Keywords: 3D printing , IP protection, SHA-256, challenge-and-response authentication

APPLICATION NOTE 5940

SECURE 3D PRINTING - THE NEW DISRUPTIVE TECHNOLOGY - AND WATCH THE MARKET GROW

By: Hamed Sanogo, Executive Business Manager, Secure Info & Authentication

Abstract: This application note focuses on modern 3D printing, also known as additive manufacturing, which is making a three-dimensional solid object of virtually any shape from a 3D model or other electronic data source. It discusses the Razor-Razorblade business model which involves selling a main item at a discount just so the complementary (often disposable) secondary goods can be sold at a considerably higher price. This same business model has been successfully used for the traditional printer market, but the model works only when there is a strong IP protection scheme implemented against cloning, counterfeiting, replicating, and imitating disposables. The DS28E15 DeepCover® secure authenticator IC is the right path for selling more 3D printers. Now, here is how we get a 3D printer in every home!

It is fair to say that 3D printing is revolutionizing the manufacturing landscape. Can you imagine sending a 3D print of your feet to have a pair of shoes customized for you? This is not really that far-fetched.

Modern 3D printing, also known as additive manufacturing, is the process of making a three-dimensional solid object of virtually any shape from a 3D model or other electronic data source. As an additive manufacturing method, the manufacturer “adds” material to an object, layer by layer, to create the final product (**Figure 1**). Given the staggering sudden growth of 3D printing and the several different 3D printing methods, all indications suggest that 3D printing is, or should be, considered a disruptive technology.[1] Following from that assertion, to say that 3D printing will change the world is not at all a stretch.

Figure 1. Sample objects created by 3D printing. Photo courtesy of 3DPS.

The 3D printing technique has been evolving to create 3D models and prototypes in the automotive, aerospace, healthcare, and consumer industries. Aficionados believe that these 3D models could help companies complete a project in less time and/or with fewer resources. Consequently, 3D printing is emerging quickly,[2] the impetus for a radical shift from rapid prototyping to rapid manufacturing. This is, indeed, a disruptive technology.

For vendors in this space, the dream is to put a 3D printer in every house. Costing often from $2,000 (U.S.), some 3D printers are now priced just under $1,000 (U.S.).[3] Many see this as a fast-evolving market, still in its infancy. Canalys, an independent market research firm, predicts that the size of the overall 3D printing market (including printer sales, materials, and related services) will rise to $3.8 billion in 2014; that by 2018 the market will amount to $16.2 billion, an expected 45.75% CAGR during that period.[4] Given these forecasted numbers, it is not surprising that 3D printing has received considerable press attention in recent years. As a disruptive technology, it has the power to reshape the industry and change manufacturing processes. Nonetheless, there remain several fundamental barriers to such a remarkable market uptake, including the cost of the printer. Even at less than $1,000 today, a 3D printer is still very expensive for a consumer product.

Is the Razor-Razorblade Model Key to 3D Printing Market Growth?

If you have ever purchased razors and their replacement blades, you have experienced the Razor-Razorblade business model. This business practice involves selling a main item at a discount just so the complementary (often disposable) secondary goods can be sold at a considerably higher price.[5] Beyond razor blades, this business model has been successfully used for the traditional printer market for a long time and continues to be a very successful strategy.

One could argue that this Razor-Razorblade model is the best business strategy and the fastest path for moving a 3D printer to mainstream with a printer in every home. In simple terms, you would dramatically

increase the adoption rate of 3D printing by selling the printer at a much reduced cost, even almost for free, and then make consistent money on the sale of the cartridge spool or printing filament. **Figure 2** below shows an example of a disposable 3D printing filament package.

Figure 2. A Cube® 3D plastic cartridge. (Image provided courtesy of 3D Systems.)

The 3D printer cartridge spool or printing filament will also let the printer support a large combination of materials, colors, and finishes at different price points. Just as with traditional ink cartridges where the customer is given the ink level in each color, the 3D printing filament usage status can be provided as well. As history has taught us well, the Razor-Razorblade model only works when there has been a strong IP protection scheme implemented on the disposable against cloning, counterfeiting, replicating, and imitating.6 There is little doubt that counterfeiters will try to replicate 3D cartridges and defraud the legitimate manufacturers of those products. How can that IP theft be thwarted? The answer is straightforward: embed secure identifying technology into each 3D printer and cartridge.

Security with a SHA-256 Challenge-and-Response Authentication System

For many years in countless products and applications a secure hash algorithm (SHA) authentication scheme has been a very effective way to protect IP from counterfeiting and illegal copying. A SHA-256 security system based on a secure hashing standard, Publication FIPS PUB 180-4, defined by the National Institute of Standards and Technology (NIST) makes for a strong anticounterfeiting or anticloning tool. Secure authentication of disposable products also has the positive affect of controlling material quality which, in turn, greatly affects the manufacturer's brand identity.

As a short digression here, Maxim's DeepCover® secure authenticators like the DS28E15 with 1-Wire® interface and 512 bits user EEPROM have enjoyed a front-runner position in many embedded applications. System designers have used the DS28E15 to protect their R&D investments because this authenticator implements advanced physical security and provides the ultimate in low-cost IP protection.

The SHA-256 communication involves a symmetric key-based bidirectional challenge-and-response authentication scheme. It is a hand-shaking protocol in which one party (the host or master, and in our discussion, the 3D printer) presents a secret question or *challenge* to another party (the slave, and here, the cartridge or spool). The slave must provide a valid answer or *response* in order to be authenticated. The slave cartridge's response, moreover, depends on both the challenge that it receives and its stored secret response. If the cartridge answers the secret question wrong, then the printer will reject the cartridge.

The major components of the authentication scheme include the 256-bit random challenge, the cartridge's ROM ID, and the secret that is unique and embedded in each slave IC at the manufacturing stage. The secret is programmed into the protected memory of a SHA-256 secure authenticator, the DeepCover DS28E15. The same secret is also programmed into the secure host authenticator, the DS2465, in the printer cartridge. A strong and secure secret key-management scheme is necessary to protect the secret key from being compromised.

Immediately after a cartridge is installed into a secured 3D printer, the following sequences of events occur **Figure 3**).

- 3D printer reads out the cartridge's ROM ID (i.e., stored in the DS28E15).
- 3D printer generates and sends a random challenge to the cartridge.
- Cartridge computes a SHA-256 message authentication code (MAC) using its ROM ID, secret, the random challenge received, and some other data elements. The cartridge sends this to the printer host.
- 3D printer then locally computes its own MAC with its locally stored secret, the random challenge (the same one which was sent to the cartridge), and the ROM ID collected from the cartridge.
- 3D printer compares the value of its MAC against the one computed by the cartridge.
- If the two MACs match, the cartridge is authenticated. This essentially means that the cartridge is genuine. With the cartridge's authenticity verified, the 3D printer might then read additional data from the cartridge's memory, such as the date, place of manufacture, lot number, filament material and colors supported, and material usage level. However, if the MACs do not match, the cartridge is a deemed a fake, knock-off, or counterfeit. The printer then immediately disables all printing functions.

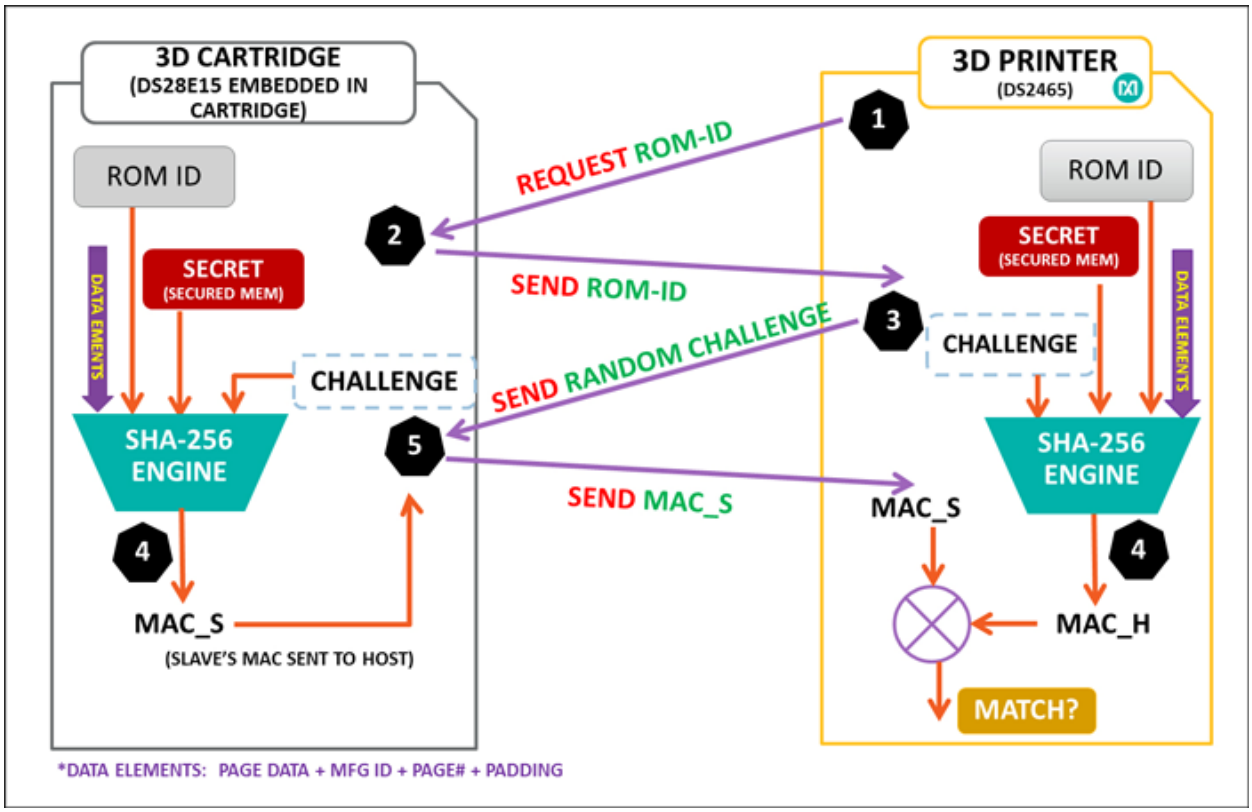

Figure 3. Diagram of a SHA-2-based challenge-and-response authentication transaction sequence for a 3D cartridge.

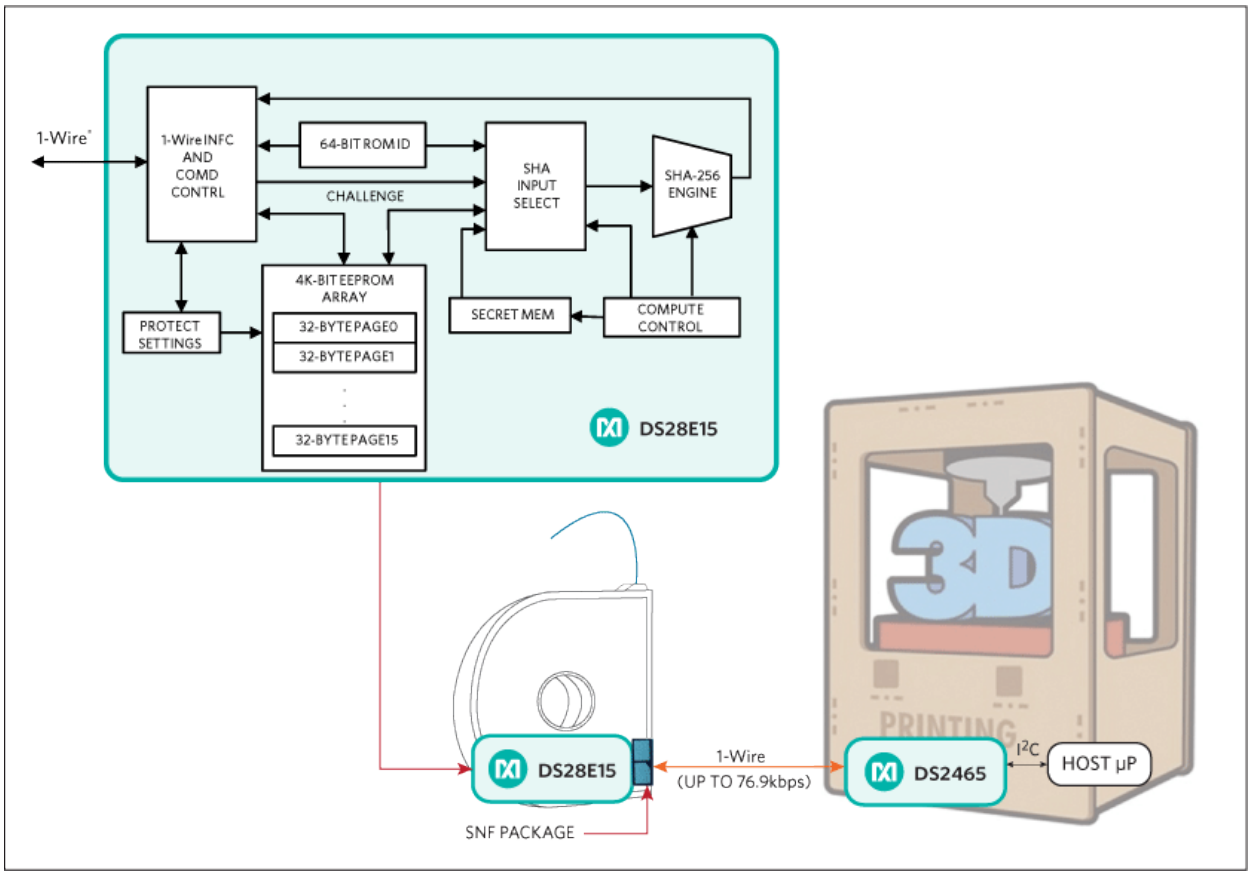

Figure 4. A SHA-2-based secure authentication circuit implementation. This illustration shows the DS28E15 DeepCover secure authenticator connected via the 1-Wire interface to the DS2465 SHA-256 coprocessor, which helps to compute the MAC on the host side before the authenticating comparison is made.

Figure 4 illustrates how SHA-256 authentication is embedded in a 3D printer and companion ink cartridge. A DS28E15 secure authenticator is the essential, protection device embedded in the host 3D printer. The 3D printer with the DS2465 (i.e., the host master) will only accept an authentic response from a genuine cartridge (i.e., slave). All this communication happens over a 1-Wire communication interface which, in this case, is also how the DS28E15 is powered on the cartridge. This authentication scheme assumes that both the 3D printer and the cartridge have the same SHA secret which was programmed during manufacture in a secure factory environment.

The DS28E15 secure authenticator has another distinct advantage. It is built with its own unique 64-bit serial or identification number (ROM ID) used as one of the inputs of the SHA-256 engine. This makes each 256-bit MAC a unique number. The DS28E15's memory can also be partitioned into areas with open access (e.g., unprotected) and into areas where the host (printer) must authenticate itself to the slave (cartridge) for EEPROM write accesses. Several protection modes are available and described in the data sheet.[7]

When EPROM Emulation (EM) protection mode on the DS28E15 is activated, individual memory bits can only be changed from 1 to 0, but not from 0 to 1. Once the EM mode is selected, this cannot be reversed.

This essentially represents the best avenue to implement a countdown or limit usage features on the cartridge which can be extremely challenging to defeat. This usage-limit feature bars a user from forcing the cartridge packaging open to add their own filament martials.

The memory protection modes on the DS28E15[7] also provide a platform or means on the 3D printer to support other features. These features include the printer's ability to support different print job finishes or to create objects using a greater combinations of materials and colors. These capabilities are ultimately the key features which will contribute to the market uptick of 3D printing.

Conclusions

Sadly, it is common for a supposedly secure disposable product to be attacked by a variety of sophisticated die-level methods to extract secure data and/or reverse device settings. All this is done to compromise system security for the sole purpose of cloning or counterfeiting it. To provide the highest affordable protection against this inevitable malicious attack, the DS28E15 employs proprietary die-level physical techniques, circuits, and cryptographic methods to protect sensitive data, control signals, and secret keys.

Maxim has a long track record, 20+ yrs of R&D, in making embedded security solutions to protect diverse end markets including financial, print consumables, medical consumables, computing, gaming, energy metering. Maxim's expertise with crypto algorithms, complex IC-level physical protection implementations (e.g., advanced die-level physical security), and customized IC packaging remain key to helping for customers protect their R&D investments.

Could the DS28E15 DeepCover secure authenticator protect 3D cartridge manufacturers from clones and counterfeits? Could it eventually drive consumers to adopt 3D printing faster and have a 3D printer in every home? Yes. With the SHA-based challenge-and-response authentication scheme implemented in the DS28E15, the 3D printer market can ensure that a genuine and vetted cartridge is being used. With their assets, IP, and brand quality protected, the printer market can then shift a sizeable portion of revenue from the sale of the printer to sale of the disposable cartridges.

As history has taught us, the Razor-Razorblade model works only when there is a strong IP protection scheme implemented against cloning, counterfeiting, replicating, and imitating disposables. The DS28E15 DeepCover secure authenticator IC is the right path for selling more 3D printers.

References

1. **WhatIs.com** defines "disruptive technology" as "a term coined by Harvard Business School professor Clayton M. Christensen to describe a new technology that unexpectedly displaces an established technology." References for additional references are noted with the article at
2. Canalys Senior Analyst Tim Shepherd notes, "We are already seeing significant numbers of early technology adopters and hobbyists investing in relatively cheap 3D printers. As prices continue to fall, the technology improves and use cases are tested, this trend is set to continue…." See *3D printers gaining significant traction among consumers*, **canalys**, June 24, 2014, http://apac.canalyschannelsforum.com/site/news?id=5.
3. Low-end printers are typically priced between $2,000 and $1,000. See Canalys report where Canalys Research Analyst Joe Kempton writes: "In reality, there is a good number of basic printer models coming to market at sub-US$1,000 price points, and some crowdfunding projects promise sub-

US$500 prices…" See *3D printers gaining significant traction among consumers*, **canalys**, June 24, 2014, http://apac.canalyschannelsforum.com/site/news?id=5.

See also. "How Much Does a 3D Printer Cost? Still Expensive, But Becoming More Affordable," **arts.mic**, May 10, 2013, http://mic.com/articles/41111/how-much-does-a-3d-printer-cost-still-expensive-but-becoming-more-affordable.

For a discussion of some very expensive 3D printers that range from $10,000 to $50,000, see Lumb, David, "The Top Nine Consumer 3-D Printers For Every Budget," **Fast Company**, www.fastcolabs.com/3016490/9-consumer-3-d-printers-for-every-budget.

For more about the dropping prices of 3D printers, see "How Much Does a 3D Printer Cost?" **inkpal.com**, www.inkpal.com/ink-news/how-much-does-a-3d-printer-cost/.

4. Canalys reports on the 3D printing market: "The size of the market, including 3D printer sales, materials and associated services, reached US$2.5 billion globally in 2013. Canalys predicts that this will rise to US$3.8 billion in 2014, with the market continuing to experience rapid growth, reaching US$16.2 billion by 2018. This represents an expected compound annual growth rate (CAGR) of 45.7% from 2013 to 2018." See *3D printing market to grow to US $16.2 billion in 2018*, **Canalys**, Monday 31 March 2014, www.canalys.com/newsroom/3d-printing-market-grow-us162-billion-2018.
5. There are many discussions of the Razor-Razorblade business model on the Internet. Some suggested sites where you can learn about the practice include: www.investopedia.com/terms/r/razor-razorblademodel.asp, www.businessdictionary.com/definition/razorblade-model.html, and http://en.wikipedia.org/wiki/Freebie_marketing.
6. You will find considerable discussion about counterfeit printer ink cartridges on the Internet. For a general background on the problem, go to Edwards, Cliff, "HP Gets Tough on Ink Counterfeiters," BloombergBusinessweek, May 28, 2009, www.businessweek.com/magazine/content/09_23/b4134044747987.htm. For a discussion of how to recognize counterfeits, go to, Shea, Mark, "How to Identify Counterfeit Ink," PCWorld, Dec 2, 2010, www.pcworld.com/article/212183/identify_counterfeit_ink.html. A general Internet search on "counterfeit ink cartridges" will present many other accounts of the problem.
7. More details about the protection modes in the DS28E15 can be found in the data sheet.

A similar version of this application note appeared November 21, 2014 in *EDN*.

Related Parts		
DS2465	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/en/support
For Samples: http://www.maximintegrated.com/en/samples
Other Questions and Comments: http://www.maximintegrated.com/en/contact

Application Note 5940: http://www.maximintegrated.com/en/an5940
APPLICATION NOTE 5940, AN5940, AN 5940, APP5940, Appnote5940, Appnote 5940, A1247