Project Deadlock
(Extended Abstract)

Kamila Součková[2*] Adam Dej[2†]

Supervisor: Tomáš Vinař[1‡]

[1] Katedra aplikovanej informatiky, FMFI UK, Mlynská Dolina 842 48 Bratislava
[2] Katedra informatiky, FMFI UK, Mlynská Dolina 842 48 Bratislava

Project Deadlock is an attempt to provide a complete system to allow ISO/IEC 14443a-compliant cards [ISO, 2011] (ISICs or ITICs) to be used for unlocking doors and gaining access to other electronic appliances. We will provide software for managing access rules (integrated with the university's electronic info system), and the embedded hardware and software. This paper provides a design and implementation overview of the system being developed.

1 Main Components of the System

1.1 Server

The components of the system are managed by a centralized server to simplify maintenance and administration. The server communicates with the other components via standard TCP/IP over Ethernet to allow for utilizing the existing networking infrastructure, and a flexible architecture (including routers, PoE switches, etc.).

The server provides auxiliary functions for the embedded devices, such as automated firmware updates, long-term logs storage, and time synchronization. It also serves as centralized data storage/database (will be discussed later – see section 2).

The server communication protocol is packet-oriented, request-response model, implemented on top of UDP. The payload is encrypted and authenticated using a device-specific key via the NaCl library[Bernstein et al., 2012]. More details are available online at [doc, 2015].

1.2 Controller

Every appliance (e.g. a door lock) is controlled by a device that communicates with the server (e.g. to retrieve application-specific data or firmware updates, and to send logs.) If at all possible, the controller should be able to operate when the server is inaccessible, as we want to provide a fault- tolerant, reliable system. The base use case of unlocking doors is specifically discussed in section 2.

1.3 Reader

The card reader is the user-visible device – it scans for the ISIC/ITIC card, authenticates the card, provides an interface for communication with the card when more complex interaction is needed, and provides user feedback (visual and auditory – one or more LEDs + speaker). More readers can be connected to a single controller, e.g. inside and outside for a door lock.

2 Use Case Analysis: Door Lock

The system will be used to open locks as follows: The reader retrieves and validates the ID of the user's smart card, and sends it to the controller. The controller then searches its (local) database for this ID, determines whether to open the door and logs the action (both locally and on the server). The local ID database is periodically updated from the server, which compiles it for every door from an easy-to-manage access rules database integrated with the university's electronic info system. The controller also logs unexpected events, such as detecting opened doors without authorisation.

3 Source code, hardware schematics, and documentation

Project Deadlock is a work in progress. The existing sources and hardware designs are published with the MIT license at [src, 2015]. The documentation is available at [doc, 2015].

References

[ISO, 2011] (2011). *ISO/IEC 14443 – Identification cards – Contactless integrated circuit cards – Proximity cards*. ISO/IEC Committee.

[doc, 2015] (2015). `https://github.com/fmfi-svt-deadlock/server/wiki`.

[src, 2015] (2015). `https://github.com/fmfi-svt-deadlock`.

[Bernstein et al., 2012] Bernstein, D. J., Lange, T., and Schwabe, P. (2012). The security impact of a new cryptographic library. `http://nacl.cr.yp.to/`.

*`kamila@ksp.sk`
†`adam@ksp.sk`
‡`tomas.vinar@fmph.uniba.sk`