CS558 Notes
2/14/17

Presentation 1: Apple vs. FBI

- 2015 - Shooting in San Bernardino, CA
- iPhone 5C used by attacked protected by passcode
- iCloud data could not be accessed since FBI reset password
- FBI wanted a custom iOS image that would disable security features, allowing brute-force attacks
- One possible way to unlock the phone would be to put it in DFU mode and upload a custom firmware image
- iOS 8 Added many security features, including default encryption
- Case was a turning point, showed company standing up to the government

Presentation 2: Equation Group Breach

- Players:
    - Discovered by Kaspersky
    - May be associated with the NSA
    - Data sold by Shadow Brokers
        - Russian Government?
        - NSA Insider
- EXTRABACON: Tool released to verify authenticity
    - Attack on a large class of enterprise routers
    - Uses buffer overflow vulnerability in SNMP protocol
    - Allows attacked to disable SSH password verification

Lecture

- Message Authentication Codes
    - Do not prevent attacker from reading the message
    - Protects integrity of message, prevents modification
- Bad MAC: MD5(k || m)
    - Suffers from length extension attacks
- Good MAC: HMAC
- Encryption + MAC
    - Encryption methods that are CPA secure but malleable cannot be CCA secure
    - In order to satisfy CCA security, you must add a MAC to the algorithm
        - Sender:
            - Encrypt message c = Enc(m)
            - MAC message t = MAC(c)
            - Send (c, t)
        - Receiver
            - Verify t
            - If valid, decrypt c, else fail