Outline of project proposal – Benjamin O’Neill

Name: Benjamin O’Neill

College: Emmanuel

User Identifier: bo271

Director of Studies: Dr. Thomas Sauerwald

Project idea:

The MIFARE classic smartcard, and most other smartcards, use symmetric cryptography for access control. Limited on-chip memory means typically only a small number of keys are used for all devices (e.g. doors) in a large organisation, so if one card or access control device is compromised, the stolen key can access all other devices.

This can be solved by the use of asymmetric cryptography, such as digital signature algorithms, where each card can hold a unique private key and access control devices contain no secret keys.

Possible extension: experiment with the timing predictability of the smartcard used, and attempt to implement a distance-bounding protocol similar to that used by the MIFARE plus EV1 chips to prevent relay attacks.

Supervisor: Dr. Markus Kuhn

Other resources:

* My computer, for working in college. Code backups will be made using Git.
* Programmable smartcard (e.g. Javacard) for testing and demonstrating the protocol.
* Contactless USB ISO 7816-compatible smartcard reader.
* Development software for the programmable smartcard (e.g. NetBeans Java Card plugin)

Success criteria:

* Should take no more an a second to determine whether a card is valid.
* Access rights of a card should be revocable without having to modify the card itself.
* system should be flexible – unlimited doors, each with different access privileges etc.
* Should be secure – Very resistant to most, or all, likely forms of attack.