

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 an intrusion detection system good for? Why not just firewall instead?

2. What does a subterfuge attack (in general) against an IDS exploit? (Don't list a specific subterfuge attack, express in general what it is.)

3. What should an administrator do when an intrusion is detected?

4. If I encrypt a message using your public key, which of the following is true? (Note: any of the following could also be true based on other features of the protocol; make the assumptions about keys made by Burrows et al.) Second, which of Burrows's rules is used to gain this result?
 1. Everyone knows it is a message for you.
 2. Only you can decrypt the message.
 3. Everyone knows it is a message from me.
 4. Only you know it is a message from me.

5. In Burrows et al.'s Logic of Authentication, explain in your own words and summarize the meaning of the statement:

$$\frac{P \text{ believes } Q \xleftrightarrow{K} P, \quad P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$

Vocabulary (some of this may be covered in class)

- BAN logic: Believes
- BAN logic: Controls
- BAN logic: Fresh
- BAN logic: Said
- chosen plaintext attack
- dictionary attack
- fail-closed vs. fail-open.
- firewall
- IDS (intrusion detection system)
- ingress filtering
- kerberos
- man-in-the-middle attack
- misbehavior
- optimistic ack
- phishing
- replay attack
- scanning
- shared key
- signatures, certificates
- smurfing
- sniffing
- spoofing
- web of trust
- zombie