problèmes de sécurité ? Combattez le feu par le feu !

Extension à mémoire analogique, protégée par ampoule de flash, pour la boîte à témoin d'effraction

Luka Matić

Dans l'article précédent de notre série de projets sur les communications hautement sécurisées [1], nous avons montré comment construire une boîte à témoin d'effraction (BTE) sécurisée qui préviendra son destinataire, Bob, qu'elle a été ouverte après qu'Alice l'a mise à la poste. Dans cet article, nous la rendons plus sûre en utilisant une technologie du début du siècle dernier.

La sécurité de la BTE repose sur la mise à zéro des codes de défi et de réponse dans la SRAM du microcontrôleur en cas d'ouverture non autorisée du dispositif. Puisque Eve (l'espionne) ne peut pas lire les codes en SRAM, elle ne peut pas la restaurer dans son état d'origine, et Bob sera averti. La communication entre Alice et Bob est alors totalement sécurisée. Est-ce bien le cas ?

Certes, Eve ne sera pas en mesure de restaurer la BTE dans son état d'origine, mais que se passe-t-il si Mallory intervient entre-temps ? Tout ce qu'elle a à faire, c'est de remplacer le microcontrôleur qu'Alice a commandé chez son fournisseur de composants préféré par une variante falsifiée. À moins qu'Alice n'ait accès à des équipements de laboratoire haut de gamme, elle n'a aucun moyen de savoir si son UC est un original vierge ou une variante modifiée malveillante. Mallory peut ajouter des portes dérobées matérielles sans modifier les plans des microcircuits de la matrice de silicium de l'UC [2], « simplement » en manipulant les niveaux de dopage. Les microcircuits auront l'air identiques, même sous le super microscope d'Alice !

L'ouverture de la BTE peut être détectée de manière fiable, mais la mise à zéro de la SRAM peut ne pas être efficace à 100 %. Même si les octets de mémoire contenant les codes critiques sont régulièrement inversés bit à bit pour limiter les effets résiduels de persistance à long terme, Eve peut toujours essayer d'exploiter la rémanence de la SRAM – du moins en théorie – en utilisant une attaque dite de démarrage à froid [3] et lire son contenu. Cela signifie-t-il qu'Alice et Bob devraient renoncer à l'espionnage avec un budget d'amateurs et chercher un emploi dans une grande agence à trois lettres ?

Eh bien, s'ils ajoutent à la BTE une mémoire vraiment irrécupérable, ils pourront poursuivre leurs opérations de guérilla à petit budget. Cela fonctionnera contre les chevaux de Troie matériels d'usage général aussi bien que contre ceux spécifiques à une application. Cependant, après avoir lu [4], [5] et [3], vous vous rendrez rapidement compte que tous les types de mémoire numérique connus au monde souffrent d'une forme de rémanence indésirable des données. Donc, si le numérique ne peut pas faire le travail, alors passons à l'analogique !

Principe de fonctionnement

Les ampoules de flash au magnésium (Mg) (**fig. 1**) sont utilisées en photographie pour l'éclairage artificiel depuis presque le premier jour. Les ampoules de flash jetables à usage unique (par ex. le type standard AG-1B) utilisent la température très élevée du magnésium en combustion pour créer un éclair chaud et brillant. Elles sont encore fabriquées aujourd'hui [6] et sont utilisées en photographie analogique et numérique en raison des effets uniques qu'elles créent.

Papier, bande magnétique ou film analogique, tous perdent leurs données lorsqu'ils sont surchauffés, voire surexposés. Si on en enroule un petit bout autour d'une ampoule, il peut être détruit (brûlé) en allumant l'ampoule. Si nous plaçons l'ampoule à l'intérieur de la BTE, on peut l'utiliser pour avertir Bob.

Ainsi, Alice écrit le code de réponse spécial sur un morceau de papier fin (ou l'enregistre sur une bande magnétique), l'enroule autour de l'ampoule de flash à l'intérieur de la BTE, arme la BTE et l'envoie à Bob. Si Eve manipule la boîte pendant son voyage, l'ampoule se déclenche et le code est détruit. Si Eve ne peut pas lire le code, elle ne pourra pas remettre la BTE dans son état d'origine et, pour finir, Bob sera au courant.

En plus d'être efficace contre les chevaux de Troie matériels, ce circuit permet également d'éviter les attaques par démarrage à froid. Bien que très difficiles à réaliser contre la BTE qui est protégée contre les basses températures et qui efface la SRAM à chaque redémarrage, elles méritent d'être mentionnées. La récupération de la SRAM ne servira à rien non plus si un flash détruit les informations contenues sur un support physique.

Figure 1. Cette ampoule de flash au magnésium est la pierre angulaire de notre alarme anti-effraction.

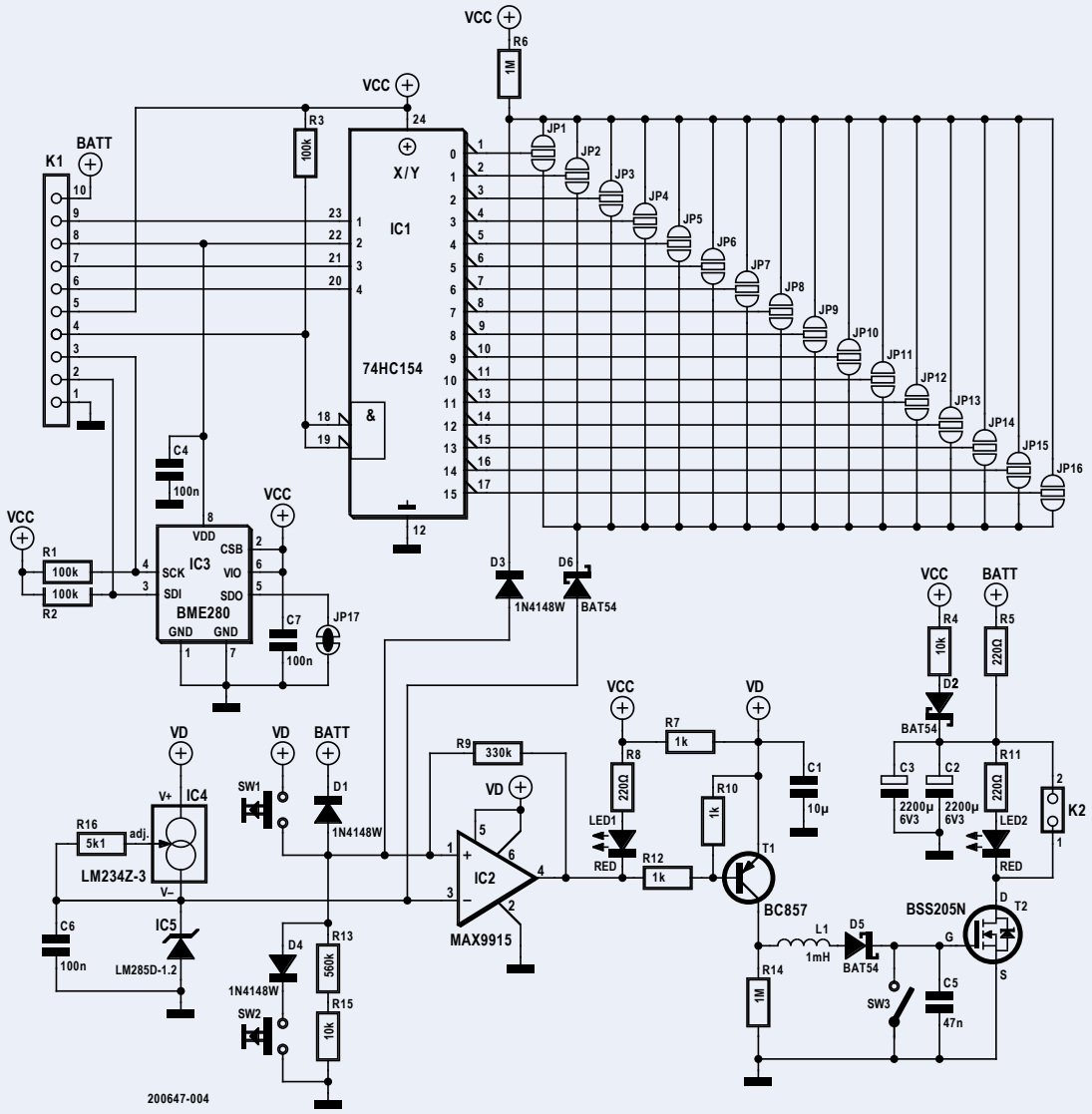


Figure 2. Le schéma de l'extension de mémoire analogique protégée par flash. La grande matrice sert de protection contre les chevaux de Troie.

Description du circuit

La **figure 2** donne le schéma de l'extension à mémoire analogique protégée par flash. Le connecteur K1 se branche sur le connecteur K3 prévu pour cela de la carte principale de la BTE [1]. À l'exception des broches d'alimentation, toutes les autres broches de K1 sont reliées au microcontrôleur de la BTE.

Lorsque l'effraction a été détectée par la BTE et que l'UC décide de mettre à zéro sa mémoire, il place une combinaison binaire sur les entrées de IC1, un décodeur binaire standard de 4 à 16, qui activera la sortie *Fire* (cathode de D3). Si, en revanche, la BTE a été déverrouillée avec succès, l'UC activera la commande *Block* (cathode de D6) à la place. Maintenant, la BTE peut être ouverte, l'interrupteur de sécurité SW3 peut être fermé et l'ampoule de flash peut être retirée de K2. Bob peut dérouler la bande de papier/cassette de l'ampoule de flash et vérifier le code de réponse spécial.

Les sorties qui activent les commandes *Fire* et *Block* sont sélectionnées par les cavaliers JP1 à JP16. (N'utilisez pas le même cavalier pour les deux commandes !) Avec IC1, ils constituent une protection contre un éventuel cheval de Troie spécifique à une application qui tenterait de désactiver la commande *Fire*. Avant chaque mission, les codes des commandes *Fire* et *Block* sont modifiés en sélectionnant différents cavaliers sur la carte (**fig. 3**) et en adaptant le microprogramme de l'UC en conséquence. Le cheval de Troie spécifique à l'application de Mallory ne peut pas fonctionner s'il ne peut pas reconnaître avec certitude le microprogramme ou les sorties. Un cheval de Troie à usage général peut copier les codes de la SRAM vers une mémoire flash secrète, mais il ne peut pas copier les codes d'un papier ou d'une bande magnétique enroulée autour de l'ampoule.

IC2 est câblé comme un comparateur avec une rétroaction positive pour réagir à une faible tension sur son entrée non-inverseuse. IC4 fournit un courant constant pour IC5, une référence de tension précise de 1,2 V à large plage de température, utilisée par IC2.

Lorsque la commande *Fire* est activée, l'entrée non-inverseuse est tirée vers le bas par la diode D3. La sortie de IC2 passe au niveau bas, permettant au transistor T1 de conduire. La charge stockée dans C1 circulera à travers L1 et D5, ce qui produit une tension sur C5 supérieure

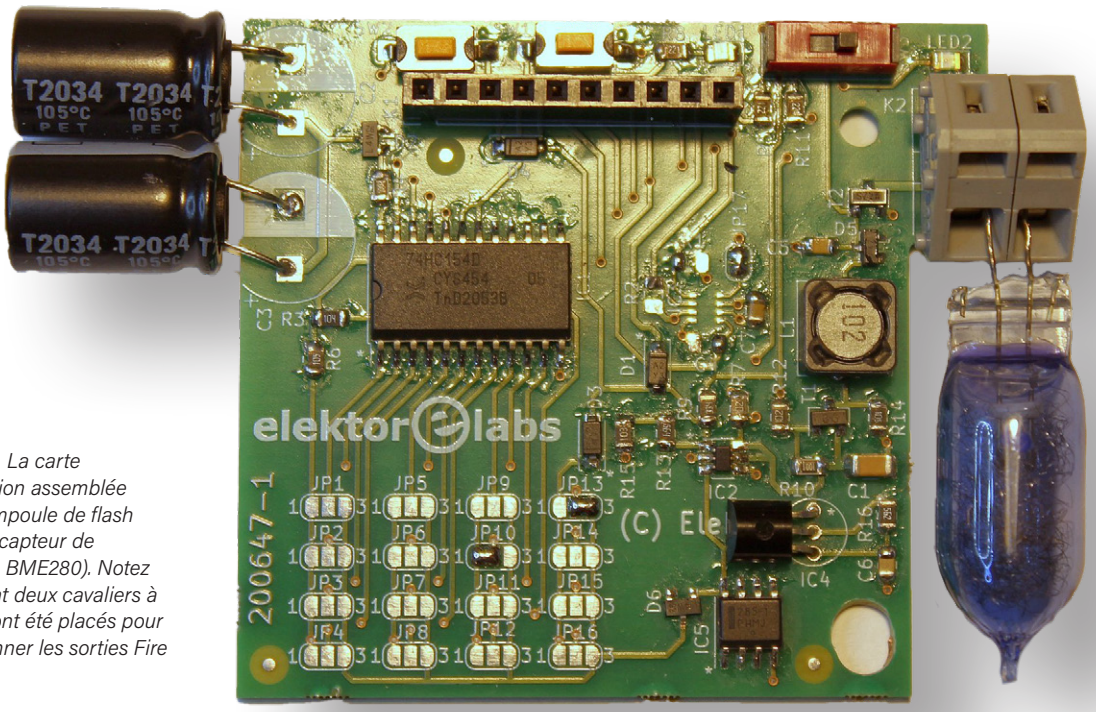


Figure 3. La carte d'extension assemblée avec l'ampoule de flash (sans le capteur de pression BME280). Notez comment deux cavaliers à souder ont été placés pour sélectionner les sorties Fire et Block.

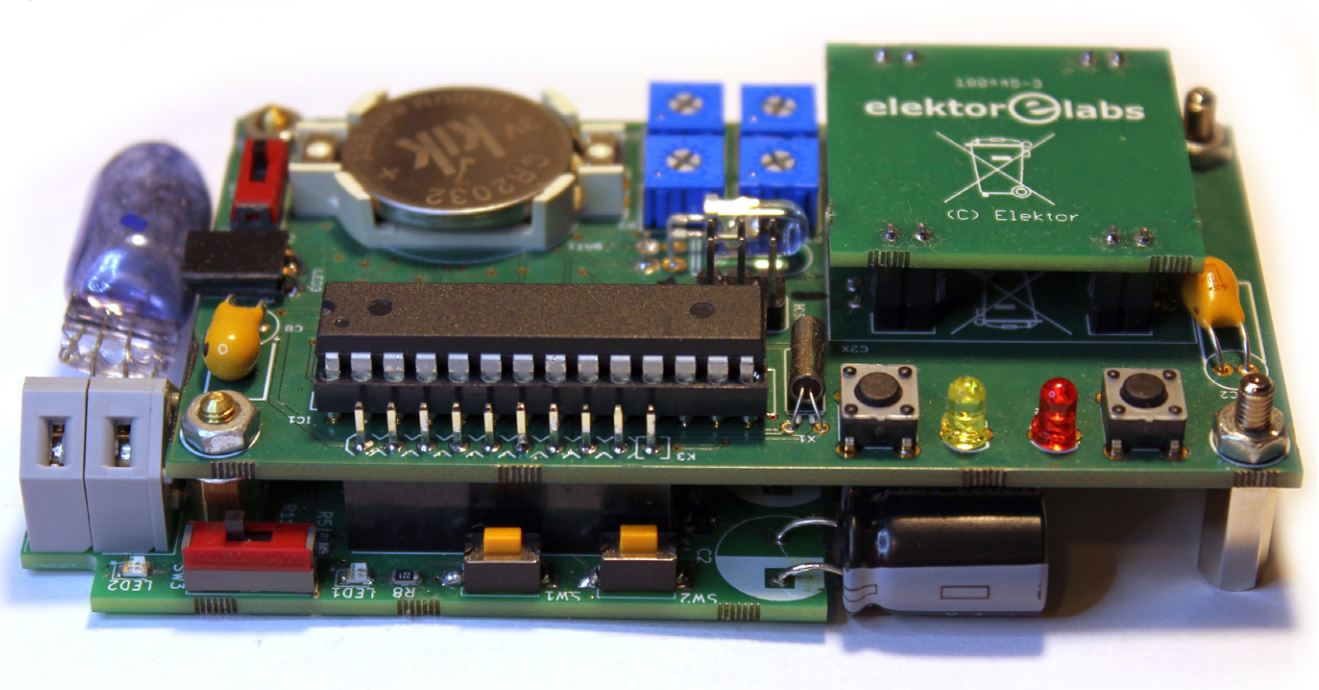


Figure 4. La carte d'extension avec ampoule de flash se branche en dessous de la carte principale de la BTE. Les deux boutons-poussoirs et son interrupteur sont accessibles sur le côté.

à V_d pour activer complètement le transistor T2. C5 maintient T2 allumé pendant au moins 10 à 20 ms, le temps nécessaire à l'allumage de l'ampoule connectée à K2. C2 et C3 stockent l'énergie nécessaire à une impulsion de courant de 1 A à 2 A pendant 10 ms pour enflammer le magnésium contenu dans l'ampoule.

Dans le cas de la commande *Block*, la diode D6 tirera l'entrée inverseuse de IC2 à 0,3 V, verrouillant effectivement la sortie de IC2 à l'état haut. Le circuit de mise à feu est maintenant désactivé.

Le bouton-poussoir SW1 est utilisé pour armer le circuit de mise à feu en chargeant C1 ; le bouton-poussoir SW2 sert à tester la mise à feu. SW3 est un interrupteur de sécurité, qui désactive la mise à feu en bloquant la grille de T2 à 0 V. Il peut être relâché une fois que tout est prêt.

LED1 et LED2 sont des témoins lumineux rouges. Si l'un d'eux ou les deux sont allumés, quelque chose n'est pas prêt, et vous ne devez pas connecter une ampoule de flash à K2 ou relâcher SW3.

Contrairement à la BTE, qui sort du mode économie d'énergie toutes les deux secondes, la carte d'extension est constamment alimentée afin de pouvoir réagir le plus rapidement possible aux courts-circuits ou aux chutes de tension provoqués par les attaques par perçage (voir ci-dessous). C'est pourquoi on utilise des circuits intégrés à faible puissance et à faible tension (jusqu'à 2,0 V). IC1, par exemple, *doit* être de type HC. Ils nécessitent un courant d'alimentation supplémentaire total de 30 µA seulement. Les trois condensateurs (C1, C2 et C3) conservent suffisamment d'énergie pour déclencher l'ampoule de flash même sans commande de l'UC en cas de court-circuit ou de faible tension sur V_{CC} ou V_{bat}.

Utilisation

Branchez la carte d'extension sur la carte principale (**fig. 4**) et mettez le système complet sous tension. Appuyez sur SW1 pour armer le circuit de mise à feu. Lorsque LED1 et LED2 s'éteignent, on peut connecter à K2 l'ampoule avec le message secret enroulé autour et relâcher SW3. On place ensuite l'ensemble dans une boîte (**fig. 5**) que l'on peut verrouiller en suivant la procédure expliquée dans [1].

Attaques par perçage

Maintenant que se passe-t-il si Eve essaie de désactiver le circuit de mise à feu de l'ampoule en perçant la BTE – par ex. en court-circuitant C1, C2 ou C3 à la masse avec une mèche de perceuse ? C'est pour cela que le circuit comporte également un capteur de pression barométrique (IC3, un BME-280 qui mesure également la température et l'humidité relative). La BTE lit la pression barométrique (absolue) de IC3 toutes les deux secondes via un bus I2C (réalisé par logiciel) sur les broches 2 et 3 de K1.

Lors de l'armement du boîtier, on doit chasser un peu d'air avec une pompe à vide. La pression de l'air mesurée par IC3 est lue par l'UC avec correction de température. Le rapport entre la pression de l'air et la température est ce qui compte pour déclencher la mise à zéro. Comme le volume de la BTE est constant, on n'autorise que des variations de pression proportionnelles à la température dans la plage de −20 °C à +60 °C (en fait 253 K à 333 K). Cela permettra de détecter une attaque par perçage dans les deux secondes (dès que le MCU se réveille du mode économie d'énergie).

Faites attention lorsque vous aspirez l'air de la BTE – il faut que Bob

puisse l'ouvrir sans avoir besoin d'un pied de biche. La force requise par Bob pour ouvrir le couvercle peut être calculée avec : $F = A \times \Delta p$, où A est la surface du couvercle et Δp la différence de pression.

Pas de place pour les logiciels libres

La mémoire protégée par une ampoule au magnésium résout efficacement le problème des chevaux de Troie matériels à usage général. Eve peut lire ce qu'elle veut dans la SRAM ou dans sa mémoire flash secrète, mais cela ne sert à rien si le code de réponse spécial est brûlé en même temps que le papier ou la bande magnétique. Cependant, un cheval de Troie spécifique à une application peut toujours empêcher l'allumage de la lampe flash, et on doit aussi se prémunir de cette menace.

Jusqu'à présent, nous avons recommandé l'utilisation de logiciels à code source ouvert chaque fois que cela était possible. Bien que les logiciels libres soient bien pour de nombreuses raisons, nous voici devant une exception.

Un cheval de Troie spécifique à une application est beaucoup plus compliqué qu'un cheval de Troie à usage général. Il ne fonctionne que s'il peut reconnaître le microprogramme avec certitude. Une façon pour Alice de contrer cette menace est d'écrire elle-même le micrologiciel. Elle le fera sur son ordinateur dédié qui n'est jamais connecté à l'internet et qu'elle utilisera aussi pour programmer l'UC. Si Mallory n'a aucune connaissance du microprogramme, son cheval de Troie ne saura pas comment le reconnaître.

La distribution des rôles

Dans les ouvrages de cryptographie, la communication a généralement lieu entre Alice (A) et Bob (B). Eve, l'espionne, essaie d'écouter passivement sans interférer, tandis que Mallory, le malveillant, n'hésite pas à modifier, substituer ou rejouer d'anciens messages.

Quelques précautions de sécurité

Les ampoules au magnésium fonctionnent avec des tensions très faibles – 1,0 V seulement peut suffire à les allumer. Cette mise en garde concerne le magnésium à l'intérieur de l'ampoule, qui brûle à des températures supérieures à 3.000 °C. Parfois, l'ampoule en verre se brise et vole en éclats en raison de ce stress thermique extrême. Les éclats de ce type de verre ne sont pas du tout tranchants, il n'y a donc aucun risque de coupure. C'est pourquoi, s'il est présent, on peut retirer le revêtement en plastique de l'ampoule de verre afin d'améliorer le transfert de chaleur et d'assurer la destruction du support qui l'entoure.

Des morceaux de métal fondu à ces températures extrêmes peuvent provoquer des brûlures. En revanche, l'allumage de l'ampoule à l'intérieur de la BTE est parfaitement sûr – de nombreux appareils électroniques courants libèrent beaucoup plus d'énergie lorsqu'ils tombent en panne en se consumant pendant leur fonctionnement (certes rarement à des températures aussi élevées). Le déclenchement d'une ampoule de flash au Mg à proximité de vos yeux non protégés peut être très désagréable et peut même provoquer une cécité temporaire (c'est ainsi que fonctionnent les grenades FlashBang). Par conséquent, enroulez le papier ou la bande autour de l'ampoule avant de la connecter à K2 – cela réduira la luminosité.

Astuce pour l'utilisation du papier

Pour utiliser du papier comme support d'écriture du code secret, il vaut mieux prendre du papier à rouler pour cigarettes fin. Il est aussi recommandé de le tremper dans une solution d'eau saturée de permanganate de potassium. Cet oxydant puissant abaisse la température d'ignition du papier. Laissez sécher le papier avant d'y écrire le message secret.

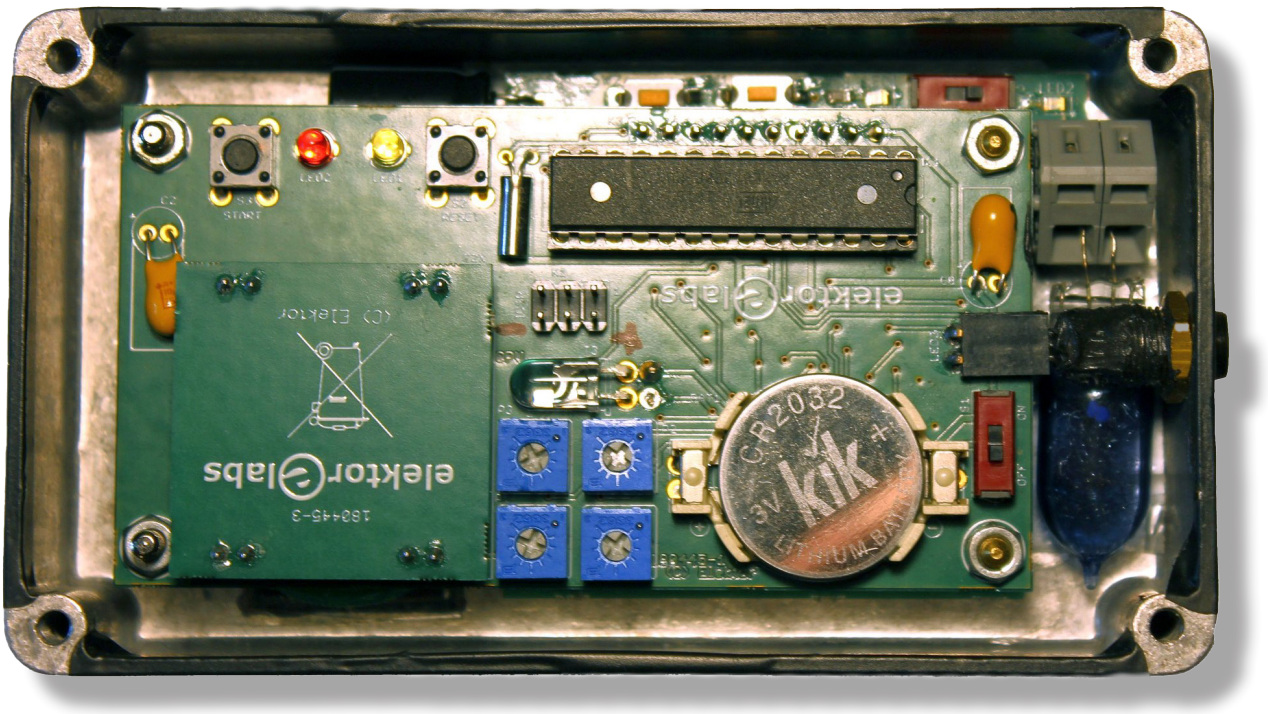


Figure 5. La boîte inviolable équipée de son flash de protection prête à être envoyée à Bob.

LISTE DES COMPOSANTS

Résistances (5%, 0805, 1/8 W)

R1, R2, R3 = 100 kΩ
R4, R15 = 10 kΩ
R5, R8, R11 = 220 Ω
R6, R14 = 1 MΩ
R7, R10, R12 = 1 kΩ
R9 = 330 kΩ
R13 = 560 kΩ
R16 = 5,1 kΩ (5,6 kΩ // 56 kΩ)

Condensateurs

C1 = 10 µF (1206)
C2, C3 = 2200 µF 6V3, pas de 5 mm
C4, C6, C7 = 100 nF (0805)
C5 = 47 nF (0805)

Inducteurs

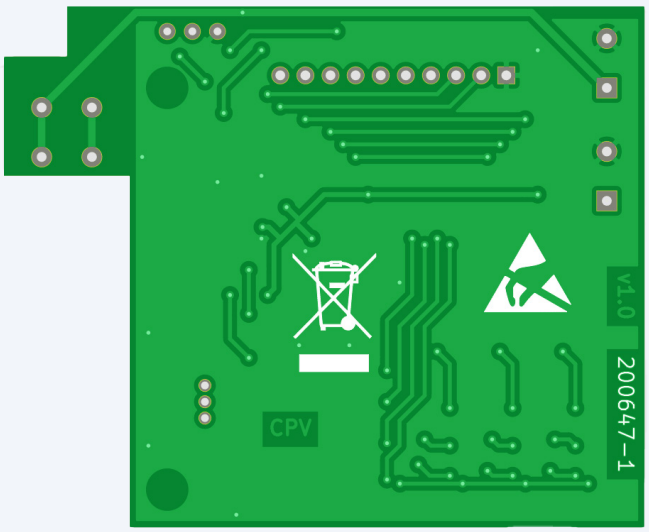
L1 = 1 mH, 10 Ω

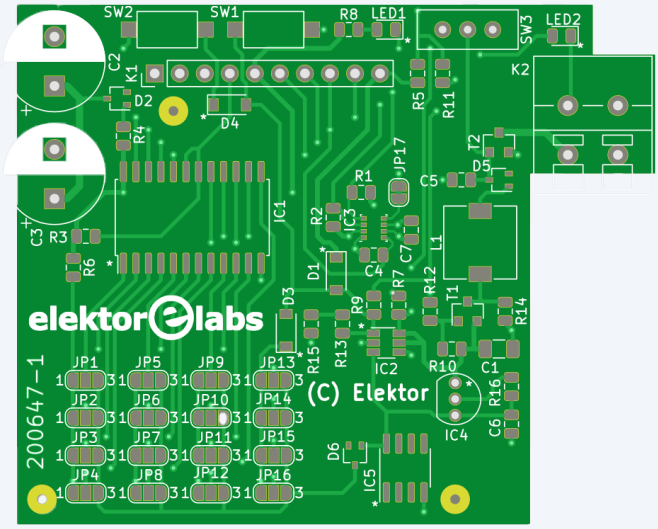
Semi-conducteurs

D1, D3, D4 = 1N4148W
D2, D5, D6 = BAT54
IC1 = 74HC154D
IC2 = MAX9915
IC3 = BME280
IC4 = LM234Z-3
IC5 = LM285D-1.2
LED1, LED2 = LED, rouge, 0805
T1 = BC857
T2 = BSS205N

Divers

K1 = barrette femelle à 10 voies, pas de 2,54 mm
K2 = connecteur à vis à 2 voies, pas de 5,08 mm, Wago 236-402
SW1, SW2 = bouton-poussoir, RS282G05A3
SW3 = interrupteur à glissière, SS12SDP2





LIENS

[1] Luka Matić, « boîte inviolable protégée par un témoin d'effraction », Elektor, 05-06/2020 : www.elektormagazine.fr/180445-02
[2] Implanter un Trojan matériel dans une puce de silicium : www.schneier.com/blog/archives/2018/03/adding_backdoor.html
[3] Rémanence des données en SRAM à basse température : https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-536.pdf
[4] Effacement des données des disques flash : https://www.schneier.com/blog/archives/2011/03/erasing_data_fr.html
[5] Rémanence des données en mémoire RAM : https://www.usenix.org/legacy/events/sec01/full_papers/gutmann/gutmann.pdf
[6] Meggaflash, fabricant d'ampoule de flash au magnésium : http://www.meggaflash.com/
[7] Ce projet sur Elektor Labs : www.elektormagazine.fr/labs/magnesium-bulb-analogue-memory-add-on-to-the-tamper-evident-box
[8] Boîte à témoin d'effraction sur Elektor Labs : www.elektormagazine.fr/labs/tamper-evident-paper-mail-box-for-secure-distribution-of-one-time-pads
[9] Entretien avec Luka Matić sur Elektor TV : www.elektormagazine.fr/news/fr-secure-communications-an-interview-with-luka-matic

Améliorations supplémentaires

Outre l'abandon des logiciels à code source ouvert, nous pouvons également faire une petite entorse à nos principes de matériel ouvert. Alice peut améliorer la sécurité en modifiant également les connexions entre K1 et IC1 (par ex. en introduisant des cavaliers de soudure comme JP1-JP16). Créer sa propre variante du circuit imprimé ne peut qu'améliorer la robustesse contre les chevaux de Troie matériels de Mallory et les attaques par perçage d'Eve.
Même si l'extension de la BTE est protégée contre les courts-circuits dus à une attaque par perçage, il faut noter qu'Eve dispose d'une fenêtre théorique de 2 s pour en effectuer une (jusqu'à ce que l'UC se réveille et détecte un changement de pression de l'air). Cela signifie qu'il faudrait renforcer mécaniquement contre le perçage les pistes vulnérables du circuit imprimé (V_d étant la plus importante) avec par ex. de fines barres d'alliages très durs insérées à l'intérieur d'un corps en métal mou (laiton ou aluminium) pour casser une mèche ou la faire dévier – comme ce qui est utilisé dans les serrures de haute sécurité.

Amélioration de la sécurité

L'extension simple et peu coûteuse décrite ici améliore considérablement la sécurité du boîtier inviolable, et le prémunit contre de nombreuses attaques à haute technologie. Tous les types de cassettes magnétiques essayés avec ce système ont été brûlés par une ampoule au magnésium AG-1. Tous les tests effectués avec du papier ont également été concluants.
Tout ceci reste abordable et réalisable par nos amis Alice et Bob avec leur budget limité. Appliquée et combinée avec soin, une technologie analogique simple et pas chère peut venir à bout de la coûteuse high-tech numérique. Cela peut sembler contre-intuitif, mais il ne faut pas toujours se fier à son intuition. Comme pour tout dispositif sécurisé, plusieurs experts indépendants devront explorer de nouveaux moyens d'attaque et de défense pour évaluer pleinement la sécurité globale.
Tous les fichiers de conception de ce projet et bien d'autres encore se trouvent sur [7], [8] et [1]. Regarder [9] peut vous aider à développer votre aptitude à la paranoïa. Bon espionnage !

200647-04

Contributeurs

Idée, conception et texte : **Luka Matić**
Conception et modification des circuits imprimés : **Clemens Valens**
Mise en page : **Harmen Heida**
Traduction : **Denis Lafourcade**

Des questions, des commentaires ?

Envoyez un courriel au rédacteur (clemens.valens@elektor.com).