Securing Anti-Counterfeiting Technologies

Louis M Parks at SecureRF Corporation discusses the importance of ensuring products are protected from counterfeiting, and suggests strategies to provide the highest level of security

Using automatic identification methods, such as barcodes or radio frequency identification (RFID), as part of item-level packaging, is seen as a way of protecting pharmaceutical products from counterfeiting and other threats. These technologies can also be used to automate electronic pedigrees, supply chain management, reverse logistics and inventory control. Pharmaceuticals must be protected from counterfeiting and theft because these affect public safety and drive up consumer drug prices. But barcodes and RFID tags used on pharmaceutical packaging must be secured if they are to provide any real protection.

Threats to the pharmaceutical supply chain include stolen products, unapproved generics, re-introduction of expired products, counterfeits, up-labelled products, diverted products, and parallel imports. The World Health Organization estimates that the percentage of drugs which are counterfeit range from around one per cent of sales in developed countries to over 10 per cent in developing countries, depending on the geographical area (1). The US-based Centre for Medicines in the Public Interest estimates that, globally, counterfeit pharmaceutical commerce will grow to become 16 per cent of the aggregate size of the legitimate industry, a six percentage-point increase from 2004. This illegal business will generate $75 billion in revenues for its participants in 2010, a 92 per cent increase from 2005 (2).

There are several anti-counterfeiting strategies that should be implemented together. Packaging should be tamper-evident or tamper-resistant, similar to that used in the food industry, so consumers can tell when the product has been compromised. Manufacturers should use overt, covert and forensic authentication features on the products themselves. Product identification, pedigree and tracking should be carried out at item level and automated identification techniques will help to facilitate this process.

In addition to the product itself, the packaging, which can include barcodes and RFID tags, can be counterfeited. "Drug companies need to be seen doing everything they can to secure their supply chains," says Daniel W Engels, Director of the Healthcare Research Initiative at MIT. "Security and privacy will have to be addressed more fully than they have been, because when we create a network information system that spans the globe – as the pharmaceutical supply chain does – the data won't always be protected by virtual private networks (VPNs) or other secure networks" (3).

Some firms prefer barcodes as the automated identification method for item level packaging because they are familiar with the technology, and because barcodes are inexpensive to print and apply. When a barcode is pre-printed as part of a product's packaging, it cannot be used to identify counterfeit products because they do not provide item level identification and are susceptible to easy reproduction. Barcodes can be generated with data that changes for each individual dose via a variable data printer, either on an in-house printing line or at a contract partner's facility. The occurrence of a duplicate code, as identified by a barcode reader that is tied to a central database of valid identification codes, could trigger an investigation of a possible counterfeit or altered product.

In May 2007, the European Federation of Pharmaceutical Industries and Associations (EFPIA) announced its support for 2D Data Matrix barcoding as a pan-European and industry-wide anti-counterfeiting solution. In May 2009, the EFPIA announced an upcoming pilot of its coding and identification solution in Sweden, in partnership with Swedish retail pharmacy chain Apoteket AB and local wholesalers Tamro and KD.

Under the EFPIA solution, "pharmacists will check a unique identification code on each individual pack when it is dispensed to the patient. These codes are generated and applied by manufacturers using a simple 2D Data Matrix barcode, which contains a unique serial number. The scan will reveal any duplication of data on packs and will trigger the system to immediately alert the pharmacist to the possibility of a counterfeit product, who can take the necessary steps" (4). This solution presumes that all data will be collected in a central location in a timely fashion and can be queried against at any time from almost anywhere. This opens up a list of questions. Who is going to be responsible for storing and managing this data? Who will pay for it? Are pharmaceutical firms willing to share their data with everyone else in the supply chain? With this solution, a pharmaceutical company still loses, because you cannot tell which product is the counterfeit, so if the fake product was dispensed first, then you are going to end up holding back the genuine product when you get a 'duplicate' hit.

The other auto-identification option is a passive RFID tag, which costs more than a barcode but offers other benefits. In comparison to 2D barcodes, it does not require line of sight for accurate reading of product information, and can scan multiple products at any given point in time. This characteristic significantly reduces the handling costs. RFID readers can also write data to a tag, thus data can be added or changed at any point in the production line or supply chain, enabling pedigree information to be stored directly on the tag. Passive RFID tags have no batteries or external components, and are powered purely by energy contained within the incoming RF signal. To keep the cost of a passive RFID device low, the area of the silicon is small and the RFID circuit cannot be complex. Passive RFID tags, which vary in size, shape, and style, can be embedded into a cap, wrapped around a vial, or printed on a label.

Adoption of RFID "ensures a good return on investment for pharmaceutical manufacturers as well as distributors", a report from Kalorama Information contends. Large manufacturers can save between $17 and $55 million and major distributors up to $10 million per year by implementing the technology, it calculates (5).

While the pharmaceutical industry recognises the critical need for packaging security and the benefits of RFID, there is also a need to identify what is required in an RFID tag from a security perspective. By using unsecured RFID tags, the pharmaceutical industry is introducing a new set of risks to the supply chain, perhaps inadvertently. Forrester Research said of unsecured tags that "the weakest link in the security chain is the RFID tag – in particular, the so-called passive tag" (6).

Unsecured RFID systems face security threats that include clandestine scanning, tracking, cloning, and even eavesdropping. The inclusion of any product information on the drug itself creates several exposure issues. Firstly, patients carrying sensitive drugs may not want to be identified with them.
Equally importantly, when it comes to high value or FDA Schedule B drugs, the manufacturers may not want to broadcast where or what is inside a tote when in transit to a wholesaler or pharmacy. Unprotected tags can be scanned to obtain detailed data on the tagged asset. If the tag contains a unique ID, then it can enable an unauthorised party to track the movements of the asset even if they did not read the actual descriptive data contained on the tag. Even in the case where an encryption key is used to protect data on a tag, unless the key can be changed, the reader/interrogator that receives the key now has undetectable access in perpetuity.

This security issue is especially viewed as a priority among key players in the pharmaceutical industry. According to Sara Shah, an analyst at ABI Research, "Security is definitely on the minds of supply chain managers, consumers and technologists. Security is not something that has been completely lacking, but it is definitely reduced in the RFID market – and the UHF market in particular. It hasn't been a huge issue in the consumer-goods retail supply chain market, but with the pharmaceutical market, security is a much bigger issue" (7).

So what is security? It is a collection of mechanisms, procedures and controls that can be implemented to

Table 1: Sample DREAD analysis comparing three Auto-ID solutions for anti-counterfeiting

Category	Unsecured tag	Unsecured tag with serialisation	Secured tag with serialisation
Damage potential	10 – If compromised, expired, tampered, or otherwise counterfeit drugs could enter the supply chain.	10 – If compromised, expired, tampered, or otherwise counterfeit drugs could enter the supply chain.	10 – If compromised, expired, tampered, or otherwise counterfeit drugs could enter the supply chain.
Reproducibility	10 – Since the tag or barcode has little inherent security, it is easily compromised	5 – Since the tag or barcode has little inherent security, it is easily compromised. But if it is cloned, it can be easily detected through checks against a centralised database or back office support systems.	1 – The private key of the tag is provisioned at the time of drug manufacture and cannot be read from the tag. Public keys are stored securely at a trusted third party (TTP). Tags cannot be re-provisioned in the field unless they have trusted access to the TTP. Cost to reverse engineer private key from tag is high and only compromises a single tag. If tag is cloned, then it can be easily detected through velocity checks at TTP and back office support systems.
Exploitability	10 – Re-use of the tag or barcoded packaging cannot be detected.	5 – Re-use of the tag or barcoded packaging can be detected through checks against a centralised database or back office support systems.	2 – Utilise checks against a centralised database or back office support systems to identify tag re-use or duplication. Other counter measures are in the key lifetime, for example, let the key expire when the drug expires. Tags that are damaged or disabled when moved, thus preventing re-use, can also be implemented as a physical security feature.
Affected users	10 – Drug wholesalers, pharmacies and consumers would be affected by having counterfeit drugs in their supply chain.	10 – Drug wholesalers, pharmacies, and consumers would be affected by having counterfeit drugs in their supply chain.	5 – Drug wholesalers, pharmacies and consumers would be affected by having counterfeit drugs in their supply chain.
Discoverability	8 – Would require someone who can scan or copy a barcode and print on a new package. Copying RFID tags is slightly harder.	5 – Would require someone who understands how data is generated and applied to the barcode or RFID tag and how it is used with the back-end systems.	1 – Counterfeiting would be very difficult, if not impossible. In order to have a successful attack, access to the provisioning tools for the tag and access to the TTP and back-end systems would be required. This could be accomplished by an insider, but could be detected by velocity checks and other forensic and/or intrusion detection analysis.
DREAD score	9.60	7.00	3.80

reduce the risk of specific threats. Examples include:

- Authentication – the act of establishing or confirming the identity of a person or machine, or assuring that a computer program is a trusted one
- Digital signatures – a type of asymmetric cryptography which gives the receiver reason to believe the message was sent by the claimed sender
- Encryption/Decryption – a cryptographic process of transforming information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Decryption is the reverse, making the encrypted information readable again. Depending on the type of cryptography used, keys can be public or private
- Hash functions – a mathematical function which converts a large, possibly variable-sized amount of data into a small datum in order to speed up table look-up or data comparison tasks such as finding items in a database or detecting duplicated or similar records in a large file

Depending on the application, these security methods should be used in different combinations and must be balanced against the apparent and real risks. One tool that can be used to evaluate the appropriate level of security is the DREAD model, which documents damage potential (data compromise, theft and reputation) and cost (to business, to repair or loss).

DREAD is a classification scheme for quantifying, comparing and prioritising the amount of risk presented by each evaluated threat. DREAD modelling influences the thinking behind the risk rating, and is also used directly to sort the risks. The DREAD algorithm, shown below, is used to compute a risk value, which is an average of all five categories:

Risk DREAD = (damage + reproducibility + exploitability + affected users + discoverability) / 5

The calculation always produces a number between zero and 10; the higher the DREAD risk number, the more serious the risk.

Table 1 (page 67) shows a sample DREAD analysis comparing three automatic identification solutions used for pharmaceutical anti-counterfeiting. The first example is an unsecured RFID tag or barcode where the same code is used for every instance of a particular product. The second example uses an unsecured RFID tag or barcode with serialisation, a unique code for every individual dose and the use of a centralised database of codes as suggested in the EFPIA's solution. The third is a secured RFID tag that uses serialisation with a centralised database and contains multiple anti-counterfeiting features. A secure tag may also include encryption and authentication to address clandestine scanning, tracking and eavesdropping issues. This analysis represents a range of options and the estimation of each DREAD score may vary.

The DREAD score varies widely based on what features the barcodes or RFID tags have, but they are just one piece of the system. One needs to view automated identification solutions as a network comprised of multiple components:

- RFID tags or barcodes
- Readers
- Middleware software to process all of the data that is collected
- Networks
- Database, perhaps centralised and distributed to all participants in the supply chain

Each of these components will need to use different security counter-measures to prevent attacks at any point in the supply chain. Having a tag or barcode with anti-counterfeiting features is a start, but does not comprise the whole security or trust model. Standards, responsibility, data ownership and cost-sharing all need to be determined. This is an area for further research and discussion within the pharmaceutical industry.

About the author

Louis Parks is a co-founder of SecureRF. As CEO of the company, Louis has helped to guide the development of new cryptographic solutions and security tools for low-resource and embedded devices like radio frequency identification (RFID) and microcontrollers (MCU). With over 21 years of senior management experience, Louis' primary roles have been in sales and marketing of technology and enterprise software solutions. Prior to co-founding SecureRF, he held operational roles assisting early and mid-stage technology companies with funding, staffing, operations and strategy. His previous positions have included Senior Vice President of Marketing for G-Log, an innovative internet logistics company and 10 years as CEO/President of Client Technologies, Inc, a provider of customer relationship management (CRM) applications specifically designed to serve the financial community. Email: lparks@securerf.com

References

1. World Health Organization, Fact sheet N 275, Revised 14th November, 2006, www.who.int/mediacentre/factsheets/2003/fs275/en
2. *21st Century Health Care Terrorism: The Perils Of International Drug Counterfeiting*, Center for Medicines in the Public Interest, 20th September, 2005, www.cmpi.org/uploads/File/21st-Century-Terrorism.Report.pdf
3. Cracks in the Pharmaceutical Supply Chain, *CIO Magazine*, 15th January, 2006. www.cio.com/article/16565/cracks_in_the_pharmaceutical_supply_chain
4. EFPIA announces launch of anti-counterfeit coding pilot project in Sweden, 15th May, 2009 www.efpia.eu/Content/Default.asp?PageID=559&DocID=6886
5. US pharma RFID market set for 60 per cent growth, *In-Pharma Technologist*, 10th March 2008 www.in-pharmatechnologist.com/packaging/us-pharma-rfid-market-set-for-60-per-cent-growth
6. Stamp P, Forrester Research, Anyone Who Says RFID Is "Completely Secure" Is Selling Something, 15th August, 2006
7. New Security-Laden RFID Tag Targets Pharma, RFID Update, 17th November, 2006, www.rfidupdate.com/articles/index.php?id=1248