Epothecary: Cost-effective Drug Pedigree Tracking and Authentication Using Mobile Phones

Michael Paik
New York University
mpaik@cs.nyu.edu

Jay Chen
New York University
jchen@cs.nyu.edu

Lakshminarayanan Subramanian
New York University
lakshmi@cs.nyu.edu

ABSTRACT

Counterfeit and expired pharmaceuticals are a significant problem in the developing world, constituting up to 80% of stock on pharmacy shelves. This is due both to poor existing controls and to lack of supporting infrastructure on which to build such controls.

Existing strategies to fight counterfeiting include holograms, special packaging, and paper invoice tracing, but each of these have been proven ineffectual in the face of increasingly sophisticated counterfeiting rings, which inject fake drugs into the market for profit and/or sell off genuine medications on the black market or in adjacent countries at marked up prices.

This paper describes Epothecary, a system which uses built-in functionality in midlevel mobile telephones including cameras, SMS, and optionally GPS to construct a robust system for tracking and verifying the pedigrees of pharmaceutical products at every point in the distribution chain, particularly in the developing world.

Categories and Subject Descriptors

C.2.4 [**Computer - Communication Networks**]: Distributed Systems—*Client/Server*; H.1.2 [**Information Systems**]: User / Machine Systems—*Human Factors*; H.4.2 [**Information Systems Applications**]: Types of Systems—*Logistics*; I.7.5 [**Document and Text Processing**]: Document Capture

General Terms

Design, Human Factors, Economics, Security

Keywords

Pedigree, Counterfeit, SMS, Barcode, Track & Trace

1. INTRODUCTION

According to estimates from the International Chamber of Commerce [1], counterfeit goods constituted some 5-7% of all global trade as 1997, with similar figures for the multi-billion dollar pharmaceutical trade. While this is a problem in the developed world, it is endemic in the developing world, with the counterfeit rate of certain high-volume drugs reaching up to 80% [6, 13, 28].

Counterfeiting of other types of goods, such as luxury goods or music, results in economic loss, but counterfeiting of pharmaceuticals poses a clear and present danger to lives and livelihoods, being subtherapeutic at best and poisonous [23] at worst.

1.1 Existing Approaches

The two types of measures used to enforce authenticity are *overt* and *covert*. We consider the former category as the latter provides no assistance to the end-user in detecting counterfeit products. Among these, common examples include special packaging, holograms, iridescent or optically variable films, and RFID tags.

Packaging [19] and holograms [5] have proven to be little defense against counterfeiting, as counterfeiters with the capacity to make facsimilies of drugs typically have access to offset and hologram printing capacity.

Track & trace systems are essentially absent in the context of the developing world, as the network infrastructure present is not adequate to run existing systems as used in the developed world. As such, the typical methodology relies heavily on paper invoices and signatures, both of which are easily falsifiable.

1.2 Motivation and Scope

The impetus behind Epothecary is to provide both authentication and track & trace functionality in the developing world at low cost using existing infrastructure capacity. We do this by leveraging the installed base of GSM mobile phone networks, which have high penetration [8] even in some of the most rural and remote regions of the world, and midlevel handsets with integrated cameras and optionally using GPS antennas.

The system is designed to provide end users, retailers, and middle distributors with a reasonable guarantee of drug authenticity by recording all transactions involving medications. Should counterfeit medication be introduced into the system, it also provides a mechanism for tracing possible points of entry.

Epothecary can also be used to track entry points and subsequent distribution of substandard or subtherapeutic medications manufactured by otherwise legitimate pharmaceutical companies. It is not, however, designed to track

SIGCOMM MobiHeld 2009 Barcelona, Spain

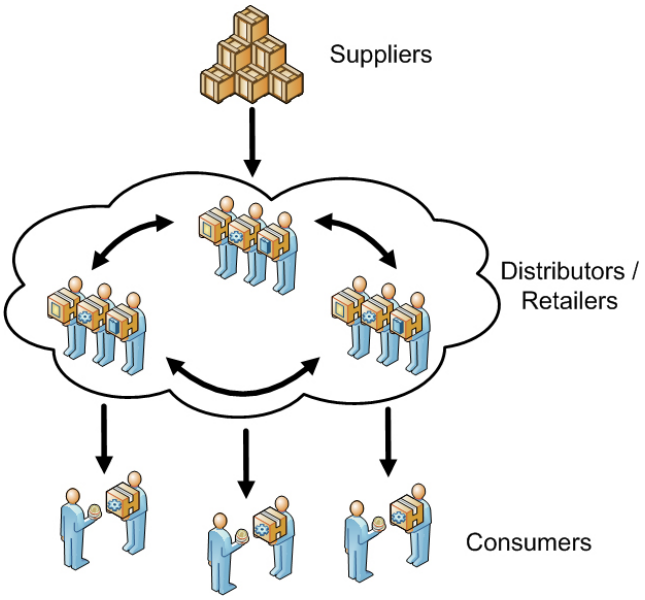

Figure 1: Simple supply chain

sales outside the system, e.g. on the gray or black market; it is expected that consumers understand they receive no warranty on the authenticity of products purchased through these channels.

2. SYSTEM OVERVIEW

2.1 Supply Chain Flow

The typical supply chain for pharmaceuticals in the developing world is shown in Figure 1. Suppliers break up large lots and sell to distributors and retailers, who may break them up further while selling them to consumers and each other. This deviates from the standard in the developed world, where such chains are typically strictly linear (hence, chain) and decreasing in sale size.

2.2 Design

Any track & trace system must at minimum have a method of reporting transactions to a central server, and in the developing world, it is a given that these transactions must be recorded by a human rather than by sophisticated and expensive machinery.

We therefore wish to make maximum use of existing skills and technological capacity to reduce overall training, capital, and marginal costs, and make these considerations primary in our overall design.

2.2.1 Infrastructure

Existing GSM installations provide some degree of network capacity in the developing world, and higher bandwidth solutions such as GPRS are available in many densely populated areas. We therefore choose SMS over mobile phones, which has a 140-byte payload per message, as our primary delivery mechanism, and use GPRS where available. This greatly increases the availability of our system as the SMS metaphor also holds on most international satellite-phone systems (e.g. Thuraya), providing access virtually anywhere with a clear line-of-sight to the sky. 140 bytes

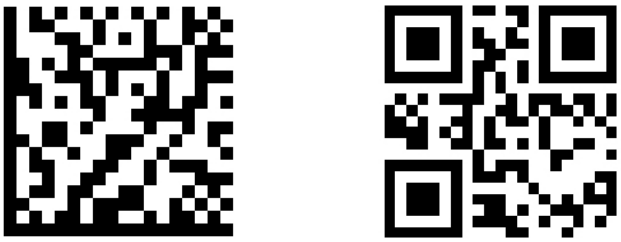

Figure 2: DataMatrix (left) and QR Code (right) glyphs of a random 20-digit number and the 4-digit month and year `0410`

proves sufficient for the small messages described in the protocols below.

In addition, mobile telephones are self-contained, typically nearly maintenance-free, physically robust in harsh environments (as readily demonstrated looking at handsets anywhere in Africa or Southeast Asia), and have low power requirements.

The system is trivially adaptable for use on PCs at higher-volume locations which have network connectivity through the use of commodity barcode scanning equipment. Furthermore, in places where telephone company cooperation can be assumed, the Unstructured Supplementary Service Data channel (USSD) provides an additional possible channel for data communcations.

2.2.2 Human Factors

Introducing new technologies always incurs a training cost, and therefore the use of mobile telephones saves at least part of this cost, presenting a familiar interface and usage metaphor to a largely numerate userbase.

In order to further reduce operator error and training costs, we make use of an integrated cameraphone, included in many low-cost handsets today, rather than requiring users to manually enter text or numbers. 2D barcodes of various types have been shown to have low error rates even when scanned by low-resolution cameraphones [12], are robust against damage when encoded with Reed-Solomon error correction, and can carry arbitrary amounts of data either by using larger glyphs or multiple smaller glyphs in sequence. The use of 2D barcodes also facilitates the entry of alphanumeric data by semiliterate users [22].

2.2.3 Asset Identification

Our strategy is to label packaging units at each level of granularity - e.g. pallets, crates/cartons, dozens, and individual units, with ID glyphs, packaged in such a way that opening e.g. a carton exposes the tags for the each of the 12 dozens in the gross (144). In addition, each non-consumer participant in the system is similarly assigned an ID number.

Each ID number is an integer uniformly randomly distributed between 0 and $10^{20} - 1$, the universe of 20 digit numbers with a four-digit month/year expiration date appended, and is printed in human-readable format on the same tag as the glyph.

Annual per-capita consumption of pharmaceuticals varies widely (e.g. Spain's in 2005 was approximately 30 units including over-the-counter medications whereas Brazil's was approximately 9.5 [2,3]). Even assuming the higher number,

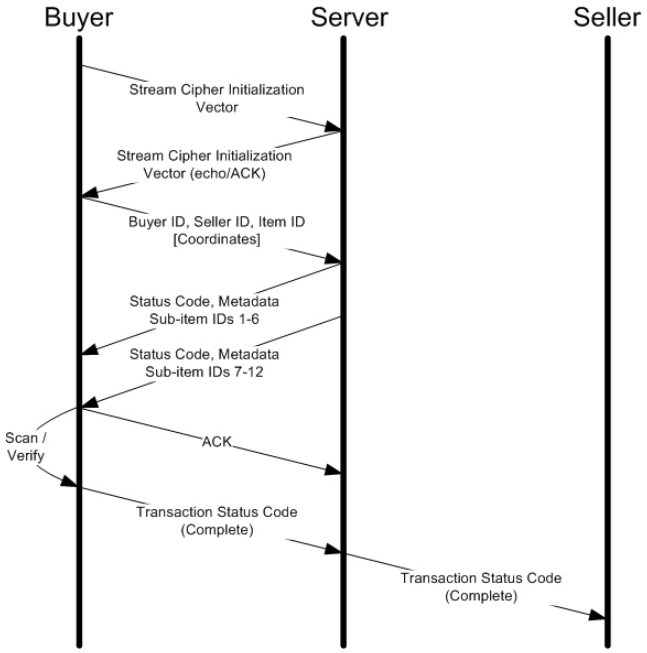

Figure 3: Protocol message flow for a successful transaction of a larger unit, e.g. a carton

the total number of units in circulation at any given time in a given country (e.g. India) can be bounded in the tens of billions, which can be handled using a few commodity computers and readily available database software such as MySQL with the InnoDB engine.

2.2.4 Protocol A: Supplier/Distributor/Retailer

Each non-consumer participant receives or purchases a cameraphone from the applicable regulatory body (e.g. NAFDAC in Nigeria). Each such user also receives a photo ID card with a unique ID glyph printed on it, with standard counterfeiting protections, and chooses a password for use with the system, to be changed at regular intervals.

The cameraphone is preinstalled with Epothecary and a random symmetric key for use with a stream cipher, unique per user, itself weakly encrypted with the chosen password and to be refreshed at the same intervals as the password. The Regulatory Body (RB) further records GPS coordinates for each user's place(s) of business and the phone number of the SIM the user will use with the phone.

We assume shipments arrive at the suppliers from external sources pre-tagged, and that the RB has received information about the IDs from the manufacturer through a secure channel, e.g. email secured with strong public-key encryption. We further assume for the purposes of this paper that the RB is impregnable; normal auditing is of course necessary but dealing with corruption at the regulatory level is not the purpose of this system. Every subsequent sale in which an end consumer is not a participant proceeds as follows:

1. The purchaser starts the Epothecary application on his phone and enters his password, which is checked against a hash of the password. If this check succeeds, the weakly encrypted keyblock is XORed against a repeated stream of the bits in the password.
2. The purchaser then chooses an option indicating a purchase and follows prompts to scan his own ID tag, the ID tag of the seller, and the ID tag of the item to be purchased, which the application packages, encrypts with the stream cipher key as appropriate. The application then sends an SMS message containing an initialization vector for the stream cipher in cleartext.
3. The RB checks the consistency of the source phone number against its list of valid users, and sends an ACK message containing the same initialization vector if it is present.
4. The purchaser sends the scanned information in ciphertext.
   (a) If the phone is GPS-enabled and a satellite signal is present, coordinates are included in the sent packet.
5. The server at the RB checks its registry for metadata about the item ID supplied, including current registered owner, lot size, medication type, expiration date, and manufacturer. The server performs standard GSM localization [25][1] and ensures that the handset is estimated to be within a reasonable distance of a known address of either the buyer or the seller. If this check passes, the metadata are sent to the purchaser's registered SMS phone number along with the tag keys for any immediately subsidiary units, e.g. the 12 tag numbers for cartons on a pallet. Depending on privacy issues in the local context, the system could also be configured to provide metadata about the seller represented by the ID for verification: age, height, gender, etc.
6. The purchaser checks this information against the item to be purchased for consistency and scans the tags of the subsidiary units. The application then sends an ACK to the RB if the tag numbers match, otherwise a NAK.
7. Upon ACK, the RB updates its registry to change the current owner of the item to the purchaser, inserts a transaction record, and sends an ACK to the registered phone number of the seller. Upon NAK, the RB tags the item for investigation and any subsequent transaction requests on it or any of its subsidiary units at any level return alerts rather than metadata.

2.2.5 Protocol B: Retailer/Consumer

It is intractable to provide every potential consumer with an ID number and appropriate equipment and credentials, so the protocol differs when individual units are sold to end customers. In particular, this is considered the end of the supply chain, so consumers are not able to resell the medication. The modified protocol operates as follows:

1. The seller starts the Epothecary application as in Protocol A, but chooses an option indicating a sale to a consumer, then follows prompts to scan his own ID tag and the ID tags of any units being sold.

[1]The crudest form of GSM localization has a precision of 32km at worst in areas with only one GSM cell. In urban areas where large distributors are likely to be, accuracy rises to approximately 550 meters.

2. This information is sent to the RB, which checks it for ownership consistency and location feasibility as in A, marks all indicated units as sold, and sends a summary to the registered phone number of the seller, along with a uniformly random 8-digit reference number.

3. The consumer can SMS this reference number, which remains valid for some period (7 days, for example, in case the consumer doesn't have immediate access to a phone) to an alternate public-facing number for the RB, and will receive SMS messages detailing purchase metadata.

3. ANALYSIS

3.1 Assumptions

We assume that any underlying issues with SMS reliability are handled using the solution outlined in [15] and fall outside of the scope of this paper.

Furthermore, as mentioned earlier, we ignore the question of corruption or collusion at the highest level as a regulatory rather than a technical problem, but a robust system of checks and regular audits would ameliorate this problem. In terms of the security model, we consider the RB a trusted party. Similarly, we consider the telephone company a trusted party and take no measures at the application level to ensure that messages are delivered and routed properly, though such checks could periodically be performed out of band.

We do not assume that the GSM traffic between the handset and the base station is secure, as some installations send traffic in cleartext. Rather, we rely on the application-level encryption outlined in the previous section to provide a reasonable level of security, augmenting A5/1 or A5/2 where available.

We assume that any party in any legitimate company, as well as external, unapproved parties, may try to attack the system, either independently or through collusion with each other, and have designed the system to detect fraudulent transactions regardless of whether the attacker is authorized to use the system or not.

3.2 Security and Technical Attack Vectors

3.2.1 Replay Attacks

SMS messages are both sniffable and spoofable in the wild [20]. In order to prevent naive replay from injecting false failing transactions into the system, we augment each message with a transaction ID related to the purchaser's phone number; any transaction ID which has been seen before is ignored. We further augment messages with a simple checksum to prevent partial replays. In addition, we keep an IMEI-to-phone number map at the telco and drop any message whose Originator Address field does not correspond to the IMEI of the submitting handset. This prevents SMS spoofing except by cloned handsets.

3.2.2 Denial of Service

Denial of Service (DOS) attacks against the RB by SMS flooding can be mitigated in several ways. First, we assign it a noncanonical number (e.g. 1234), so no handset can spoof it and receive its messages. We further disable routing of SMS messages to it at the telephone company level except from the set of numbers registered with the RB, which also obviates defense against other vectors such as Internet SMS gateways.

DOS attacks against individual handsets are low-value as they affect only very small parts of the system and present no economic incentive to counterfeiters.

We consider DOS attacks against the GSM network as a whole out of scope for this paper.

3.2.3 Man-in-the-Middle

Man-in-the-Middle attacks are impossible to execute as an attacker cannot stop the GSM network from attempting delivery of messages to their intended destinations. Therefore while an attacker can potentially sniff messages in either direction, it cannot control the communication channel between them.

3.2.4 SIM/Identity Cloning

GSM SIM cloning is commonplace and can be performed with commodity tools using a brute-force attack. However, it requires physical access to the SIM module to be cloned, and is only effective against older SIMs whose authentication key (Ki) is extractable without damaging the SIM. The fact that entering a valid transaction into the system requires several factors (user ID tag, item ID tag, password, cipher key, SIM) means a user whose identity is misused is either in collusion with the attacker or a victim of theft, which leads us to consider nontechnical attack vectors.

3.3 Counterfeit Injection/Substitution

We assume that ID tags themselves are resistant to counterfeiting, using optically variable films or physically unclonable functions such as those described by Sharma et al [26] but accept that this may not provide perfect protection.

Assuming a counterfeiting operation could duplicate any tag to a high degree of accuracy affordably, it could either collude with a legitimate distributor or covertly tamper with existing stock, by replacing legitimate drugs with counterfeits and hoping to sell the originals on the black market. Track & trace would make finding the entry point for these merely a matter of detective work, as any such counterfeits would have to enter the supply chain at the legitimate distributor holding them or they would fail the various checks Epothecary enforces.

For such a switch not to be detected immediately, the shipment replaced would have to match in every particular - ID number, manufacturer, quantity, dosage, expiration date, etc., meaning the counterfeiting ring would have to intercept or steal a shipment, disassemble it to read and duplicate every tag, and repackage the counterfeits in the same units. Currently such an operation would switch the genuine shipment with one of approximately equal size with mass-cloned holograms and packaging manufactured cheaply well ahead of time. Making many copies of a single valid tag would fail because once one unit bearing the tag was sold, any subsequent sales of the unit by the distributor serving as the entry point would fail the checks. As each tag is unique and has to be uniquely copied, counterfeiters completely lose economies of scale.

Thus, cost per counterfeit unit increases whereas the number of units safely saleable without being detected and the rate at which counterfeit units can be prepared and introduced fall dramatically. A counterfeiter might try to print

tag ranges ahead of time hoping to force a collision, but the likelihood of finding a single given instance of such a collision is infinitesimal.

If we consider a case in which a trillion tags are valid and we guess a range of anywhere within 36 months for expiration dates, the probability of a single particular collision is $\frac{10^{12}}{10^{20}*36} = \frac{1}{10^{8}*36}$, and an attacker would have to anticipate 157 tags and group them correctly to replicate a carton of 144 in advance.

3.4 Economic Factors

The system as described has relatively low fixed costs, and marginal costs for use are controllable. Though some expenditure for training, phones, ID cards, etc. is inevitable, because this process augments rather than fundamentally changes the existing channels for transacting business, we do not, for instance, anticipate a need for a significant increase in manpower. Some cost for publicizing the service to prevent spoofing of the entire service by attackers is also to be expected.

The two most important marginal costs are for the tags themselves and for the SMS messaging upon which the system is built. The former is trivially subsumed in packaging costs; simple printing of such tags cost a fraction of a cent per unit, with costs potentially rising somewhat with counterfeit protection. The latter is a more significant issue, with each message costing approximately $0.05 USD in the contexts this system might be deployed in, and with the system using several such messages per transaction.

A pilot in Ghana, mPedigree [7], has an agreement with service providers to allow messages to and from its service to be sent for free. A similar arrangement could possibly be reached for Epothecary, with an added fiscal forcing function: any providers agreeing to provide SMS messaging between Epothecary handsets and the RB would become the de facto official carriers for all participants and receive all revenues from other calls and messages used in the regular course of business, with all others receiving no such revenue.

4. RELATED WORK

Cybercode [24] was the first work to deal with the use of cameras in mobile telephones to scan 2D barcode tags, and other systems such as CAM [22] use similar systems for various other traditionally paper-based tasks.

Lei et al. [18] illustrate the intuition of using tags scanned by mobile phones in the context of counterfeit detection, but do not deal with any practical implementation or security issues in any significant depth.

mPedigree [7] is an ongoing effort geared specifically towards combating the problem of counterfeit drugs in the developing world (Ghana in particular). This approach provides what appears to be an idempotent binary yes/no authenticity response based on an 8-digit code affixed to medication packaging. Based on publicly available information about the mPedigree trial conducted in early 2008, it is unclear how the proposed platform defends against the various attack vectors discussed in 3.2.

In addition, various works [14, 16, 17, 27, 29] deal with the use of RFID tags in authentication and track & trace applications, but these focus on questions of tag security and depend on the presence of robust internet infrastructure for trusted-party verification.

ePedigree [10] provides a standard for recording transactions between parties in a supply chain, but is only a document standard and is not associated with a design or reference implementation of an actual system to execute tracking & tracing. However, IBM [11] and other firms have systems prepared to meet this need, albeit with significant infrastructure, server, and print facility requirements.

5. CONCLUSION

The state of purity and safety controls for pharmaceuticals in the developing world today is nothing short of dismal. In this paper we have presented a technically robust, cost-effective system for tracking, tracing, and authentication of pharmaceuticals. The system is implementable immediately using technologies already deployed on the field and existing low-cost hardware.

While no system can claim to provide an absolute guarantee against counterfeiting, we believe we have erected a significant technical and regulatory barrier to those hoping to prey on the ill. We hope to work closely with institutions in the developing world to deploy a pilot of this system in the near future.

6. ACKNOWLEDGMENTS

We would like to thank various anonymous friends in the developing world for providing key insights into the problems and shortcomings of existing systems, as well as colleagues at World Relief Juba for invaluable field experience.

We would also like to thank Aditya Dhananjay and Ashlesh Sharma for their input and suggestions in the course of preparing this paper.

7. REFERENCES

[1] *Countering counterfeiting: A guide to protecting and enforcing intellectual property rights.* ICC Publishing, Paris, France, 1997.

[2] Brazilian Medicine Sales Rise by Almost 7% in H1, Boosted by Higher Generics Sales. `http://www.globalinsight.com/SDA/SDADetail6700.htm`, 2006.

[3] Figures for 2005 Show Spanish Pharmaceutical Sales up by 6%, Slowest Growth in 12 Years. `http://www.globalinsight.com/SDA/SDADetail6250.htm`, 2006.

[4] WHO | Counterfeit and substandard medicines. `http://www.who.int/medicines/services/counterfeit/en/`, 2006.

[5] CDC Fake Artesunate Warning Sheet No. 5. `http://www.cdc.gov/malaria/pdf/Fake%20Artesunate%20Warning%20Sheet%20No%205%2024%2007%202006.pdf`, 24 July 2007.

[6] NAFDAC Nigeria - Global Trends. `http://www.nafdacnigeria.org/globaltrends.htm`, 2007.

[7] World First Developed in Ghana: Real-time GSM Drug Pedigree Assurance. Talk. Presented at Technology Transformation Seminar, Ghana-India Kofi Annan Centre of Excellence in ICT. `http://www.mpedigree.org/docs/AITI_mPedigree.pdf`, 17 July 2008.

[8] GSM Coverage Maps. http://www.gsmworld.com/roaming/gsminfo/index.shtml, 2009.

[9] Report on BASCAP mission, achievements, work plan, and membership. http://www.iccwbo.org/uploadedfiles/BASCAP/Statements/BASCAP%20Prospectus%202009.pdf, January 2009.

[10] EPCglobal Pedigree Standard. http://www.epcglobalinc.org/standards/pedigree.

[11] IBM. ePedigree feature: Product overview. http://publib.boulder.ibm.com/infocenter/rfidhelp/v1r1/topic/com.ibm.rfid_ePed.help.doc/c_ePedigree_prod_ovr.html, March 2008.

[12] H. Kato and K. T. Tan. Pervasive 2D Barcodes for Camera Phone Applications. *IEEE Pervasive Computing*, 6(4):76–85, Oct.-Dec. 2007.

[13] T. Kelesidis, I. Kelesidis, P. Rafailidis, and M. Falagas. Counterfeit or substandard antimicrobial drugs: a review of the scientific evidence. *Journal of Antimicrobial Chemotherapy*, 60(2):214–236, August 2007.

[14] R. Koh, E. Schuster, I. Chackrabarti, and A. Bellman. Securing the Pharmaceutical Supply Chain. Whitepaper. http://www.autoidlabs.org/uploads/media/MIT-AUTOID-WH021.pdf, 1 June 2003.

[15] A. Kumar, J. Chen, M. Paik, and L. Subramanian. ELMR: Efficient Lightweight Mobile Records. In *In Submission*, 2009.

[16] M. Lehtonen, T. Staake, F. Micahelles, and E. Fleisch. The Potential of RFID and NFC in Anti-Counterfeiting. In *Networked RFID Systems and Lightweight Cryptography Part III*, chapter 9, pages 211–222. Springer, Berlin/Heidelberg, Germany, 2008.

[17] M. Lehtonen, T. Staake, and F. Michahelles. From Identification to Authentication - A Review of RFID Product Authentication Techniques. In *Networked RFID Systems and Lightweight Cryptography Part II*, chapter 9, pages 169–187. Springer, Berlin/Heidelberg, Germany, 2008.

[18] P. Lei, F. Claret-Tournier, C. Chatwin, and R. Young. A Secure Mobile Track and Trace System for Anti-counterfeiting. In *EEE '05*, pages 686–689, Hong Kong, 2005.

[19] C. Lon, R. Tsuyuoka, S. Phanouvong, N. Nivanna, D. Socheat, C. Sokhan, N. Blum, E. Christophel, and S. A. Counterfeit and substandard antimalarial drugs in Cambodia. *Transactions of the Royal Society of Tropical Medicine and Hygiene*, 100(11):1019–1024, November 2006.

[20] S. Lord. Trouble at the Telco: When GSM Goes Bad. *Network Security*, 2003(1):10–12, January 2003.

[21] P. Newton, S. Proux, M. Green, F. Smithuis, J. Rozendaal, S. Prakongpan, K. Chotivanich, M. Mayxay, S. Looareesuwan, J. Farrar, F. Nosten, and N. White. Fake artesunate in southeast Asia. *The Lancet*, 357(9272):1948–1950, 16 June 2001.

[22] T. Parikh. CAM: A Mobile Paper-based Information Services Architecture for Remote Rural Areas in the Developing World. In *VL/HCC 2005*, Dallas, Texas, 2005.

[23] C. Purefoy. Poisoned medicine kills dozens of children in Nigeria. http://www.cnn.com/2008/WORLD/africa/12/18/nigeria.poison.drugs/, 18 December 2008.

[24] J. Rekimoto and Y. Ayatsuka. CyberCode: designing augmented rality environments with visual tags. In *DARE 2000*, pages 1–10, Elsinore, Denmark, 2000.

[25] J. Schiller and A. Voisard. *Location-Based Services*. Morgan Kaufmann, April 2004.

[26] A. Sharma, L. Subramanian, and E. Brewer. Secure Rural Supply Chain Management Using Low Cost Paper Watermarking. In *NSDR '08*, Seattle, Washington, 2008.

[27] T. Staake, F. Thiesse, and E. Fleisch. Extending the EPC network: the potential of RFID in anti-counterfeiting. In *SIGAPP 2005*, pages 1607–1612, Santa Fe, New Mexico, 2005.

[28] R. Tomlinson. China cracks down on counterfeit medicines. *British Medical Journal*, 316(7184):624, March 6 1999.

[29] P. Tuyls and L. Batina. RFID-Tags for Anti-counterfeiting. In *Topics in Cryptology - CT-RSA 2006*, chapter 9, pages 115–131. Springer, Berlin/Heidelberg, Germany, 2006.