

# L'authentification de dispositif contrecarre la contrefaçon

Par **Michael D' Onofrio**, Directeur de division Associé pour la Sécurité embarquée, chez Maxim Integrated

L'une des principales méthodes pour assurer la sécurité électronique est le recours à l'authentification matérielle. L'authentification de dispositifs sert à protéger les utilisateurs finaux et les fabricants, contre les périphériques, les capteurs, les consommables, ou d'autres dispositifs contrefaits. Cette méthode permet au système hôte de vérifier que le dispositif connecté est bien authentique et digne de confiance.

## Problèmes posés par les dispositifs contrefaits

Commençons par convenir de ce que nous appelons "contrefaçon" dans ce qui suit. Un dispositif contrefait peut simplement être un clone bon marché du dispositif original. Considérez par exemple, un capteur médical à brancher sur un module de commande. Le dispositif contrefait est fabriqué avec soin pour ressembler et se comporter comme l'original, mais sa qualité et sa précision sont sujets à caution, et sont donc susceptibles d'entraîner un diagnostic erroné et un traitement inadapté<sup>1</sup>. Dans un tel cas, il est clair que l'authentification du dispositif permet de protéger les patients des risques associés à des appareils défectueux, et aussi d'éviter aux fournisseurs de produits de santé d'être jugés responsables d'une défaillance professionnelle<sup>2</sup>.

Un exemple moins frappant, et peut-être plus banal, est celui des cartouches d'encre contrefaites pour imprimantes jet d'encre. De nombreux fabricants vendent leur imprimante à prix coûtant ou presque, dans l'espoir de générer des bénéfices et de rentabiliser leurs coûts de recherche et développement, grâce à la vente de cartouches jet d'encre jetables. Mais lorsque des cartouches jet d'encre contrefaites sont conditionnées et commercialisées comme s'il s'agissait de produits authentiques, le fabricant se trouve floué. Ces cartouches contrefaites de mauvaise qualité peuvent aussi nuire au bon fonctionnement, voire endommager l'imprimante, et nuire à la réputation de la marque.

Alors que le monde et nos nombreux appareils électroniques sont de plus en plus interconnectés, les constructeurs de périphériques ont de plus en plus conscience des menaces de sécurité et de l'impact potentiellement préjudiciable des dispositifs contrefaits. Ce n'est donc pas une surprise si les fabricants mettent en place différentes mesures de sécurité, pour détecter et contrecarrer les contrefaçons.

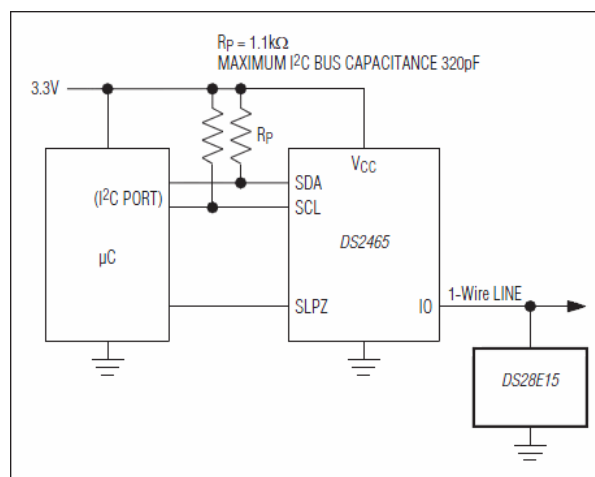
## Méthodes d'authentification

La sécurité électronique recouvre aujourd'hui toute une série de méthodes à base d'algorithmes de cryptage et de protocoles d'authentification, plus ou moins efficaces les uns que les autres en fonction de l'application.

Une méthode d'authentification simple fonctionne en gros comme une identification. A partir du moment où le système hôte "maître" reçoit des données correctes d'identification du périphérique "esclave", celui-ci est considéré comme authentique. Le défaut de cette méthode est que les données d'identification elles-mêmes sont exposées pendant la transmission de l'esclave à l'hôte, et sont alors accessibles à un éventuel attaquant. Ce genre d'identification peut facilement être contourné en enregistrant puis en "rejouant" les données d'identification, puis en fonctionnant comme un dispositif authentique.

Une autre méthode qui s'avère très robuste consiste à utiliser une fonction "hash" monodirectionnelle, qui est facile à générer, mais virtuellement impossible à inverser pour un attaquant qui voudrait en retrouver la valeur d'entrée. SHA-256 est une fonction hash éprouvée et bien testée. A l'aide d'un protocole "challenge-response" (défi-réponse), SHA-256 calcule un code MAC (Message Authentication Code, ou code d'authentification de message), basé sur plusieurs données publiques et privées. Le CI d'authentification du périphérique calcule un code MAC et l'envoie au système hôte ; de son côté, l'hôte calcule lui aussi le code MAC, à partir de la même entrée convenue. Alors l'hôte compare ensuite le code MAC qu'il a généré, à celui généré par le périphérique et, s'ils sont identiques, l'authenticité du périphérique est alors confirmée<sup>3 4</sup>.

Les algorithmes SHA-256 peuvent être implémentés sous forme logicielle, à la fois dans l'hôte et dans les dispositifs périphériques, mais les implémentations logicielles peuvent être délicates. Un hacker capable de passer à travers les protections du contrôleur, et de décompiler le code, pourra avoir accès aux données secrètes utilisées par la procédure d'authentification. Par conséquent, un système d'authentification sécurisé SHA-256 s'appuyant sur un CI d'authentification sécurisée, comme un DeepCover DS28E15, sera plus robuste<sup>5</sup>.



[DS28E15: Typical Application Circuit](#)

Un authentificateur<sup>6</sup> sécurisé DeepCover offre à la fois les avantages d'une fonction hash monodirectionnelle, et ceux d'un cryptage matériel. Dans le cas d'implémentations SHA-256, le coprocesseur stocke de manière sécurisée dans la mémoire protégée les données sensibles, comme le code secret côté hôte, qui peuvent servir d'entrée à l'algorithme, mais qui ne peuvent pas être lues. Le coprocesseur exécute également les calculs SHA-256 côté hôte. Pour vérifier l'authenticité, le MCU envoie une défi aléatoire au coprocesseur et à l'authentificateur, puis récupère les réponses MAC générées par le coprocesseur et l'authentificateur pour les comparer. Des contre-mesures sont implémentées au niveau matériel dans le CI d'authentification, pour rendre virtuellement impossible l'extraction des données sensibles, et le contournement par examen physique du dispositif.

Pour éviter d'avoir à protéger le secret côté hôte, les algorithmes à base de clé publique comme ECDSA<sup>7</sup> n'utilisent pas de secret côté hôte. En revanche, la clé privée est stockée de manière sécurisée dans le CI d'authentification, lui-même sécurisé, et l'hôte utilise une clé publique pour vérifier l'authenticité du périphérique. Dans le cas d'implémentations ECDSA, le coprocesseur n'a pas besoin de protéger la clé publique côté hôte, mais il doit exécuter des calculs ECDSA complexes, et retourner le résultat au MCU. L'approche matérielle permet d'obtenir une plateforme d'authentification sécurisée plus résistante aux attaques, et permet aussi de réduire le temps et les coûts nécessaires à son développement au sein de l'hôte et des périphériques.

L'implémentation d'un authentificateur sécurisé DeepCover se fait simplement en utilisant une interface 1-Wire pour communiquer entre le coprocesseur et l'authentificateur. Les coprocesseurs sont dotés d'une passerelle I<sup>2</sup>C-1-Wire intégrée. Les authentificateurs 1-Wire sont alimentés de manière parasite par la broche E/S, afin de simplifier encore l'intégration côté périphérique. L'interface 1-Wire supporte le "multidrop", ce qui permet d'alimenter plusieurs authentificateurs 1-Wire à partir du même bus E/S si l'application l'exige.

## Résumé

L'authentification sécurisée des dispositifs périphériques est critique pour protéger les clients et les fabricants contre les dispositifs contrefaits. De nombreuses méthodes d'authentification existent, chacune avec ses forces et ses faiblesses. L'authentification sécurisée matérielle à base d'authentificateur sécurisé DeepCover offre un compromis équilibré entre sécurité, coût de BOM (Bill of Materials, ou nomenclature), et simplicité d'intégration au sein de conceptions existantes ou nouvelles.

[www.maximintegrated.com](http://www.maximintegrated.com)

[Deepcover](#)

[DS28E15](#)

**A propos de l'auteur :**

**Michael D' Onofrio** a rejoint Maxim Integrated en tant que Directeur de division Associé, pour les produits d'authentification sécurisée, en 2012. Il a étudié à Duke University, où il a obtenu un diplôme en Management et marchés et Politique publique.

1-Wire et DeepCover sont des marques commerciales déposées de Maxim Integrated Products, Inc.

## Références

<sup>1</sup> Pour une discussion sur la façon dont des appareils médicaux contrefaits sont susceptibles d'impacter la qualité de soins médicaux, voir Tremlet, Christophe, "Hardware Security ICs Offer Large Security Returns at a Low Cost," **Electronic Products**, 20 août 2013, [http://www.electronicproducts.com/Software/EDA\\_Software\\_and\\_Hardware/Hardware\\_Security\\_ICs\\_Offer\\_Large\\_Security\\_Returns\\_at\\_a\\_Low\\_Cost.aspx#.U7wlp0A-eSo](http://www.electronicproducts.com/Software/EDA_Software_and_Hardware/Hardware_Security_ICs_Offer_Large_Security_Returns_at_a_Low_Cost.aspx#.U7wlp0A-eSo) ; également disponible dans la note d'application Maxim Integrated, No 5716 at <http://www.maximintegrated.com/AN5716>.

<sup>2</sup> Découvrez comment des compteurs contrefaits ont causé des pertes financières considérables à une centrale de Puerto Rico, et comment la sécurité embarquée aurait pu éviter le problème. Voir Andeen, David, "Smart Grid Security: Recent History Demonstrates the Dire Need," **Power Systems Design Europe**, décembre 2012, pages 33-35, [http://www.powersystemsdesign.com/library/resources/images/IssuePDF/psde\\_december12.pdf](http://www.powersystemsdesign.com/library/resources/images/IssuePDF/psde_december12.pdf) ; également disponible dans la note d'application Maxim Integrated, No 5546, sur <http://www.maximintegrated.com/AN55237>.

Pour une discussion plus générale sur la façon dont les dispositifs contrefaits peuvent affecter les smart grids ou les systèmes de commande industriels, voir également Andeen, David, "Energy Measurement and Security for the Smart Grid--Too Long Overlooked," **EETimes China**, 7 janvier 2013, [http://www.eet-china.com/articleLogin.do?artId=8800680222&fromWhere=/en/ART\\_8800680222\\_617693\\_TA\\_a2c42dcf.HTM&catId=617693&newsType=TA&pageNo=null&encode=a2c42dcf](http://www.eet-china.com/articleLogin.do?artId=8800680222&fromWhere=/en/ART_8800680222_617693_TA_a2c42dcf.HTM&catId=617693&newsType=TA&pageNo=null&encode=a2c42dcf) (en chinois), et la note d'application Maxim Integrated, No 5536, sur <http://www.maximintegrated.com/AN5536>.

<sup>3</sup> Pour une présentation détaillée d'un système d'authentification maître/esclave, voir Linke, Bernhard, "The Fundamentals of a SHA-256 Master/Slave authentication System," **EETIMES**, 19 juin 2013, [http://www.eetimes.com/document.asp?doc\\_id=1280942](http://www.eetimes.com/document.asp?doc_id=1280942). Plus de détails sont disponibles dans la note d'application Maxim Integrated, No 5546, sur <http://www.maximintegrated.com/AN5546>.

Voir aussi Linke, Bernhard, "A SHA-256 master/slave authentication system," **Electronic Products**, 16 juin 2014, [http://www.electronicproducts.com/Digital\\_ICs/Communications\\_Interface/A\\_SHA-256\\_master/slave\\_authentication\\_system.aspx#.U7ws6kA-eSo](http://www.electronicproducts.com/Digital_ICs/Communications_Interface/A_SHA-256_master/slave_authentication_system.aspx#.U7ws6kA-eSo) ; plus de détails sont disponibles dans la note d'application Maxim Integrated, No 5785, "THE DS28C22 DEEPCOVER SECURE AUTHENTICATOR IN A SHA-256 MASTER/SLAVE AUTHENTICATION SYSTEM," sur <http://www.maximintegrated.com/AN5785>.

<sup>4</sup> Voir note <sup>3</sup>.

<sup>5</sup> Pour une discussion sur les raisons pour lesquelles les CI à sécurité embarquée au niveau matériel constituent les "composants de protection ultimes", voir Tremlet, Christophe, "Industrial Systems Need Embedded Security ICs," **EETimes**, 1er novembre 2012, [http://www.eetimes.com/document.asp?doc\\_id=1280102](http://www.eetimes.com/document.asp?doc_id=1280102); également disponible sous forme de note d'application Maxim Integrated, No 5522, sur <http://www.maximintegrated.com/AN5522>.

<sup>6</sup> Tremlet, Christophe, "How to protect embedded software against attacks," **New Electronics**, 11 février 2014, <http://www.newelectronics.co.uk/electronics-technology/how-to-protect-embedded-software-against-attacks/59422/>; également disponible sous forme de note d'application Maxim Integrated, No 5796 "Implementing secure boot with DeepCover™ MAXQ1050" sur <http://www.maximintegrated.com/AN5716>. Voir aussi la note <sup>3</sup>.

<sup>7</sup> Voir aussi Linke, Bernhard, "Using the Elliptic Curve Digital Signature Algorithm effectively," **Embedded.com**, 2 février 2104, <http://www.embedded.com/design/safety-and-security/4427811/Using-the-Elliptic-Curve-Digital-Signature-Algorithm-effectively>; également disponible sous forme de note d'application Maxim Integrated, No 5767, sur <http://www.maximintegrated.com/AN5767>.

<sup>8</sup> Pour une discussion sur la manière dont des mesures de sécurité "cradle-to-grave" (de bout-en-bout) embarquées au niveau matériel, permettent de protéger les dispositifs industriels et les "smart grids" (réseaux de distribution intelligents), voir Ardis, Kris, "Stuxnet and other things that go bump in the night," **EDN**, 11 octobre 2012, <http://www.edn.com/design/systems-design/4398386/2/Stuxnet-and-other-things-that-go-bump-in-the-night>; également disponible sous forme de note d'application Maxim Integrated, No 5445, sur <http://www.maximintegrated.com/AN5445>.

Voir aussi Ardis, Kris, "Silicon, Security, the Internet of Things, and the Smart Grid, Part 3: IoT and Security," **Smart Grid News.com**, Nov 26, 2013, [http://www.smartgridnews.com/artman/publish/Technologies\\_Security/Smart-grid-the-Internet-of-Things-and-security-an-inside-look-6188.html#.U7wnt0A-eSp](http://www.smartgridnews.com/artman/publish/Technologies_Security/Smart-grid-the-Internet-of-Things-and-security-an-inside-look-6188.html#.U7wnt0A-eSp). Cette série en 4 parties sur la sécurité de l'Internet des objets est également disponible sous forme de note d'application Maxim Integrated, No 5725, sur <http://www.maximintegrated.com/AN5725>.