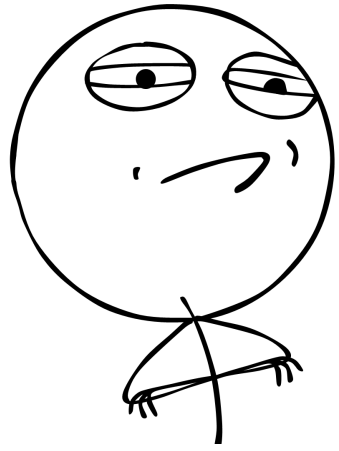
remote-upgrading microcontroller firmware

like a boss



sECuRE, 2012-02-21

`github.com/raumzeitlabor/hausbus` 265e07 .. 9fcad

Ist-Zustand (2011-11-13)

- General-PIN hardcodiert
- Tastendrücke werden per Hausbus weitergegeben
- Perl-Script läuft auf der Blackbox und validiert Benutzer-PINs, öffnet Tür nach korrekter Pin-Eingabe
  $\rightarrow$ langsam (Hausbus), viele Fehlerquellen

Soll-Zustand

- Notfall-PIN hardcodiert, aber nicht verteilt
- Benutzer-PINs im EEPROM (2048 B) des Pinpad-Controllers
- periodische Übertragung der Änderungen

Design

- Hausbus instabil, geringe Paketgröße (32 Bytes)
  $\rightarrow$ effiziente, zuverlässige Übertragung und Recovery

- **Keine** Debugmöglichkeit
  $\rightarrow$ möglichst wenig Code-Änderung auf dem Pinpad-Controller

- Kritische Infrastruktur
  $\rightarrow$ gestaffelter Rollout mit gründlichen Tests

Quality Assurance (2011-11-13)

- Code zunächst in C schreiben, nicht für Mikrocontroller
- Code für Mikrocontroller anpassen, separat testen
- Mikrocontroller-API mockup, mit valgrind testen
- Code Review

Upgrade 1: EEPROM write (2011-11-18)

```
'E' <uint16_t dest><uint8_t len><bytes><uint32_t crc32>
```

- Schreibt noch nicht ins EEPROM
- sendet CRCERR oder ACK zurück
- Perl-code zum Testen auf Hausbus-Zuverlässigkeit und Kompatibilität der Implementation:

```
perl -Ilib -MBusmaster -E 'Busmaster->new()->send('pinpad',
    "E\0\0\4abcd\x3D\x19\xA7\x2D")'
```

Upgrade 2: EEPROM checksum (2011-11-19)

- sendet EEPROM-CRC mit dem Türstatus
- Perl-code kann nun EEPROM synchronisieren
- Pinpad-Controller kann überprüfen, ob das EEPROM intakt ist, bevor es entsperrt

Upgrade 3: Test-Verifikation (2011-11-19)

- Für 7 Tage prüft der Pinpad-Controller Benutzer-PINs zusätzlich zur Blackbox
- Ergebnis wird nur auf den Hausbus gesendet
- Fehlerrate/Erfolgsrate wird vom Validator-script auf der Blackbox erfasst (100% Erfolg)

Upgrade 4: Unlock! (2011-11-26)

Unlock the door when the EEPROM pin verify says it's OK.

We've had 0 false verifications (and 7 total verifications) within the last 7 days.

```
--- a/firmware-pinpad/main.c
+++ b/firmware-pinpad/main.c
@@ -405,9 +405,7 @@ void handle_command(const char *buffer) {
    pincnt = 0;
    memset(pin, '\0', sizeof(pin));
-   // After 7 days of testing and no problems, we can turn
-   // this on:
-   //unlock_door();
+   unlock_door();
    return;
```