This week's readings


---

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:
   \[ P \text{ believes} \; Q \xrightarrow{K} \; P, \quad P \text{ sees} \; \{X\}_K \]

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