Network Security HW 17

<!-- pagebreak -->

Network Security HW 17

David Ayeke April 10. 2017

A. Brute-Force SSL uses keys up to 168 bits. This makes brute force impractical. B. Plaintext Dictionary. SSL uses effectively 128 bits for the keys. The rest of the key is generated from the hello messages. The dictionary would need to be much loarger. C. Replay Attacks SSL uses nonces so this can't happen. D. Man-in-the-middle attack. SSL uses certificates for authentication, so it is not possible to pretend to be a server. E. Password Sniffing Everything is encrypted. F. IP spoofing Even with the IP, the spoofer needs the secret key in order for this to work. G. IP hijacking Everything is still encrypted so the hijacker gets nothing. H. Syn flooding. There is nothing to stop this attack.