

Name: \_\_\_\_\_

## This week's readings

- [1] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, 1990. ISSN 0734-2071. URL <http://doi.acm.org/10.1145/77648.77649>.
  - [2] Vern Paxson. Bro: A system for detecting network intruders in real-time. In *Proceedings of the USENIX Security Symposium*. January 1998. URL <ftp://ftp.ee.lbl.gov/papers/bro-usenix98-revised.ps.gz>.
  - [3] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting mobile communications: the insecurity of 802.11. In *Proceedings of the International Conference on Mobile Computing and Networking (MOBICOM)*, pages 180–189. Rome, Italy, 2001. URL <http://doi.acm.org/10.1145/381677.381695>.
  - [4] Stuart Staniford, Vern Paxson, and Nicholas Weaver. How to Own the Internet in your spare time. In *Proceedings of the USENIX Security Symposium*. 2002. URL <http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf>.
- 

1. What is the main pitfall of using a stream cipher that WEP falls victim to?

2. What is the main design flaw of WEP?

3. What would a easy and effective incremental implementation change be to patch WEP's keystream reuse?

4. What's wrong with how WEP uses a CRC?

5. Express the vulnerability to authentication spoofing using the rules and message meaning from the logic of authentication paper, and note the difference between the goal and the result. (If you can't do this, explain in words using the vocabulary of the BAN logic).