

Verzendbox met manipulatie-indicatie

gegevens veilig met de post verzenden

Luka Matić (Kroatië)

In beveiligde communicatiesystemen op basis van one-time pad's (OTP's) worden berichten versleuteld en gedecodeerd met een unieke, toevallige sleutel. Om dit te laten werken, moeten zowel de zender – doorgaans Alice genoemd – als de ontvanger (beter bekend als Bob) dezelfde sleutel gebruiken. Alice genereert de sleutel, maar hoe kan ze deze op een veilige manier naar Bob sturen? Het is dit kip-en-ei probleem dat het in dit artikel beschreven project probeert op te lossen.



Specificaties

- Open source-ontwerp zonder verborgen 'trucs'
- Capacitieve box-open detectie
- Detectie van invallend licht
- Reistijdinformatie
- Temperatuurdetectie
- IR-communicatie
- Herbruikbaar

Dit project is een (logisch) vervolg op mijn "Echte Random Number Generator" [1] en "One-time Pad Crypto Shield" [2] en probeert het probleem op te lossen van het veilig uitwisselen van *one-time pad*-sleutels (OTP) die op bijvoorbeeld een SD-card zijn opgeslagen. Ik begon met het idee om een manipulatiebestendig apparaat te ontwerpen, maar kwam erachter dat het veilig wissen van gegevens van een op flash-ge-

heugen gebaseerd apparaat zoals een solid-state drive (SSD) of een SD-kaart vrijwel onmogelijk is [3]. Bovendien vertoont zelfs SRAM-geheugen enkele parasitaire burn-in effecten, waardoor de gegevens die het bevatte kunnen worden gereconstrueerd [4]. Met dit in het achterhoofd heb ik besloten om niet een box te bouwen die bestand is tegen manipulatie, maar een die aangeeft dat er gemanipuleerd is.

Werkingsprincipe

Alice slaat een vers aangemaakte OTP-sleutel op een microSD-card op en legt deze in de speciale verzendbox. Ze sluit de doos en zet hem op scherp door er een *challenge-and-response string* in op te slaan met behulp van een contactloze (IR) link. Vervolgens stuurt ze de box per post naar Bob. Als hij die ontvangt, vraagt hij Alice om de *challenge string*. Hij kan hiervoor elk 'onveilig' kanaal gebruiken – bijvoorbeeld telefoon of e-mail – omdat alleen Alice deze string kent en Bob de box heeft. Met behulp van de optische link ontgrendelt Bob de box door de *challenge string* in te voeren. De box reageert ofwel met de *response string* ofwel met een waarschuwing voor mogelijke manipulatie. Alleen Alice kan de geldigheid van de *response string* bevestigen. Als de *response string* ongeldig is of als de box een manipulatie-waarschuwing heeft gegeven, gooit Bob de SD-kaart gewoon weg en gebruikt hij de potentieel onveilige OTP-sleutel niet voor een veilige communicatie met Alice. Als de box wordt geopend zonder eerst

te worden uitgeschakeld met behulp van de *challenge string*, of als er op een andere manier mee wordt geknoeid, zal hij de *challenge-and-response strings* veilig uit zijn geheugen verwijderen. Kwaadwillenden kunnen de box onderscheppen om de SD-kaart te lezen en te kopiëren en de doos dan door te sturen naar Bob, maar ze kunnen de doos niet opnieuw op scherp zetten met dezelfde *challenge-and-response string* omdat alleen Alice die kent, en dus zal Bob merken dat er geknoeid is.

Beschrijving van de hardware

Zie **figuur 1** voor het volledige schema van de verzendbox. Microcontroller IC1 is het hart van de schakeling. Elke twee seconden ontwaakt die uit de spaarstand en controleert in minder dan 50 ms verschillende parameters te controleren. Als die op een manipulatiepoging wijzen, wist de MCU veilig de SRAM-inhoud (inhoud met nullen overschrijven), iets wat niet mogelijk is met flash of EEPROM. Het openen van de box wordt op twee manieren gedetecteerd:

PROJECT-INFO



veilige communicatie

encryptie

IR communicatie

AVR



beginners

➔ gevorderden

experts



ca. 3 uur

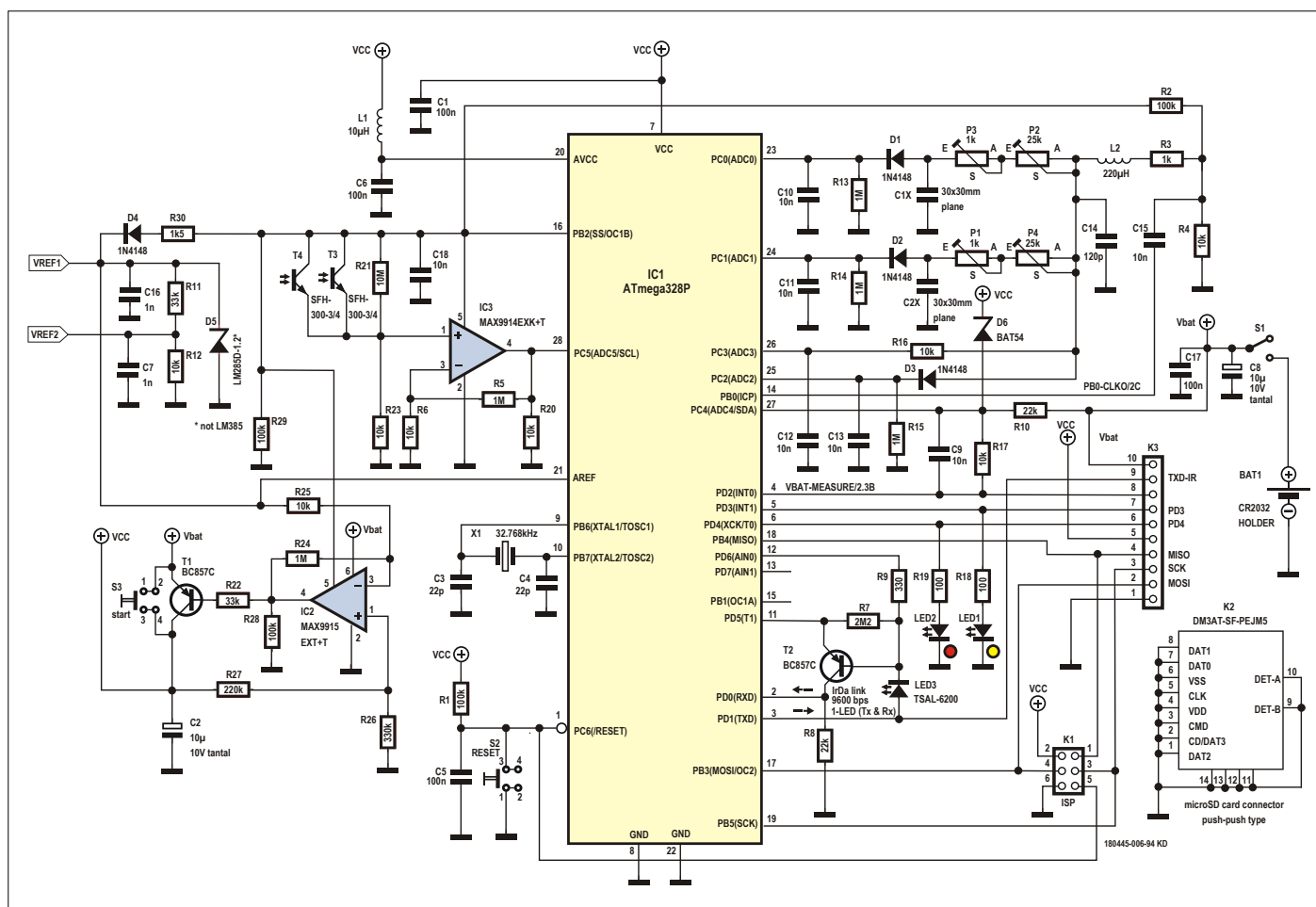


(SMD) soldeergereedschap,

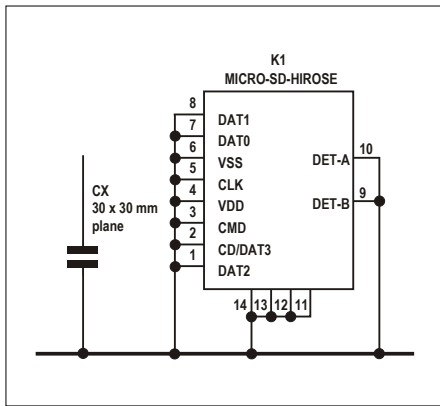
AVR-programmer



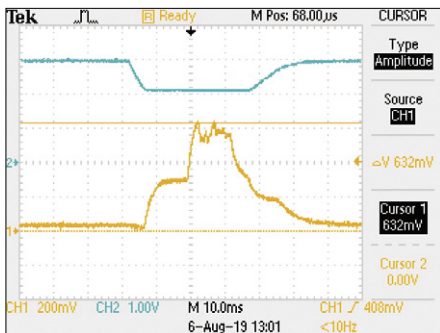
ca. € 50



Figuur 1. De verzendbox met manipulatie-indicatie maakt gebruik van fototransistoren en open plaatcondensatoren voor het detecteren van manipulatiepogingen.



Figuur 2. De open plaatcondensatoren C1x en C2x bestaan uit stukjes enkelzijdig printmateriaal van 30x30 mm. Er kan ook een microSD-cardhouder worden gemonteerd.



Figuur 3. Om stroom te sparen wordt de box slechts om de twee seconden wakker gedurende ongeveer 50 ms. De spanningsregelaar wordt geactiveerd (bovenste curve) om vitale parameters te meten. De onderste curve toont het stroomverbruik.

- verandering van capaciteit van de box (het moet een *metalen* box zijn). C1x en C2x (figuur 2) zijn open plaatcondensatoren die de tussengelegen SD-kaart 'beschermen'. De andere plaat is het metaal van de box zelf. Een capaciteitsverandering duidt op manipulatie;
- lichtdetectie. De doos is verzegeld en 100% lichtdicht; in de doos is het absoluut donker. Fototransistoren T3 en T4 detecteren infrarood en zichtbaar licht zodra de doos wordt geopend.

Voor het invoeren van de *challenge-and-response* codes wordt een IrDA-achtige infrarood link gebruikt. LED3 zorgt voor bidirectionele communicatie. Het maximale bereik is ongeveer een centimeter, maar dat is meer dan genoeg.

De schakeling wordt gevoed door een CR2032-knoopcel met een nominale spanning van 3 V. Deze gaat meer dan een maand mee (figuur 3), wat zelfs voor de traagste slakkenpost voldoende zou moeten zijn. Een nieuwe batterij begint meestal bij 3,3 V, en de schakeling werkt nog als die spanning is gedaald tot 2,1 V dankzij de *low-dropout* (LDO) spanningsregelaar die rond IC2 is opgebouwd en die een stabiele 2,0 V op V_{CC} levert.

D5 zorgt voor een nauwkeurige spanningsreferentie voor de A/D-omzetter (ADC) van de MCU. De LM285 is een variant van de LM385 maar met een groter temperatuurbereik, waardoor de schakeling veilig en met voldoende precisie functioneert van -20°C tot $+60^{\circ}\text{C}$ – temperaturen dus die bij verzending per post kunnen optreden.

De MCU wordt geklokt met zijn interne 1-MHz RC-oscillator. Om het energieverbruik tot een minimum te beperken, wordt deze klok slechts om de twee seconden ingeschakeld gedurende ongeveer 50 ms. De low power 32.768-kHz-klok op basis van horlogekrystal X1 loopt continu en maakt dit periodiek ontwakken mogelijk. Het signaal wordt ook gebruikt om de UART-klok van de MCU tijdens elke waakperiode af te regelen, en biedt ook de mogelijkheid de reisduur van de box precies te meten.

R3, L2 en C14 filteren de 1MHz-blokgolf (afkomstig van de MCU-klokuitgang op PB0) tot een sinus die kan worden gebruikt om de C1x- en C2x-capaciteiten nauwkeurig te meten. Zowel de piek als de gemiddelde waarden worden gemeten, en de verhoudingen van de AC-spanning op C1x en C2x ten opzichte van de AC-spanning op C14 worden berekend. Een significante verandering in een van deze verhoudingen duidt op sabotage.

LED1 en LED2 geven verschillende toestanden van het kastje aan. Zo knippert LED1 als er een juiste *challenge code* is ingevoerd en knippert LED2 als deze foutief is. Ze knipperen allebei één keer na het inschakelen. LED1 knippert één keer telkens als de MCU ontwaakt, omdat deze de LDO-uitgang helpt snel 2 V te bereiken. Als LED2 één keer knippert bij elke MCU-wakeup, dan is manipulatie gedetecteerd.

S1 is de aan/uit-schakelaar van de box en S2 is de resetknop van de MCU. Met drukknop S3 kan de schakeling worden opgestart als de batterijspanning een

beetje aan de lage kant is.

Merk op dat de print aan beide zijden van componenten is voorzien. Dat is om een deel van de schakeling te verbergen voor een kwaadwillende ogen, waardoor het moeilijker wordt om een goede plek te vinden voor het plaatsen van sondes of anderszins de werking te storen zonder de print te verwijderen. De open plaatcondensator aan de onderzijde detecteert dit.

De IR-communicatieadapter

Een infrarood (IR) link is beschikbaar voor de communicatie met de hermetisch verzegelde verzendbox. Deze verbinding is niet bijzonder snel (9.600 baud) en heeft een vrij gering bereik (1 cm), maar werkt zonder de doos te openen. De adapter (figuur 4 en figuur 5) die dit mogelijk maakt bestaat uit een kleine microcontroller, een ATtiny45, uitgerust met een IR-transceiver die vrijwel hetzelfde is als die in de box. De schakelingen verschillen enigszins door de low power-beperkingen van de box, die niet van toepassing zijn op de IR-adapter.

Aan de gebruikerszijde van de adapter zit een seriële poort. Omdat het invoeren van de *challenge-and-response* codes een veiligheidskritische procedure is, kan de IR-adapter op verschillende manieren met een computer worden verbonden, bijvoorbeeld via een USB/serieel-converter (kabel), via een 'echte' RS232-poort en zelfs via Ethernet als u een WIZnet WIZ107 Ethernet/serieel-adapter toevoegt. Deze opties maken het mogelijk om een goedkoop notebook te gebruiken die nooit verbinding maakt met het internet.

Afregelen van de capacatieve detectoren

Voor een goede werking van de capacatieve manipulatie-detectie moeten de trimpots P1, P2, P3 en P4 worden afgeregeld. Schakel de box in (LED2 knippert één keer, gevolgd door LED1) en zet de IR-LED van de adapter voor LED3 van de box op minder dan 1 cm afstand. Sluit de IR-adapter aan op een computer met een seriële aansluiting (9600n81). Na het intypen van 'U' (0x55) in de terminal, ziet u dit datablok elke twee seconden aankomen:

```
Box unlocked. Status-1. Define
challenge string.
Capacitor Cx1 voltage ratio: 0.703
Capacitor Cx2 voltage ratio: 0.703
```

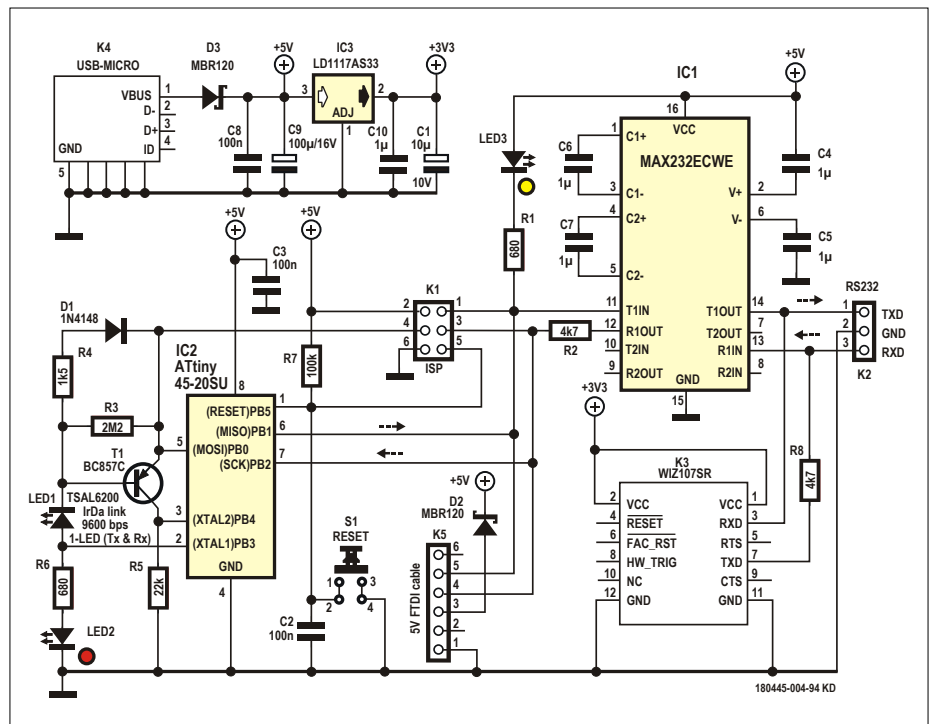
Phototransistor voltage [V]: 0.181
 Box temperature [degC]: +22
 Battery voltage [V]: 2.900

Voor maximale meetgevoeligheid moeten trimmers P1...P4 zo worden ingesteld dat de gecombineerde weerstand [P2+P3] gelijk is aan de reactantie C1x, en de som [P1+P4] gelijk is aan de reactantie C2x. Dit klinkt ingewikkeld, maar de statusgegevens bevatten spanningsverhoudingen om u hier te helpen. Ze moeten dicht bij $1/\sqrt{2}$ liggen, dus 0,707. Omdat de doos zelf fungeert als een condensatorplaat voor de open plaatcondensatoren C1x en C2x, moeten de spanningsverhoudingen kloppen als het deksel van de box gesloten is. Gebruik P2 en P4 voor grove afregeling en P1 en P3 voor de fijnregeling.

Temperatuurmetingen

De MCU heeft een ingebouwde temperatuursensor. De nauwkeurigheid is gering – ongeveer $\pm 5^\circ\text{C}$ – maar goed genoeg om abnormale temperaturen te detecteren en om de minimum- en maximumtemperaturen tijdens de reis van de box ruwweg te loggen. De temperatuur wordt gemeten door ADC-kanaal 8 (de interne thermometer van de MCU) in te lezen. Hoewel ontworpen om te werken met de interne spanningsreferentie van de MCU (1,1 V en niet erg stabiel), kan een externe spanningsreferentie (D5) worden gebruikt om dit te verbeteren als we er wat wiskunde tegenaangooien gooien (een zogenaamde affine functie). Op die manier kan een veel betere nauwkeurigheid worden verkregen dan in de datasheet van de MCU wordt vermeld. Indien nodig kan de helling van de affine functie binnen het programma worden aangepast, in de functie `measure_signals()`.

De temperatuursensor moet worden gekalibreerd om hem bruikbaar te maken. Hiervoor is het commando 'TP' beschikbaar, te versturen vanaf de terminal. De syntaxis is 'TPsxx' waarbij 's' het teken '+' of '-' is (het teken is verplicht) en 'xx' de offset is (als tweecijferige waarde, dus '00' tot '99'). Een voorbeeld:, als de waarde van 'Box temperature' +40 °C is terwijl de omgevingstemperatuur in werkelijkheid +25 °C is, dan moet u 'TP-15' versturen vanuit de terminal. Met 'TP+00' te sturen wordt de offset weer op nul gezet. De offset wordt opgeslagen in de interne EEPROM van de MCU.



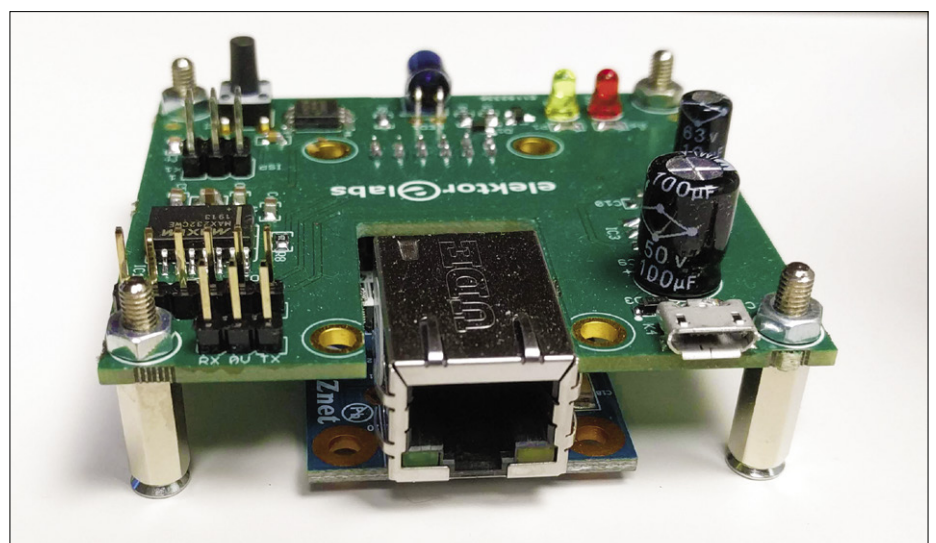
Figuur 4. De IR-communicatieadapter vormt een interface tussen de hermetisch afgesloten verzendbox en een computer.

Handleiding voor spionnen

Alice maakt met haar ERNG een bestand met toevalsgetallen aan en kopieert dit naar een nog niet eerder gebruikte SD-kaart. Ze zet een verse batterij in de box en schakelt de voeding in met S1. Omdat de batterij vers is, is het niet nodig om op S3 te drukken om de schakeling op te starten. Vervolgens steekt ze de SD-kaart in de houder en sluit ze de box. Met de IR-adapter voor de IR-LED van box stuurt ze eerst het karakter 'U' (0x55) vanaf haar terminal.

Hierdoor kan de MCU van de IR-adapter haar UART-klok kalibreren. De terminal zal dan de berichten van de box ontvangen met een resultaat als dit:

```
Box unlocked. Status-1. Define
challenge string.
Capacitor Cx1 voltage ratio: 0.710
Capacitor Cx2 voltage ratio: 0.704
Phototransistor voltage [V]: 0.181
Box temperature [degC]: +25
Battery voltage [V]: 3.354
```



Figuur 5. De IR-communicatieadapter met gemonteerde (optionele) Ethernet-module.

De box voert deze blokken met gegevens om de twee seconden uit op zijn infraroodpoort, behalve in status-3 en status-5. In die beide toestanden stoppen de datatransmissies na 60 seconden om stroom te besparen.

Status-1

Status-1 is de begintoestand van de box na het inschakelen; hij wacht op een *challenge string* op zijn infraroodontvanger. Alice voert de *challenge string* in de terminal in (maximaal 65 tekens, langere strings worden afgekapt). De box

komt dan in status-2.

Belangrijk: alle strings, inclusief commando's die uit meerdere tekens bestaan, moeten in de terminal met copy/paste worden ingevoerd en niet karakter voor karakter worden getypt!

Box unlocked. Status-2. Define

response string.

Capacitor Cx1 voltage ratio: 0.710

Capacitor Cx2 voltage ratio: 0.704

Phototransistor voltage [V]: 0.181

Box temperature [degC]: +25

Battery voltage [V]: 3.354

Status-2

De box wacht op de invoer van een *response string*. De spanningsverhoudingen van Cx1 en Cx2 en de fototransistorspanning zijn opgeslagen in het SRAM van de MCU. Als deze spanningen tijdens de reis te veel veranderen, wordt een manipulatie-waarschuwing gegeven. Alice voert de *response string* in (tot 65 karakters) om de box op scherp te zetten en te vergrendelen en in status-3 te brengen. De reistijd klok wordt ook gestart. Alice noteert de datum en het exacte tijdstip, samen met de *challenge*



ONDERDELENLIJST

verzendingbox met manipulatie-indicatie

Weerstanden:

(alle 0805 tenzij anders vermeld)

R18,R19 = 100Ω

R9 = 330Ω

R3 = 1k

R30 = 1k5

R4,R6,R12,R16,R17,R20,R23,R25 = 10k

R8,R10 = 22k

R11,R22 = 33k

R1,R2,R29,R28 = 100k

R27 = 220k

R26 = 330k

R5,R13,R14,R15,R24 = 1M

R7 = 2M2

R21 = 10M

P3,P1 = instelpotmeter 1k

P2,P4 = instelpotmeter 25k

Condensatoren:

(alle 0805 tenzij anders vermeld)

C3,C4 = 22p

C14 = 120p

C7,C16 = 1n

C9,C10,C11,C12,C13,C15,C18 = 10n

C1,C5,C6,C17 = 100n

C2,C8 = 10μ/10V, tantaal, steek 2mm

Spoelen:

L1 = 10μH (0805)

L2 = 220μH (1812)

Halfgeleiders:

D1,D2,D3,D4 = 1N4148WS (SOD-323)

D5 = LM285D-1.2V

D6 = BAT54

IC1 = ATmega328P-PU (geprogrammeerd)

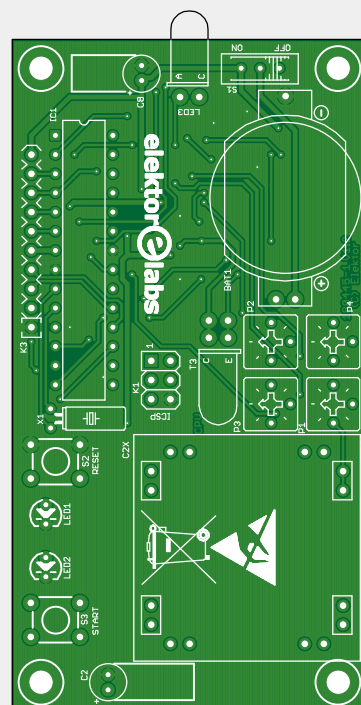
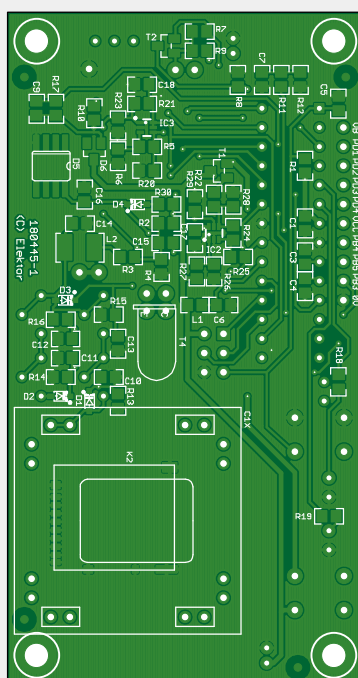
IC2 = MAX9915EXT+T

IC3 = MAX9914EXK+T

LED1 = 3mm, geel

LED2 = 3mm, rood

LED3 = TSAL6200



T1,T2 = BC857C

T3,T4 = SFH-300-3/4

Diversen:

BAT1 = batterijhouder, 2032, bijv. Renata HU2032

C1x,C2x = 2-polige pinheader + busstrip voor C1x & C2x, raster 0,1"

K1 = 6-polige (2x3) pinheader, raster 0,1"

K2 = microSD cardhouder, push-push

K3 = 10-polige pinheader, raster 0,1"

S1 = schuifschakelaar, SPDT

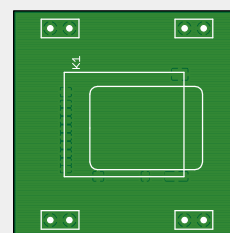
S2,S3 = druktoets, 6x6mm

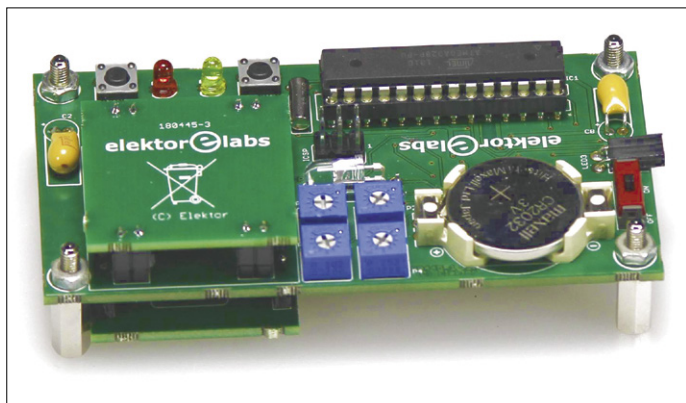
X1 = 32.768kHz kristal

LED-houder voor LED3 (dicht)

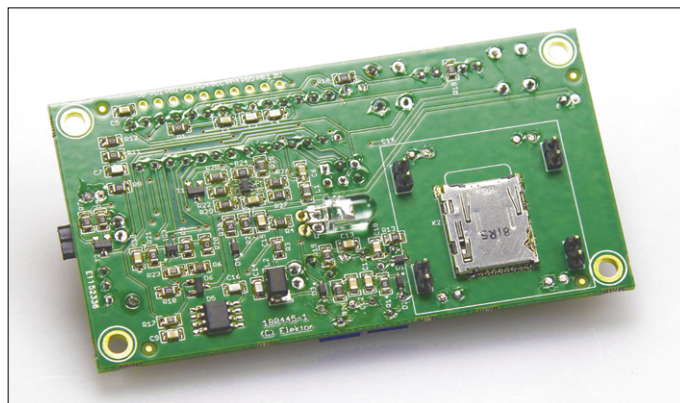
print #180445-1

print #180445-3 (2 stuks)





Figuur 6. De volledig gemonteerde print met aan beide zijden de open plaatcondensatoren.



Figuur 7. Aan de onderkant van de print zijn SMD-componenten gemonteerd, alsmede de through-hole transistor T4 die er als een LED uit ziet. Condensator C1x wordt boven de microSD-cardhouder gemonteerd.

en *response strings* en bergt dit alles veilig op (in haar geheugen, indien mogelijk). Het zal later worden gebruikt voor verificatie. Vervolgens verstuurt ze de box per post naar Bob.

```
Box locked. Status-3. Enter
challenge string to unlock.
Capacitor Cx1 voltage ratio: 0.710
Capacitor Cx2 voltage ratio: 0.704
Phototransistor voltage [V]: 0.181
Box temperature [degC]: +25
Battery voltage [V]: 3.354
```

Status-3

De challenge-and-response-strings zijn ingevoerd, de box staat op scherp en is vergrendeld. Bij manipulatiepogingen of vijfmaal het invoeren van een onjuiste *challenge string* wordt het proces van *zeroisation* (met nullen overschrijven) gestart. De box blijft tijdens de gehele reis per postbode in status-3.

De SRAM-buffers met de *challenge-and-response-strings* worden om de twee seconden gecomplementeerd (bitgewijs geïnverteerd). Op deze manier wordt de parasitaire burn-in van SRAM-cellen [4] voorkomen, omdat elk bit even veel tijd in de '0'- en in de '1'-toestand verkeert.

Bij Bob

Na een lange en hachelijke reis komt de box (hopelijk) bij Bob aan. Hij sluit zijn IR-adapter aan op een computer, zet deze voor de IR-LED van de box en drukt op de reset-knop op de adapter. De adapter produceert dan een 3 seconden durende puls op de IR-poort om de box op te dragen dat zijn IR-poort te activeren en met de communicatie te beginnen. Na die drie seconden verzendt

Bob het teken 'U' om de UART van de IR-adapter te kalibreren, en zal de terminal gegevens gaan weergeven:

```
Box locked. Status-3. Enter
challenge string to unlock.
Capacitor Cx1 voltage ratio: 0.703
Capacitor Cx2 voltage ratio: 0.711
Phototransistor voltage [V]: 0.175
Box temperature [degC]: +23
Battery voltage [V]: 2.752
```

We zien dat de batterijspanning is afgenomen, maar er zijn geen zichtbare tekenen van manipulatie omdat de Cx-spanningsverhoudingen en de waarde van de fototransistorspanning niet veel zijn veranderd. Bob belt Alice op en vraagt haar om de *challenge string*. Hij voert die in zijn terminal in, en als alles in orde is zal hij dit zien:

```
Box unlocked. Status-4. Challenge
string correct!!
Capacitor Cx1 voltage
ratio: 0.703
Capacitor Cx2 voltage ratio: 0.711
Phototransistor voltage [V]: 0.178
Box temperature [degC]: +24
Battery voltage [V]: 2.752
Min temperature [degC]: -2
Max temperature [degC]: +31
Travel time [s]: 502,164
Response:
Trust no one 01a2g23w46e57f80g12r
3e34fv245hasdvfr4.
```

Status-4

Bob schrijft onmiddellijk de huidige tijd en datum op en belt Alice opnieuw op om de *response string* te verifiëren. Als Alice

die accepteert, vertelt ze Bob de exacte tijd en datum die ze heeft opgeschreven toen ze de box op slot deed. Zo kan Bob de theoretische reistijd berekenen en deze vergelijken met de werkelijke tijd die door de box is gemeten. Als de twee overeenkomen, dan mag Bob de OTP-sleutel gebruiken die op de microSD-kaart is opgeslagen om zijn beveiligde communicatie met Alice te versleutelen en te ontcijferen. Als er onderweg mee geknoeid is, zal de box het deel van het SRAM met de codes en de reistimer wissen. In dat geval zal de box iets in deze geest melden:

```
Box zeroized. Status-5. Tampering,
wrong password, or low battery!
Capacitor Cx1 voltage ratio: 0.712
Capacitor Cx2 voltage ratio: 0.713
Phototransistor voltage [V]: 0.179
Box temperature [degC]: +12
Battery voltage [V]: 2.793
```

Status-5

Omdat er een manipulatiepoging was gedetecteerd of nadat er vijf maal een ongeldige *challenge string* was ingevoerd, is de inhoud gewist (met nullen overschreven). De spanningswaarden om manipulatie te detecteren worden niet meer bijgewerkt, zodat de ontvanger van de box de laatst opgeslagen toestand kan zien voordat manipulatie werd gedetecteerd.

Het op nul zetten wordt uitgevoerd in een van de volgende gevallen:

- na vijf keer invoeren van een foutieve *challenge string*;
- de werkelijke spanningsverhouding van de condensatoren verschilt te

- veel van de geregistreerde waarde;
- de werkelijke fototransistorspanning wijkt te veel af van de geregistreerde waarde;
- de batterijspanning is te laag (onder 2,1 V);
- extreme temperaturen gemeten (minder dan -20 °C of meer dan +60 °C).

Om te voorkomen dat status-3 door strooilicht wordt getriggert, moet de box lichtdicht gesloten zijn. Breng wat zwarte kit aan rond LED3 aan de binnenkant van de box en maak de randen van de box met zwarte isolatietape lichtdicht. Test uw werk door de gesloten doos (in status-3) aan direct sterk zonlicht bloot te stellen. Nu kan Bob het commando 'DE' invoeren om te zien waarom de inhoud gewist is:

```
Box zeroized. Status-6. Tampering
status display!
Capacitor Cx1 voltage ratio: 0.683
Capacitor Cx2 voltage ratio: 0.656
Phototransistor voltage [V]: 0.188
Box temperature [degC]: +10
Battery voltage [V]: 2.775
Min temperature [degC]: -5
Max temperature [degC]: +30
Cause of zeroization:
Capacitor Cx2. kCx2= 0.656
```

Status-6

Na ontvangst van het 'DE'-commando

zal de box details over de oorzaak van het wissen doorgeven.

De gegevens die worden weergegeven in status-5 of status-6 hoeven niet geldig te zijn, aangezien dit afhangt van wat eventuele onverlaten met de box hebben uitgespookt. Het kan zijn dat de box is gereset en *challenge* en *response strings* zijn ingevoerd voordat de box in status-3 naar Bob is doorgestuurd. Maar zelfs als ze er op de een of andere manier zijn geslaagd om de juiste tekenreeksen in te voeren, zal de reistimer ook moeten worden bedot, en dat is veel moeilijker.

Terug naar status-1

Met het commando 'RE' kan de box worden gereset naar status-1 zonder deze te openen. Het indrukken van de S2-resetknop in de box doet hetzelfde.

Over hardware-Trojanen gesproken

Aangezien de meeste mensen zich meestal alleen zorgen maken over software-malware en Trojanen die hun computers aanvallen, zijn hier enkele opmerkingen over hardware-Trojanen op hun plaats. Een eenvoudig systeem met een enkele MCU die nooit met het internet is verbonden, is 100% veilig tegen de typische malware die tegen uw PC of smartphone is gericht. Zie [5] voor principiële informatie over de problemen met sterk geïntegreerde solid-state geheugens.

Een hardware backdoor-Trojaan bestaat uit extra schakelingen die zijn toegevoegd aan de halfgeleiderchip van de MCU. Dit kan net zo schadelijk zijn als een softwarematige Trojaan – of zelfs nog gevaarlijker. Het vormt een groot gevaar voor de huidige MCU's met hun CPU, SRAM, EEPROM en flash-geheugen geïntegreerd op één plakje silicium, en die met een lage spanning (3...5 V) geprogrammeerd kunnen worden. In principe zijn er twee soorten:

1: general-purpose Trojanen

Een kwaadwillende kan een hardware-Trojaan in de MCU aanbrengen, bijvoorbeeld om periodiek het SRAM en de registers van de MCU te kopiëren naar een geheim deel van het flashgeheugen. Ongeacht de toepassing van de MCU zal een 'bevroren' momentopname van het RAM altijd van pas komen. Met zo'n Trojaan op zijn plaats kunnen de door Alice gedefinieerde *challenge-and-response strings* eenvoudig worden uitgelezen. Het bedotten van de reistimer zal echter iets moeilijker blijken.

2: toepassings specifieke hardware Trojanen

Om dit soort hardware Trojanen te planten, moet een kwaadwillende eerst kennis hebben over de firmware van de MCU. Vervolgens voorziet hij de MCU van een schakeling die in staat is om de firmware te herkennen die Alice in



ONDERDELENLIJST

IR-adapter

Weerstanden:

(alle 0805 tenzij anders vermeld)

R1,R6 = 680Ω

R4 = 1k5

R2,R8 = 4k7

R5 = 22k

R7 = 100k

R3 = 2M2

Condensatoren:

(alle 0805 tenzij anders vermeld)

C2,C3,C8 = 100n

C4,C5,C6,C7,C10 = 1μ, X7R, 50V

C1 = 10μ/10V, tantaal, steek 2mm

C9 = 100μ/16V, steek 3,5mm

Halfgeleiders:

D1 = 1N4148WS (SOD-323)

D2,D3 = MBR120

IC1 = MAX232ECWE

IC2 = ATtiny45-20SU (geprogrammeerd)

IC3 = LD1117AS33

LED1 = TSAL6200

LED3 = 3mm, geel

LED2 = 3mm, rood

T1 = BC857C

Diversen:

K1 = 6-polige (2x3) pinheader, raster 0,1"

K2 = 3-polige pinheader, raster 0,1"

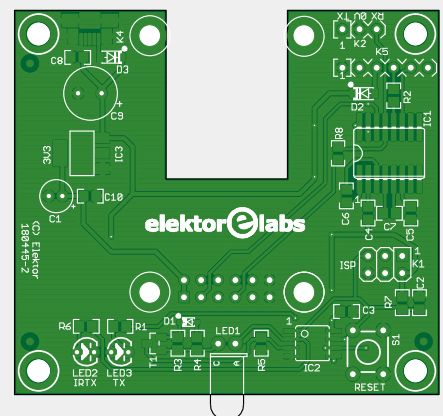
K3 = 12-polige (2x6) busstrip, raster 0,1"

K4 = micro USB-connector type B

K5 = 6-polige pinheader, steek 0,1"

S1 = druktoets, 6x6mm

WIZ107 Ethernet-module



print #180445-2

de MCU heeft geflasht. Bij het starten van de MCU zal de Trojaan als een bootloader fungeren en enkele regels in het programma van de MCU wijzigen (bijvoorbeeld vullen met NOP's met behulp van het beruchte SPM-commando van de AVR) om bijvoorbeeld een aantal cruciale beschermende acties uit te schakelen. De kans op een succesvolle aanval van dit type is veel kleiner dan bij een 'algemene' Trojaan.

Is verdediging mogelijk?

Gelukkig voor Alice en Bob zijn er veel manieren om dit soort hardwarebedreigingen tegen te gaan. De eenvoudigste is om terug te keren naar de technologie van de jaren '80 en een eenvoudig Z80-systeem te gebruiken zoals [6] met SRAM en EPROM als afzonderlijke IC's. De EPROM wordt gewist met UV-licht en heeft een spanning van 13...14 V op de V_{pp} -pen nodig om geschreven te worden, wat het veel moeilijker maakt om een hardware-backdoor aan te brengen. Bovendien is de interne architectuur van de Z80 en 27C-type EPROM's (waarvan er gedurende meer dan 20 jaar vele miljoenen zijn geproduceerd) zeer bekend en is het eenvoudig om het IC open te maken en indien nodig onder een microscoop te inspecteren. Met miljoenen exemplaren wereldwijd is het onmogelijk die allemaal te 'prepareren'.

Het porten van de MCU-firmware van de ERNG of OTP Crypto-Shield naar een Z80 kan ten koste gaan van de uitvoeringssnelheid en de fysieke grootte, maar de systemen zouden nog steeds prima werken. En er heerst tegenwoordig nog een andere ontwerp-misvatting: kleine, mini-, micro- en nano-apparaten zijn niet altijd beter!

Natuurlijk zou een Z80-gebaseerd systeem te lomp en energievretend zijn om voor de verzendbox te gebruiken, maar dit probleem kan op een andere

manier worden opgelost, met een beetje extra elektronica, en alles zou nog prima in de box passen. Wanneer u de schema's zorgvuldig bestudeert, vraagt u zich wellicht af wat de functie van K3 is. Die is bedoeld voor een latere uitbreiding om de box te beschermen tegen hardware Trojanen. Meer hierover in een later artikel in Elektor – reden genoeg om het blad te blijven lezen!

Tot slot

Het prototype van de box zoals op de foto's te zien is, is verschillende malen met verschillende postmaatschappijen verstuurd en bleek goed te functioneren. Sommige bedrijven springen echter ruwer om met pakjes dan andere en het bleek nodig om C1x en C2x zo vast te zetten dat ze niet kunnen losraken. Dat kan bijvoorbeeld met niet-geleidend schuimplastic. Als de MCU in een voetje is gemonteerd, dan wilt u die wellicht ook vastzetten. De batterij zit vrij weliswaar stevig in de houder, maar je weet maar nooit.

Als u andere suggesties heeft voor het verbeteren van het apparaat zoals beschreven in dit artikel, met name met betrekking tot de verdediging tegen een hardware-backdoor, neem dan contact met mij op via de projectpagina bij



Eindelijk ontmoeten Bob en Alice elkaar persoonlijk.

Elektor Labs [7]. Ik heb zelf een paar ideeën, maar u hebt misschien betere ideeën, en andere methoden kunnen altijd worden overwogen. Om de veiligheid te bevestigen, moet elk crypto-apparaat worden beoordeeld door een aantal onafhankelijke deskundigen, dus neem deel – op welke manier dan ook! Zoals gewoonlijk kunnen de ontwerpbestanden en de broncode voor dit project worden gedownload van de Labs-pagina van het project [7]. ◀

180445-04



IN DE STORE

→ Verzendbox – set met alle kale printen
www.elektor.nl/180445-1

→ Verzendbox – geprogrammeerde microcontroller ATmega328P-PU
www.elektor.nl/180445-41

→ IR-adapter – geprogrammeerde microcontroller ATtiny45-20SU
www.elektor.nl/180445-42

Weblinks

- [1] Random Number Generator: www.elektormagazine.com/labs/random-number-generator-150116
- [2] One-Time Pad (OTP) Crypto Shield: www.elektormagazine.com/labs/one-time-pad-otp-crypto-system
- [3] Data wissen van flash-drives: www.schneier.com/blog/archives/2011/03/erasing_data_fr.html
- [4] Remanentie van data in halfgeleiders: www.usenix.org/legacy/events/sec01/full_papers/gutmann/gutmann.pdf
- [5] Elektor video-interview over veiligheid: www.elektormagazine.com/news/secure-communications-an-interview-with-luka-matic
- [6] Een kleine en simpele Z80-computer: www.sunrise-ev.com/z80.htm
- [7] Verzendbox met manipulatie-indicatie:
www.elektormagazine.com/labs/tamper-evident-paper-mail-box-for-secure-distribution-of-one-time-pads