Picking Electronic Locks Using TCP Sequence Prediction

Ricky Lawshae 2009

Who am I?

- **OSCP, GPEN**
- **Network Technician for Texas State University**
- **Have been working with electronic building access systems for more years than I like to think about**

Abstract

- Testing of security of building access systems always focused on ID cards and other authentication mediums
  - RFID
  - Magstripe
  - Biometrics
- More prevalent usage of networked building access systems means more focus needs to be put on the controllers themselves
  - Lack of encryption
  - Persistent TCP sessions
  - Predictable sequence numbering

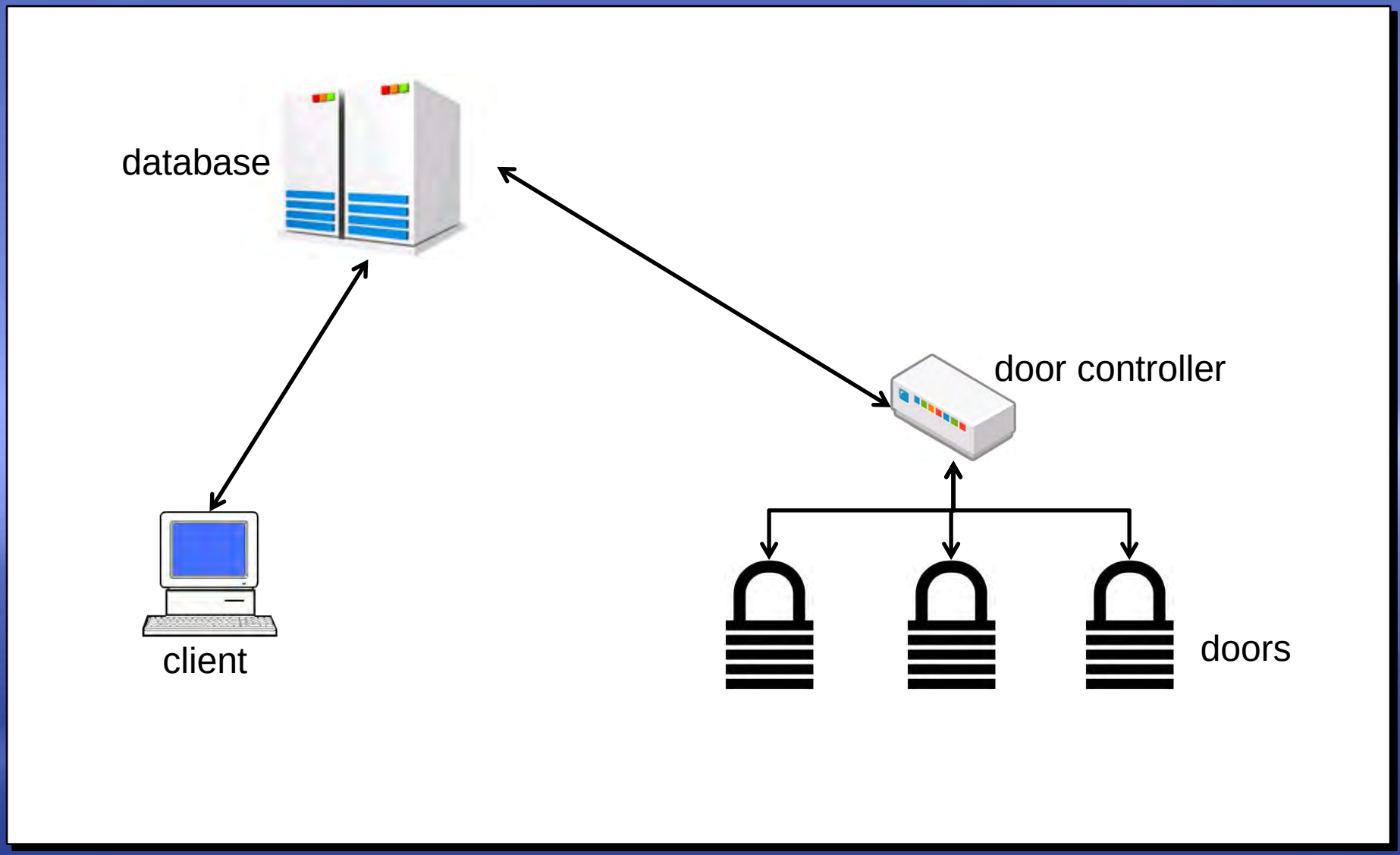
The Question

Is it possible for attackers to spoof commands to these access systems without needing an authentication medium at all?

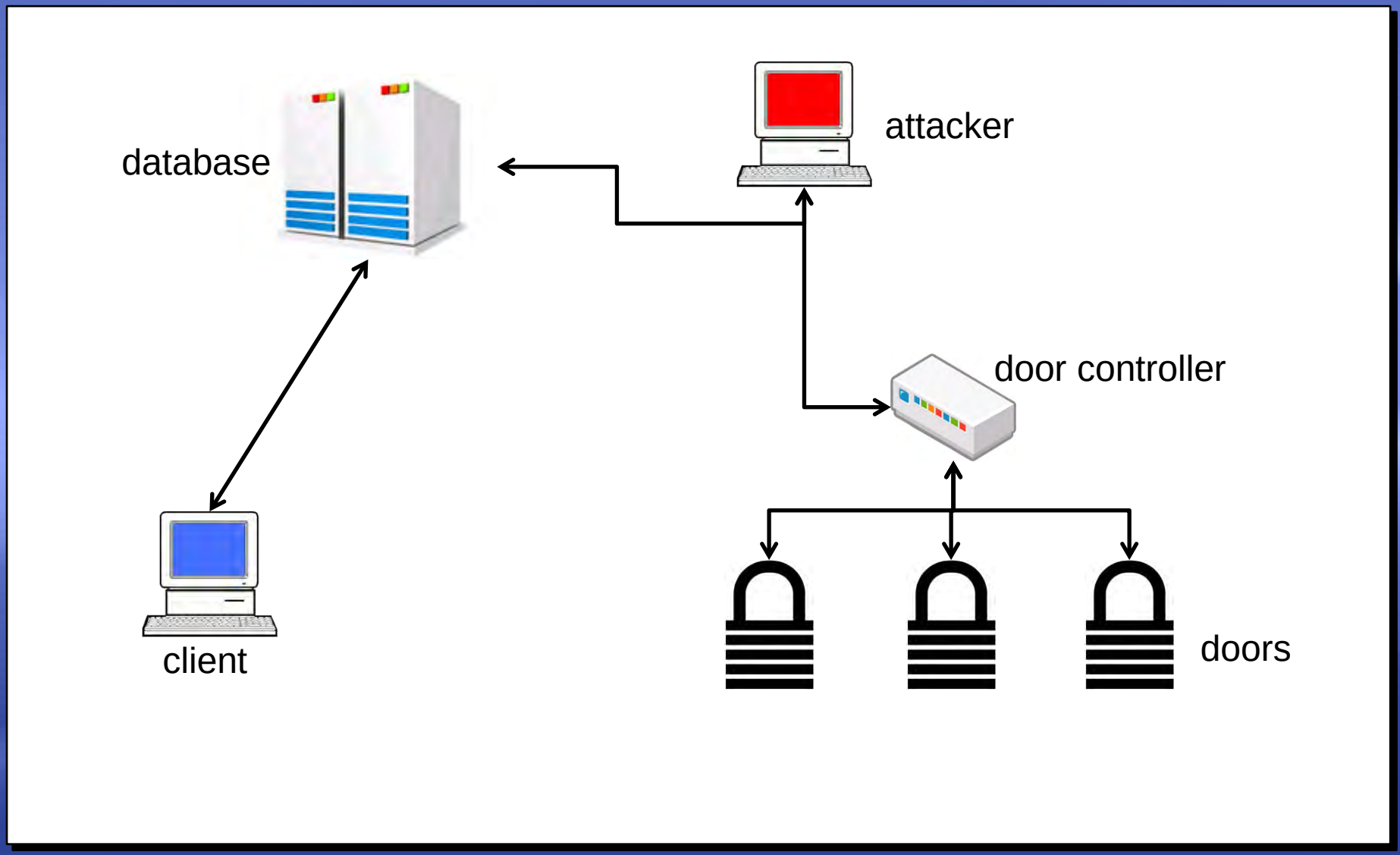
Brief Overview of Electronic Building Access

- Authentication devices and locking devices both connected to control system (door controller)
- Door controllers connected via TCP/IP to central database
  - Client programs used to make changes to database which are propagated down to door controllers
  - Status of locks/alarm points monitored remotely
  - Commands to lock and unlock(!!) doors can be sent across the network

Picking the Lock



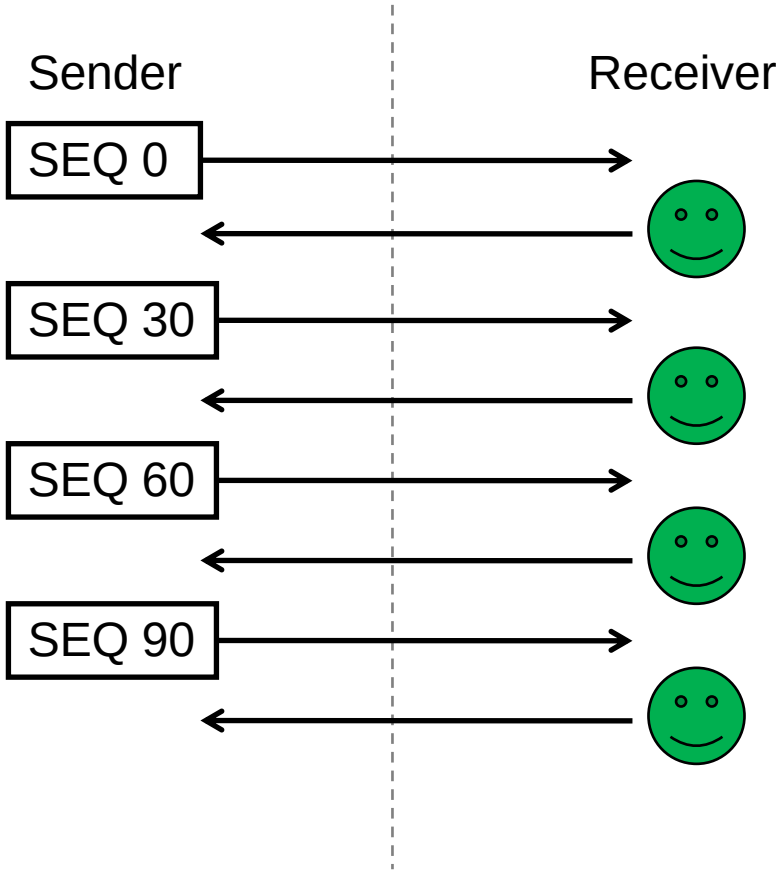
Picking the Lock



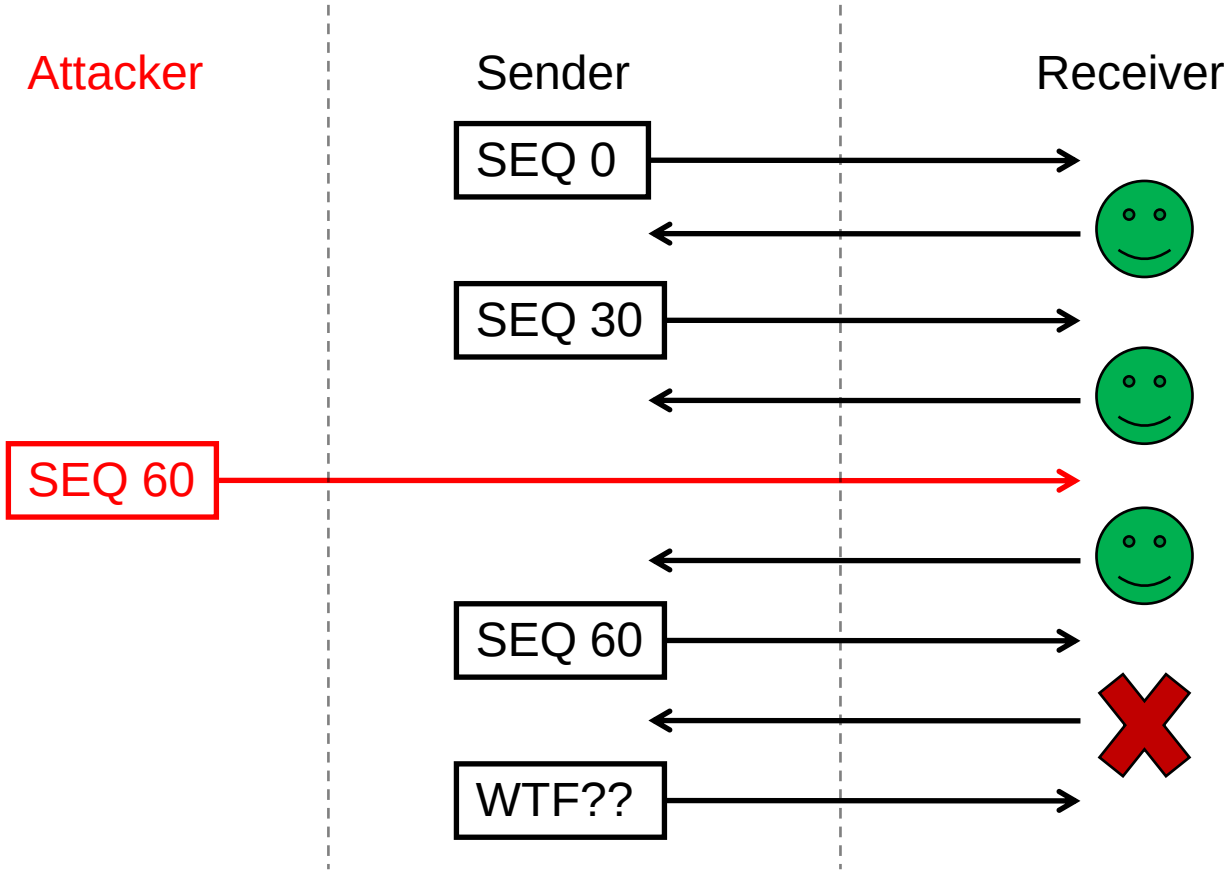
Why It Works

- All comes down to TCP sequence prediction
  - Usually used to hijack TCP sessions
  - Guess the next sequence number, inject a packet into an existing session
- Has been fixed in most modern operating systems and applications
- Embedded systems are still notoriously bad

TCP Sequence Prediction Illustrated



TCP Sequence Prediction Illustrated



Proof of Concept?

Conclusion

- Breaking authentication medium not necessary to bypass networked electronic building access system
- Any networked device must protect itself against networking vulnerabilities
- These problems are not hard to fix!
  - You
    - Put door controllers on separate LAN
    - Monitor for MITM attacks
  - Vendor
    - Make sequence numbers harder to guess
    - ENCRYPT THE TRAFFIC

The End