boîte inviolable
protégée par un témoin d'effraction
Envoyer des données en toute sécurité par la poste

Luka Matić (Croatie)

Dans les systèmes de communication sécurisés basés sur des blocs-notes numériques à usage unique, les messages sont cryptés et décodés à l'aide d'une clé aléatoire. Pour que cela fonctionne, l'expéditrice, appelée Alice par convention, et le destinataire, appelé Bob ou Bernard, doivent utiliser la même clé. Si Alice produit la clé, comment l'envoie-t-elle à Bob de manière sécurisée ? C'est à ce problème de la poule et de l'œuf que s'attaque cet article. Jouissif !

Caractéristiques

- Code source ouvert sans astuces cachées
- Détection capacitive d'ouverture de boîte
- Détection lumineuse d'ouverture intempestive
- Vérification du temps de voyage
- Détection des attaques de température
- Communication infrarouge
- Réutilisable

Ce projet est la suite (logique) de mon TRNG [1] et de mon OTP Crypto Shield [2] et tente de résoudre le problème de l'échange sécurisé de clés OTP (*one-time pads* ou OTP), stockées p. ex. sur une carte SD. J'ai commencé par l'idée de concevoir un dispositif inviolable, mais j'ai ensuite appris qu'il est pratiquement impossible d'effacer en toute sécurité les données d'un dispositif à mémoire flash comme une mémoire de masse à semi-conducteurs (SSD) ou une carte SD [3]. De plus, même la mémoire SRAM présente des effets parasites de *brûlage* ou de rémanence, permettant de récupérer les données qu'elle contient [4]. C'est dans cet esprit que j'ai renoncé à construire une boîte inviolable, pour en concevoir une qui indiquera qu'elle a été crochetée.

Principe de fonctionnement

Alice stocke une clé OTP fraîchement produite sur une carte microSD et la met dans une boîte qu'elle ferme. Elle

l'arme en y stockant une chaîne dite de défi et de réponse (*challenge-and-response string*) au moyen d'une liaison sans contact (infrarouge). Elle envoie la boîte à Bob par la poste. Lorsqu'il la reçoit, il demande à Alice la chaîne de défi. Pour cela, il utilise n'importe quel canal *non sécurisé*, le téléphone p. ex. ou le courriel, car seule Alice connaît cette chaîne et Bob a la boîte. Bob déverrouille la boîte en lui envoyant la chaîne de défi par la liaison optique. La boîte répondra soit avec la chaîne de réponse, soit avec l'avertissement d'une éventuelle tentative d'intrusion. Seule Alice peut confirmer la validité de la chaîne de réponse. Si la chaîne de réponse est incorrecte, ou si la boîte émet un avertissement de sabotage, Bob jette simplement la carte SD et n'utilisera pas pour des communications sécurisées avec Alice la clé de ce bloc-notes OTP potentiellement dangereuse.

Si la boîte est ouverte sans avoir été désarmée au préalable à l'aide de la chaîne de défi, ou si elle est crochetée d'une autre manière, elle effacera en toute sécurité les chaînes défi-réponse de sa mémoire. Ève, qui **é**coute aux portes, ou Mallory, qui est **m**alveillante, peuvent intercepter la boîte, lire et copier la carte SD, puis transmettre la boîte à Bob, mais ils ne peuvent pas réarmer la boîte avec les mêmes chaînes défi-réponse que seule Alice connaît, et Bob finira donc par le découvrir.

Description du matériel

Sur la **fig. 1** au cœur du schéma de la boîte, le µC IC1 est le cerveau de l'appareil. Toutes les deux secondes, il se réveille du mode de veille pendant moins de 50 ms pour vérifier plusieurs paramètres. Si ces paramètres indiquent une intrusion, le µC efface (met à zéro) de manière sécurisée le contenu de sa SRAM, ce qui n'est pas possible avec une mémoire flash ou une EEPROM.

L'ouverture de la boîte est détectée de deux façons :

- Modification de la capacité de la boîte (il doit s'agir d'une boîte métal-

INFOS SUR LE PROJET

communication sécurisée
cryptage
communication IR AVR

débutant
connaisseur
expert

±3 h

fer à souder (CMS), programmateur AVR

±50 €.

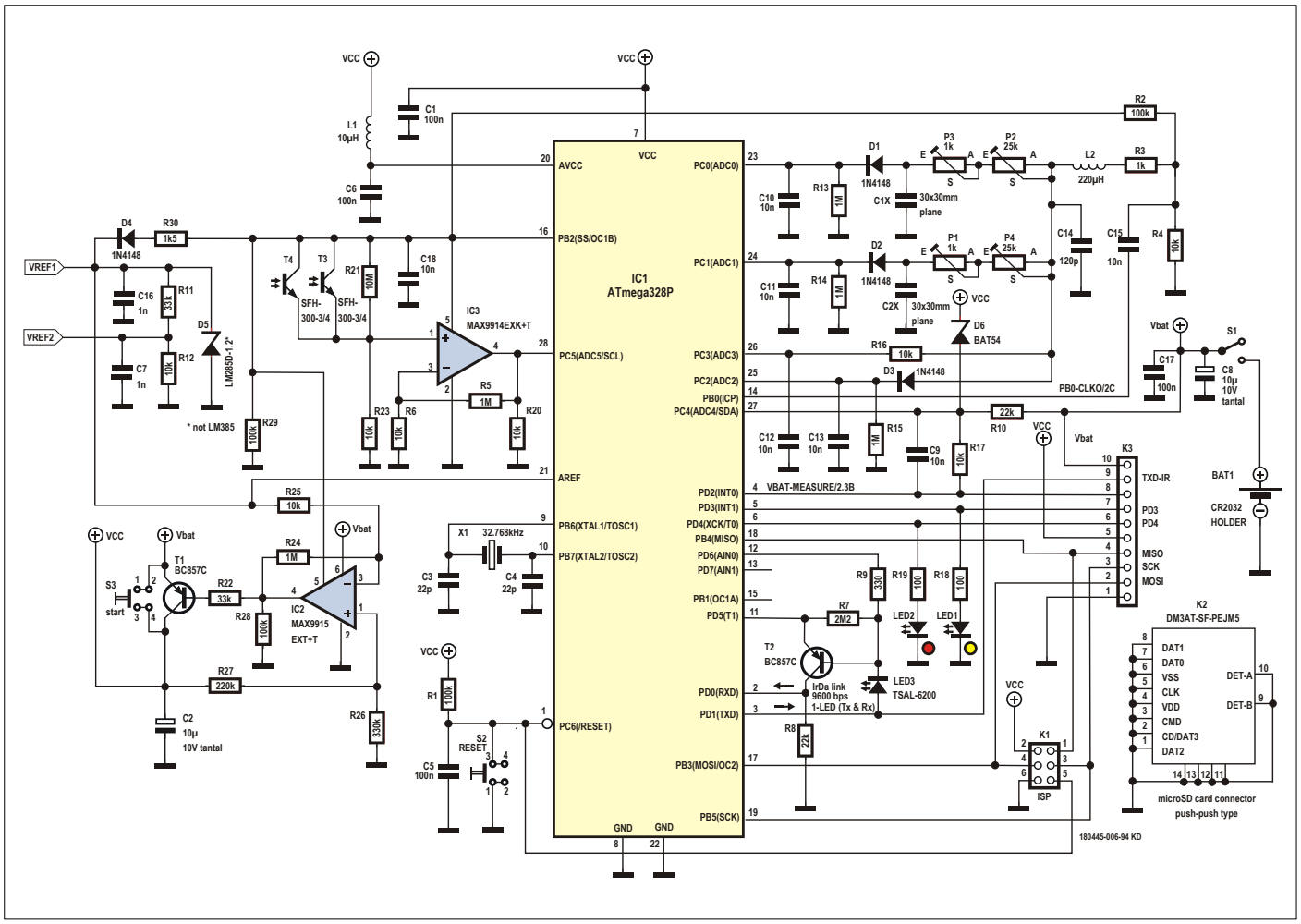


Figure 1. La boîte protégée par un témoin d'effraction utilise des phototransistors et des condensateurs à plaque ouverte pour détecter les effractions.

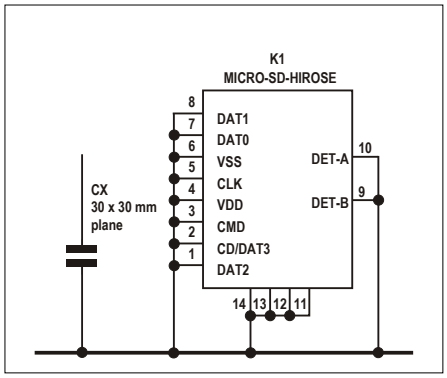


Figure 2. Les condensateurs à plaque ouverte C1x et C2x sont des plaques cuivrées de 30 x 30 mm (matériau pour PCB simple face). Un connecteur de carte microSD peut également être monté.

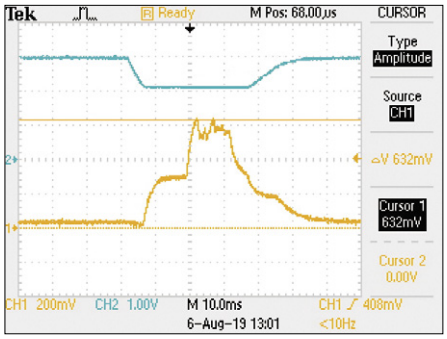


Figure 3. Pour limiter sa consommation, la boîte ne se réveille que toutes les deux secondes pendant environ 50 ms. Le régulateur de tension est activé (trace supérieure) pour mesurer les paramètres de surveillance d'intrusion. La trace du bas indique la consommation de courant.

lique). C1x et C2x (**fig. 2**) sont des condensateurs à plaque ouverte qui protègent la carte SD placée entre eux. Leur autre plaque est la paroi métallique (!) de la boîte : toute modification de leur capacité = intrusion.

- Détection de la lumière. La boîte scellée est étanche à la lumière ; il y fait noir. Les phototransistors T3 et T4 détectent l'un la lumière infrarouge et l'autre la lumière visible aussitôt que la boîte est ouverte.

La LED3 infrarouge IrDA assure les communications bidirectionnelles pour les codes défi-réponse. Sa portée est d'environ 1 cm, c'est peu mais c'est assez.
Le circuit est alimenté par une pile CR2032 (3 V). Elle durera plus d'un mois (**fig. 3**), ce qui devrait suffire même si le facteur fait sa tournée à pied. La tension d'une telle pile neuve est généralement de 3,3 V. Ce circuit fonctionnera jusqu'à 2,1 V, grâce au régulateur de tension à faible perte (LDO) autour de IC2, qui produit une tension V_{cc} stable de 2,0 V. D5 fournit une référence de tension précise pour le convertisseur analogique-numérique (ADC) du µC. Le LM285 est une variante à plage de température étendue du LM385, ce qui permet au circuit de fonctionner en toute sécurité avec une précision suffisante de -20 °C à +60 °C, c'est-à-dire les températures que l'on peut rencontrer lors d'un périple par courrier postal.
Le µC est cadencé par son oscillateur RC interne de 1 MHz. Pour réduire la consommation, cette horloge n'est allumée que toutes les 2 s pendant environ 50 ms. L'horloge à faible consommation de 32,768 kHz, calée sur le quartz horloger X1, fonctionne en continu et chronomètre ces moments de réveil. Elle est également utilisée pour régler l'horloge UART du µC à chaque réveil, et fournit la base de temps pour mesurer précisément la durée du voyage de la boîte.
R3, L2 et C14 filtrent l'onde carrée de 1 MHz dérivée de la sortie d'horloge du µC sur PB0, pour obtenir une onde sinusoïdale utilisable pour mesurer avec précision les capacités C1x et C2x. On mesure les valeurs de crête et moyennes et on calcule les rapports de la tension alternative sur C1x et C2x par rapport à la tension alternative sur C14. Un changement significatif de l'un de ces rapports est le signe d'une intrusion.
LED1 et LED2 indiquent les différents états de la boîte. LED1 clignote lorsqu'un code de défi correct a été saisi. LED2 clignote s'il est incorrect. Elles clignotent une fois toutes les deux après la mise sous tension. LED1 clignote une fois à chaque réveil du µC, car elle est utilisée pour aider la sortie LDO à atteindre rapidement 2 V. Si LED2 clignote une fois à chaque réveil du µC, c'est qu'un sabotage a été détecté.
L'interrupteur S1 est l'interrupteur d'alimentation du boîtier, et S2 est le bouton de réinitialisation du µC. Le bouton S3 permet de redémarrer le circuit au cas où la tension de la batterie serait un peu trop faible.
Notez qu'il y a des composants des deux côtés de la carte. L'idée est de cacher une partie du circuit à un intrus, notamment les bons endroits pour placer des sondes ou interférer autrement sans retirer le PCB, ce que le condensateur à plaque ouverte du bas détecterait aussitôt.

Interface IR

Une liaison infrarouge (IR) est disponible pour communiquer avec la boîte inviolable quand elle est hermétiquement fermée. Cette liaison n'est pas particulièrement rapide (9600 bauds) et sa portée est courte (1 cm). Elle fonctionne sans qu'il soit nécessaire d'ouvrir la boîte. L'adaptateur (**fig. 4** et **fig. 5**) qui rend cela possible est constitué d'un petit µC ATtiny45, équipé d'un émetteur-récepteur IR presque identique à celui de la boîte. Les circuits diffèrent légèrement en raison des contraintes de faible puissance de la boîte, lesquelles ne s'appliquent pas à l'adaptateur IR.
Côté utilisateur de l'adaptateur, il y un port série. Comme la saisie des codes de défi-réponse est critique pour la sécurité, l'adaptateur IR peut se connecter à un ordinateur de différentes manières, p. ex. par un convertisseur USB-série (câble), par un «vrai» port RS-232, et même par Ethernet si vous ajoutez un adaptateur WIZnet WIZ107 Ethernet-série. Ces options permettent de réserver à la communication avec cette boîte un PC portable bon marché qui ne se connecterait jamais à l'internet.

Ajustement des détecteurs capacitifs

Pour garantir la fiabilité de la détection de sabotage capacitive, les ajustables P1, P2, P3 et P4 doivent être réglés. Mettez le boîtier sous tension (la LED2 clignotera une fois, suivie de la LED1) et placez la LED IR de l'adaptateur IR devant la LED3 du boîtier à moins de 1 cm. Connectez l'adaptateur IR à un ordinateur équipé d'un terminal série (9600n81). Après avoir tapé «U» (0x55) dans le terminal, vous verrez ce bloc de données arriver toutes les deux secondes :

```
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
```

Pour une sensibilité maximale, P1 à P4 doivent être réglés de telle sorte que la résistance combinée [P2+P3] soit égale à la réactance C1x, et que la somme [P1+P4] soit égale à la réactance C2x. Cela semble compliqué, mais les données d'état contiennent des rapports de tension pour vous aider ici. Ils doivent

être proches de 1/√2, c'est-à-dire 0,707. Comme la boîte elle-même sert de plaque de condensateur pour les condensateurs à plaque ouverte C1x et C2x, les rapports de tension doivent être corrects avec le couvercle de la boîte en place. Utilisez P2 et P4 pour les réglages grossiers et P1 et P3 pour les réglages fins.

Mesures de la température

Le µC est équipé d'un capteur de température intégré. Sa précision est médiocre (±5°C) mais suffisante pour détecter des températures anormales et pour enregistrer les températures minimales et maximales approximatives pendant le voyage de la boîte. La température est mesurée par la lecture du canal 8 de l'ADC, qui est le thermomètre interne du µC. Bien que conçu pour fonctionner avec la référence de tension interne du µC (1,1 V et pas très stable), si l'on ajoute un peu de mathématiques (une fonction *affine*), une référence de tension externe (D5) peut être utilisée pour améliorer les choses. On obtient ainsi une précision bien meilleure que celle indiquée dans la fiche technique du µC. Si nécessaire, la pente de la fonction *affine* peut être modifiée à l'intérieur du programme, dans la fonction `measure_signals()`.
Pour qu'il puisse servir, le capteur de température doit être calibré avec la commande «TP», à envoyer depuis le terminal. Sa syntaxe est «TPsxx» où «s» est le signe «+» ou «–» (le signe est obligatoire), et «xx» est le décalage (sous forme de valeur à 2 chiffres, c'est-à-dire de «00» à «99»). Par exemple, si la valeur de la «température de la boîte» est de +40°C alors que la température ambiante est réellement de +25°C, vous devez envoyer «TP-15» depuis le terminal. Pour remettre le décalage à zéro : «TP+00». Le décalage est stocké dans l'EEPROM interne du µC.

Manuel pour les espions

Alice crée un fichier de nombres aléatoires avec son TRNG et le copie sur une carte SD jamais utilisée. Elle insère une pile neuve dans la boîte et l'allume avec S1. Comme la pile est fraîche, il ne sera pas nécessaire d'appuyer sur S3 pour faire démarrer l'appareil. Puis Alice met la carte SD dans la prise et ferme la boîte. Avec l'adaptateur IR en face de la LED IR du boîtier, elle envoie d'abord le caractère «U» (0x55) de son terminal. Cela permet au µC de l'adaptateur IR de calibrer son horloge UART. Le terminal

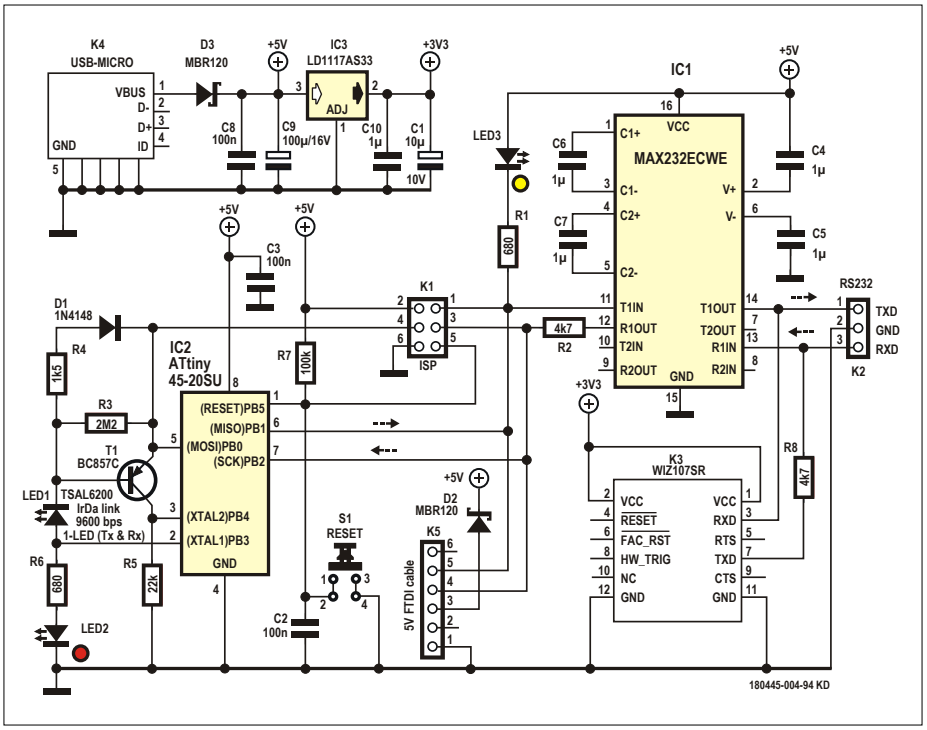


Figure 4. L'adaptateur de communication IR fournit une interface entre le boîtier inviolable hermétiquement fermé et un ordinateur.

commencera à recevoir des messages de la boîte, affichant quelque chose de ce genre :

```
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
```

Le boîtier émet ces blocs de données toutes les deux secondes sur son port infrarouge, sauf dans les états 3 et 5. Dans ces états, les transmissions de données s'arrêtent après 60 s pour économiser l'énergie.

Statut 1

L'état 1 est l'état initial du boîtier après la mise sous tension, et l'appareil attend qu'une chaîne de défi arrive sur son récepteur infrarouge. Alice saisit la chaîne de défi dans le terminal (jusqu'à 65 caractères, les chaînes plus longues sont

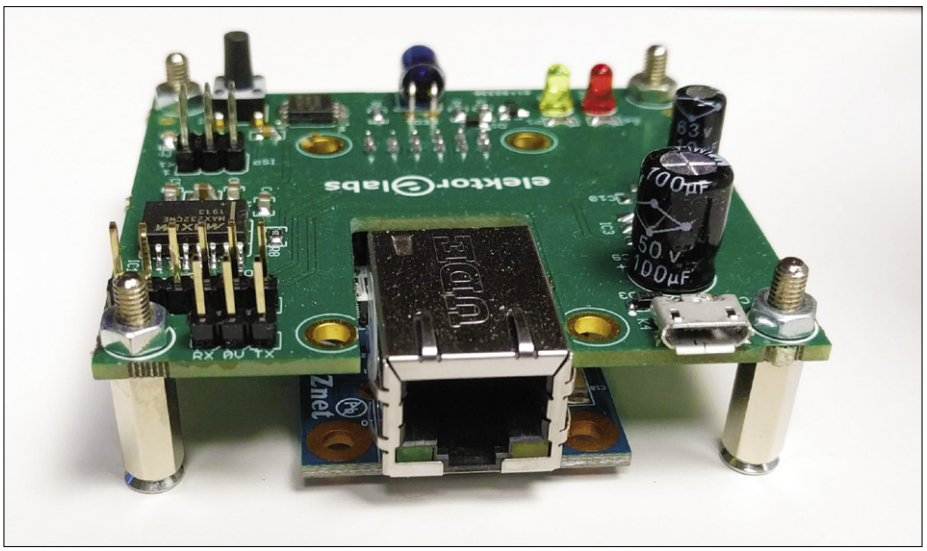


Figure 5. L'adaptateur de communication IR avec le module Ethernet (en option) monté.

tronquées). La boîte passe alors à l'état 2. *Remarque importante : toutes les chaînes de caractères, y compris les commandes à plusieurs caractères, doivent être copiées dans le terminal et non tapées caractère par caractère !*

```
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
```

Statut 2

La boîte attend qu'une chaîne de réponse soit saisie. Les rapports de tension de Cx1 et Cx2 et la tension du phototransistor sont stockés dans la SRAM du µC. Si ces tensions changent trop pendant le voyage, une alerte de sabotage est donnée. Alice entre la chaîne de réponse (jusqu'à 65 caractères) pour armer et verrouiller la boîte et la faire passer à l'état 3. La pendule de voyage est également mise en marche. Alice note la date et l'heure exacte, ainsi que les chaînes défi-réponse, et cache le tout de manière sûre (dans sa tête, si possible). Ces infos de vérification seront utilisées plus tard. Elle envoie ensuite la boîte à Bob par la poste.

```
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
```

Statut 3

Les chaînes de défi et de réponse ont été

LISTE DES COMPOSANTS

Boîte inviolable

Résistances

Par défaut : SMD 0805
R18,R19 = 2 MΩ
R9 = 100 Ω
R3 = 22 kΩ
R30 = 1,2 MΩ
R4,R6,R12,R16,R17,R20,R23,R25 = 220 kΩ
R8,R10 = 33 kΩ
R11,R22 = 1 kΩ
R1,R2,R29,R28 = 22 kΩ
R27 = 330 kΩ
R26 = 1 kΩ
R5,R13,R14,R15,R24 = 220 kΩ
R7 = 2,22 kΩ
R21 = 10 MΩ
P3,P1 = 1 kΩ aj.
P2,P4 = 10 kΩ aj.

Condensateurs

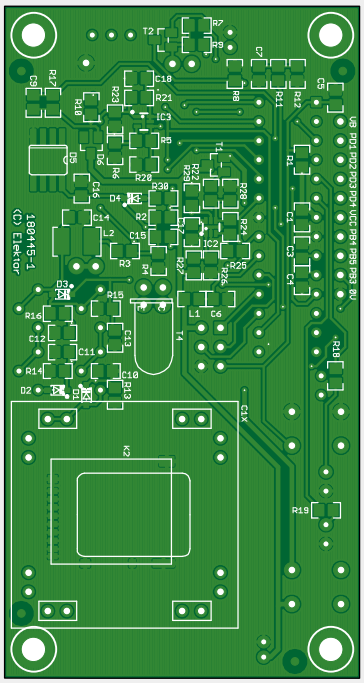
Par défaut : SMD 0805
C3,C4 = 22 pF
C14 = 120 pF
C7,C16 = 1 nF
C9,C10,C11,C12,C13,C15,C18 = 10 nF
C1,C5,C6,C17 = 100 nF
C2,C8 = 10µF 10 V, tantale, pas 2 mm

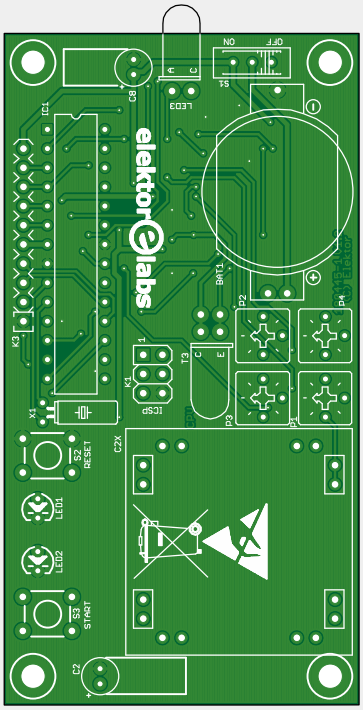
Inductances

L1 = 10 µH (0805)
L2 = 220 µH (1812)

Semi-conducteurs

D1,D2,D3,D4 = 1N4148WS (SOD-323)
D5 = LM285D-1,2 V
D6 = BAT54
IC1 = ATmega328P-PU, programmé
IC2 = MAX9915EXT+T
IC3 = MAX9914EXK+T
LED1 = 3 mm, rouge
LED2 = 3 mm, jaune

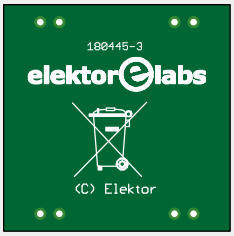


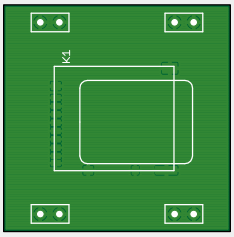


LED3 = TSAL6200
T1,T2 = BC857C
T3,T4 = SFH-300-3/4

Divers

BAT1 = support de pile, 2032,
p. ex. Renata HU2032
C1x,C2x = connecteur à 2 broches + prise
pour C1x & C2x, pas 2,54 mm
K1 = connecteur à 6 broches (2x3),
pas 2,54 mm
K2 = connecteur de carte microSD, poussoir
K3 = connecteur à 10 broches, pas 2,54 mm
S1 = interrupteur à glissière, SPDT S2,
S3 = interrupteur tactile, 6x6 mm
X1 = cristal de quartz 32,768 kHz
support scellé pour LED3
circuit imprimé #180445-1 (1x)
circuit imprimé #180445-3 (2x)





saisies et la boîte est armée et verrouillée. Toute manipulation ou saisie d'une chaîne de défi incorrecte cinq fois de suite déclenchera la séquence de remise à zéro. La boîte reste en statut 3 pendant son voyage par la poste.
Toutes les deux secondes, les mémoires tampons SRAM contenant les chaînes défi-réponse sont complémentées (inversées bit par bit). De cette façon, puisque chaque bit passe le même temps à l'état «0» qu'à l'état «1», on évite de brûler des cellules SRAM [4].

Chez Bob

Après un long et périlleux voyage, la boîte arrive (espérons-le) chez Bob. Il connecte son adaptateur IR à un ordinateur, le place devant la LED IR du boîtier et appuie sur le bouton Reset de l'adaptateur. Cela produira une impulsion de trois secondes sur le port infrarouge pour indiquer à la boîte d'activer son port infrarouge et de commencer à communiquer. Au bout de trois secondes, Bob envoie un seul caractère «U» pour calibrer l'UART de l'adaptateur infrarouge et le terminal commence à afficher les données :

```
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
```

Comme on le voit, la tension de la batterie a diminué, mais il n'y a aucun signe de sabotage car les rapports de tension Cx et les valeurs de tension du phototransistor n'ont pas beaucoup changé. Bob appelle Alice et lui demande la chaîne de défi qu'il saisit dans son terminal et, si tout va bien, il verra :

```
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 01a2g23w46e57f80g12r3
   e34fv245hasdvfr4.
```

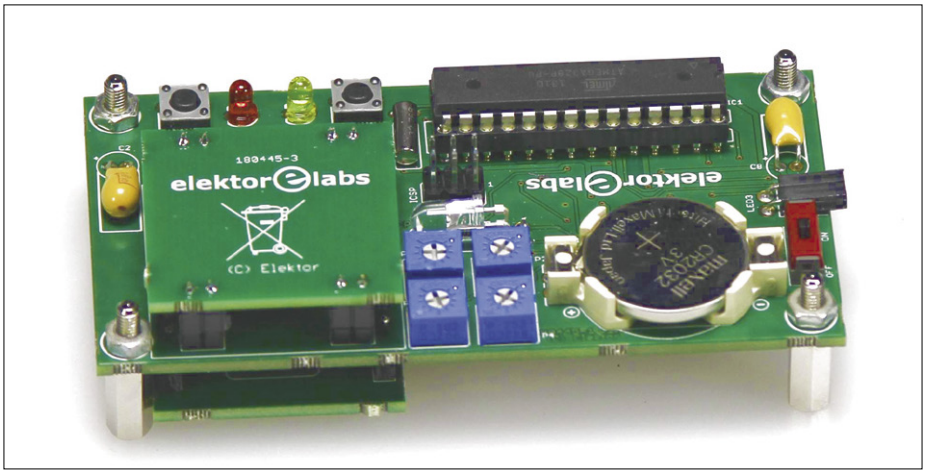


Figure 6. La carte entièrement assemblée avec des condensateurs à plaque ouverte installés des deux côtés.

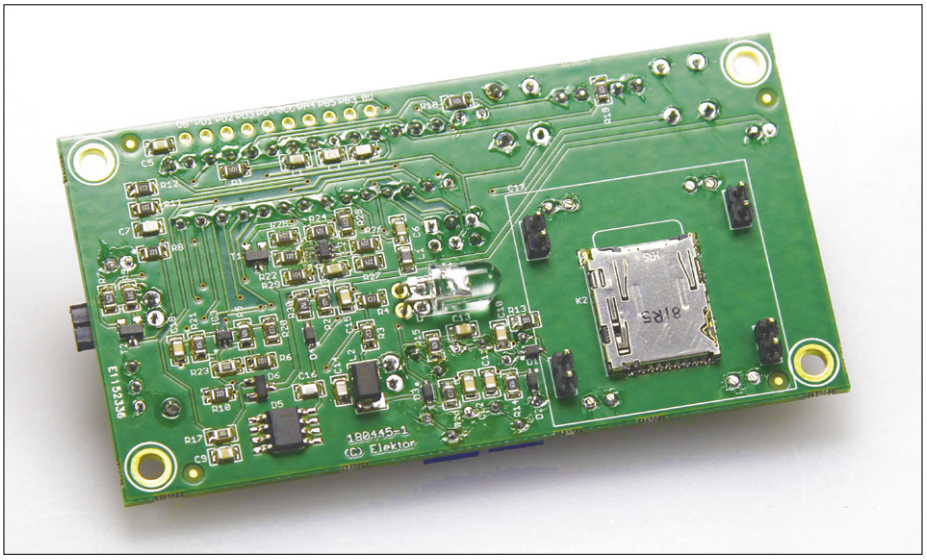


Figure 7. La face inférieure de la carte est peuplée de composants CMS et d'un transistor T4 traversant qui ressemble à une LED. Le condensateur C1x est monté sur le connecteur de la carte microSD.

Statut 4

Bob note immédiatement la date et l'heure actuelles et appelle à nouveau Alice pour vérifier la chaîne de réponse. Si Alice l'accepte, elle donnera à Bob l'heure et la date exactes qu'elle a notées lorsqu'elle a fermé la boîte. Cela permet à Bob de calculer le temps de trajet théorique et de le comparer au temps mesuré par la boîte. Si les deux correspondent, alors Bob est autorisé à utiliser la clé OTP stockée sur la carte microSD pour crypter et décrypter ses communications sécurisées avec Alice. En cas d'altération en cours de route, la boîte effacera la partie de la SRAM contenant les codes et la minuterie de voyage. Dans ce cas, la boîte affichera quelque chose comme ceci :

```
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
```

Statut 5

La séquence de mise à zéro a été exécutée en raison de la détection d'un événement de sabotage ou après avoir saisi cinq chaînes de défi invalides. Les tensions de contrôle de l'altération ne sont plus mises à jour, ce qui permet au détenteur de la boîte de voir le dernier état enregistré avant la détection de l'intrusion.

La séquence de mise à zéro est exécutée dans l'un des cas suivants :

- Après avoir saisi une chaîne de défi incorrecte cinq fois ;
- Le rapport de tension réel du condensateur diffère trop de la valeur enregistrée ;
- La tension réelle du phototransistor diffère trop de la valeur enregistrée ;
- Tension de la batterie trop faible (inférieure à 2,1 V) ;
- Température hors limites (inférieure à –20°C ou supérieure à +60°C).

Pour éviter que la lumière parasite ne déclenche l'événement d'intrusion 3, assurez-vous de la fermeture hermétique de la boîte. Appliquez une pâte noire autour de la LED3 à l'intérieur de la boîte et scellez les bords de la boîte avec du ruban adhésif noir. Testez-le en exposant la boîte fermée (dans l'état 3) à une forte lumière solaire directe. Maintenant, Bob peut entrer la commande «DE» pour voir ce qui a causé la mise à zéro :

```
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
```

Statut 6

Après avoir reçu la commande «DE», la boîte transmet des détails sur la cause de la mise à zéro.

Les données affichées dans les états 5 ou 6 n'ont pas besoin d'être valides car elles dépendent de ce que Mallory a fait de la boîte. Elle peut l'avoir réinitialisée et avoir entré des chaînes défi-réponse avant de transmettre la boîte à Bob dans l'état 3. Cependant, même si elle parvient à entrer les bonnes chaînes, elle devra également usurper le temps de parcours, ce qui sera beaucoup plus difficile.

Retour au statut 1

La commande «RE» peut être utilisée pour redonner à la boîte le statut 1 sans l'ouvrir. En appuyant sur le bouton de réinitialisation S2 à l'intérieur de la boîte, vous obtiendrez la même chose.

Chevaux de Troie matériels

On ne s'inquiète généralement que des logiciels malveillants et des chevaux de Troie qui attaquent un ordinateur. Quelques mots sur les Troyens matériels ne seraient pas déplacés. Un système simple avec un seul µC, jamais connecté à l'internet, est à l'abri des logiciels malveillants typiques qui cibleraient votre PC ou votre téléphone. La référence [5] donne une explication de base des problèmes liés aux dispositifs de mémoire à semi-conducteurs à très haut niveau d'intégration.

Un Troyen matériel à porte dérobée consiste en un circuit supplémentaire ajouté à la puce de silicium du µC. Cela peut faire autant de mal qu'un cheval de Troie logiciel ou même plus. Il représente un danger pour les µC d'aujourd'hui dont le processeur, la SRAM, l'EEPROM et la mémoire flash sont intégrés sur une puce de silicium et sont programmables à basse tension (3 à 5 V). Il en existe essentiellement deux types :

1. Troyens matériels à usage général

Mallory peut implanter un cheval de Troie matériel dans le µC, p. ex. pour copier périodiquement la SRAM et les registres du µC dans une partie secrète de la mémoire flash. Quelle que soit l'application du µC, un instantané «gelé» de la RAM sera toujours utile pour elle et Ève. Avec un tel cheval de Troie en place, Mallory peut facilement lire les chaînes de défi et de réponse définies par Alice. Il sera un peu plus difficile de pirater la minuterie de voyage.

2. Troyens matériels spécifiques à une application

Pour installer ce type de cheval de Troie matériel, Mallory doit d'abord connaître le micrologiciel de l'unité centrale de traitement. Ensuite, elle installe sur le µC un circuit capable de reconnaître le micrologiciel qu'Alice a flashé dans son µC. Au démarrage du µC, le cheval de Troie agira comme un chargeur de démarrage et modifiera quelques lignes du programme du µC (p. ex. les remplir de NOP en utili-

LISTE DES COMPOSANTS

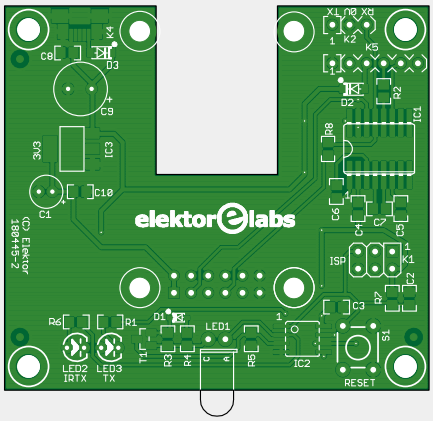
Adaptateur IR

Résistances
Par défaut : SMD 0805
R1,R6 = 680 Ω
R4 = 1,5 kΩ
R2,R8 = 4,7 kΩ
R5 = 22 kΩ
R7 = 100 kΩ
R3 = 2,2 MΩ

Condensateurs
Par défaut : SMD 0805
C2,C3,C8 = 100 nF
C4,C5,C6,C7,C10 = 1 µF, X7R, 50 V
C1 = 10 µF 10 V tantale, pas 2 mm
C9 = 100 µF 16 V, pas 3,5 mm

Semi-conducteurs
D1 = 1N4148WS (SOD-323)
D2,D3 = MBR120
IC1 = MAX232ECWE
IC2 = ATtiny45-20SU, programmé
IC3 = LD1117AS33
LED1 = TSAL6200
LED3 = 3 mm, jaune
LED2 = 3 mm, rouge
T1 = BC857C

Divers
K1 = connecteur à 6 broches (2x3), pas 2,54 mm
K2 = connecteur à 3 broches, pas 2,54 mm
K3 = douille à broche à 12 voies (2x6), pas 2,54 mm
K4 = connecteur micro USB de type B
K5 = connecteur à 6 broches, pas 2,54 mm



S1 = interrupteur tactile, 6x6 mm
module Ethernet WIZ107
circuit imprimé #180445-2

sant la fameuse commande SPM de l'AVR) pour désactiver par exemple certaines actions de protection cruciales. Les chances de succès d'une attaque de ce type sont beaucoup plus faibles qu'avec un cheval de Troie à usage général.

Quelle parade ?

Il existe de nombreux moyens de contrer ce genre de menaces matérielles. La plus simple est de revenir à la technologie des années 1980 et d'utiliser un simple système Z80 [6] avec SRAM et EPROM comme circuits intégrés séparés. L'EPROM est effacée par une lumière UV et a besoin d'une tension de 13 à 14 V sur sa broche V_{pp} pour l'écriture, ce qui rend beaucoup plus difficile l'installation d'une porte dérobée matérielle. Les architectures internes des EPROM de type Z80 et 27C (produites par millions durant plus de 20 ans) sont très connues, et il est facile de décapsuler le CI et de l'inspecter au microscope si nécessaire. Avec les millions de pièces qui traînent autour du globe, Mallory aurait fort à faire pour les trafiquer toutes.

Le portage du micrologiciel de l'unité centrale de traitement du TRNG ou de l'OTP Crypto Shield sur un Z80 peut se faire au détriment de la vitesse d'exécution et de la taille physique, mais les systèmes fonctionneraient quand même bien. Je signale ici une autre idée fausse de l'ingénierie de conception actuelle : les dispositifs mini, micro et nano ne sont pas forcément meilleurs !

Bien sûr, un système basé sur le Z80 serait trop lourd et trop gourmand pour être utilisé pour notre boîte postale, mais ce problème peut être résolu d'une autre manière, avec un peu de circuits supplémentaires, tout étant installé à l'intérieur de la boîte existante. Si vous avez étudié attentivement le schéma, vous vous demandez peut-être quelle est la fonction de K3. Il est destiné à un circuit supplémentaire pour protéger la boîte contre les Troyens matériels. Vous en saurez plus dans un prochain article.

Portes dérobées

Le prototype de la boîte sur les photos a fait plusieurs voyages avec différents transporteurs et il a fonctionné correctement. J'ai eu l'occasion de constater que chez certains transporteurs les paquets sont plus chahutés que chez d'autres. J'ai compris qu'il fallait arrimer C1x et C2x pour qu'ils ne se détachent pas. Une des méthodes consiste à coller dessus de la mousse non conductrice ou des morceaux de plastique. Si le µC est monté sur support, vous pouvez également l'assujettir. La pile est en principe assez serrée dans son support, mais on ne sait jamais.

Si vous avez d'autres suggestions d'améliorations, notamment de défense contre les portes dérobées, veuillez me contacter sur la page du projet sur Elektor Labs [7]. J'ai des idées, mais vous en avez peut-être d'autres et de meilleures.

Bob et Alice finissent par se rencontrer.

Proposez-les. Pour confirmer sa sécurité, tout dispositif de cryptage doit être examiné par nombre d'experts indépendants, alors n'hésitez pas !

Les fichiers de conception et le code source de ce projet peuvent tous être téléchargés sur la page du projet [7]. ⏮

180445-02

Liens

[1] Générateur de nombres aléatoires : www.elektormagazine.com/labs/random-number-generator-150116

[2] Système de cryptage à bloc-notes à usage unique (OTP) : www.elektormagazine.com/labs/one-time-pad-otp-crypto-system

[3] Effacer les données des clés USB : www.schneier.com/blog/archives/2011/03/erasing_data_fr.html

[4] Rémanence des données dans les dispositifs à semi-conducteurs : www.usenix.org/legacy/events/sec01/full_papers/gutmann/gutmann.pdf

[5] Entretien vidéo d'Elektor avec l'auteur sur la sécurité : www.elektormagazine.com/news/secure-communications-an-interview-with-luka-matic

[6] Z80 : un petit ordinateur simple : www.sunrise-ev.com/z80.htm

[7] Boîte aux lettres inviolable pour la distribution sécurisée de blocs-notes à usage unique : www.elektormagazine.com/labs/tamper-evident-paper-mail-box-for-secure-distribution-of-one-time-pads