend on data values.
8. **T/F** It is critical for the functional operation of a Feistel network that the operator that combines the output of the f function with half the result from the previous stage be an XOR. In other words, no other function could replace the XOR, with no other changes to the Feistel network, and still have the property that decrypting is the same as encrypting, but with a reversed key schedule.