Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 353 – 359

ISBN 978-83-60810-22-4
ISSN 1896-7094

Text Messaging to Authenticate Products through Matching Hidden Codes

Ashifi Gogo and Elsa Garmire
Thayer School of Engineering
Dartmouth College, Hanover,
NH 03755-8000

***Abstract*—Fake, counterfeit, or adulterated products have become a dangerous reality to consumers in developing countries. High value-added products are of particular concern, with pharmaceuticals topping the list, followed by packaged food. The prevalence of mobile phones, even in the poorest communities, and the availability of text-messaging, suggest that they may be used to solve this problem. This paper shows how an innovative system allows any member of the populace in the developing world to authenticate a drug before use by a simple text message over mobile phone. This system has been used to authenticate pharmaceuticals in a prototype demonstration project in Ghana. The prevalence of fake drugs and the willingness of customers to use this system were verified in a study involving a consumer base of eight pharmacies in Accra, Ghana, with almost 1000 responses over a three-month period. The opportunities and challenges to implementing such a system on an international basis will be described. Finally, the proposed technology will be compared with other options, showing why mobile phones may offer the most viable option for solving this vexing problem.**

I. Introduction

THE World Health Organization (WHO) estimates that counterfeit drug prevalence rates are between 10% to 30% in the developing world, compared to 1% or less in industrialized nations. The U.S.-based Center for Medicines in the Public Interest (CMPI) projects that by 2010, US$ 75 billion worth of counterfeit drugs will be sold. Fake drug sales are expected to grow by 13% yearly, a rate significantly higher than the estimated 7.5% annual growth for genuine pharmaceutical commerce. [1] .

How can technology help with this problem? Industrialized nations have a range of technologies at their disposal, such as 2D bar code readers and Radio Frequency Identification (RFID) readers. However, there is a general dearth of socio-culturally sensitive technological means of discerning drug pedigree for the developing world, which bears a disproportionately larger burden of the counterfeit medication load. Developing nations are generally not in a position to invest financially in the research and development needed to yield effective anti-counterfeit technologies. Where such countries have chosen to tackle the fake drug problem, stepped up regulatory enforcement (raids on syndicates and legal proceedings) is the only deployable tool. [2] Nigeria offers an example of the increased enforcement approach. In 2003, Interpol discovered that 80% of the drugs available in Lagos, Africa's most populous city, were fake. [3] Because of a well-executed stepped-up enforcement effort headed by Prof. Dora Akunyili, the director general of Nigeria's National Agency for Food and Drug Administration and Control (NAFDAC), the prevalence is believed to have dropped to 16% three years later. [2] E ven when enforcement is in place, however, the availability of internet-sourced drugs of questionable pedigree presents a challenge for both developing and developed nations, needing complementary technological solutions.

An RFID drug pedigree tracking system has been tested in the U.S. to facilitate mass-surveillance of genuine drugs as they filter through the supply chain, from legitimate manufacturers to consumers. [4] Soon, first-world consumers will be able to purchase drugs with the confidence that the drug's entire pedigree has been authenticated by the appropriate trust networks and national authorities. Developing nations, on the other hand, are technologically well behind the times; new anti-counterfeit technologies are often beyond their means. History has shown that by the time such technologies are affordable, resourceful counterfeiters would have copied the technology. This trend is evidenced by counterfeiters' compromise of microprint, advanced product packaging, security inks, tabletting molds, unique blister packs and even holograms as fool-proof product security technologies. [5]

This paper describes the mobile-based technology solution that we have determined has the greatest chance of succeeding in developing countries, followed by a review of the alternative technology solutions, which demonstrates that none are as promising as the scheme outlined here.

A. Mobile-based Technology Solution

The mobile phone provides a very accessible platform in developing nations – 97% of people surveyed in Tanzania said they could access a mobile phone, while only 28% could access a land line phone. The approach described here is based on mobile phones, utilizing unique, human-readable codes that are placed on drug packaging. Consumers can look up drug pedigree information via their mobile phone using the Short Message Service (SMS, or text message). The WHO has noticed that the explosive growth in mobile phone teledensity in developing nations makes a

compelling case for employing this method in such regions. [7]

The "pay-as-you-go" mobile phone subscription model is popular in low-income areas, with as many as 95% of all African mobile subscribers using this pre-paid scheme. [8] Prepaid patrons top up their mobile phone credit by purchasing vouchers with concealed unique, single-use codes. They scratch or tear off the concealing cover, revealing the code. Customers then upload the codes to the mobile carrier via Unstructured Supplementary Service Data (USSD) or SMS. This technology will allow the pedigree of drugs to be verified by printing similar scratch- or tear-off labels on genuine drugs at source. The consumer will then authenticate drugs in a similar fashion to topping up credit on mobile phones. In this fashion, developing countries can achieve levels of security comparable to more "high-tech" schemes envisioned for developed countries.

II. Pilot Project

In the first quarter of 2008, a pilot service was conducted in Ghana using this model. [9] Ghana was eminently suitable to this technology because it had over 5 million mobile phone subscribers in 2006, as compared to only 356,400 fixed line account holders. [10] Indeed, the GSM Association expects 85% of all Africans to live in mobile-enabled areas by 2010. [11] With a history of political stability and a progressive Drug Regulation Authority (DRA) that is not overwhelmed by the challenges of fake drugs, Ghana offered a good test-bed for the concept.

Working with a local drug manufacturer, uniquely-coded single-use scratch-off panels were placed on individual drugs. At the point of sale, consumers were prompted to authenticate their drugs. Under this scheme, consumers could authenticate their drugs by sending the code under the scratch-off panel to a single SMS shortcode across all mobile networks, obtaining an instant response at the point of sale pertaining to the drug's genuineness. If the drug is deemed fake, consumers can immediately request an exchange. Such human-readable codes could be nested by packaging hierarchy, allowing a scheme of cascading authentication from the manufacturer with the option of flagging products that did not pass through the approved supply chain.

Over two months in the first quarter of 2008, any member of the general populace in the Ghanaian city of Accra could confirm drug genuineness when purchasing from select pharmacies. Survey agents were hired to attend to customers at the partner pharmacies. Eight pharmacies in high volume trade areas were selected, to maximize the chance of interviewing numerous consumers. If a consumer didn't purchase a coded drug, they were invited to witness a demonstration of the method as part of the survey. Of 834 respondents in Accra, about a fifth suspect they have purchased a fake drug, based on its apparent inefficacy or unforeseen side effects. The overwhelming majority of respondents pointed to open markets as the source of counterfeits in Ghana. Such open markets are unstructured and difficult to regulate. Often roaming vans advertise and sell drugs to serve consumers at their doorstep. Respondents universally showed interest in the method demonstrated in this pilot project, and a detailed analysis of the trial results will be published in a follow-on paper.

III. Ensuring Tamper-proof Authentication

The use of a single overt SMS shortcode and unique covert codes exhibits some strong similarities to the well-established asymmetric cryptography method widely used in electronic trade and banking today. Under asymmetric cryptography, two encryption keys are generated: an overt public key and a covert private key. A user's public key allows anyone to encrypt a message that only the said user can decrypt with their private key. In order to ensure that the public key actually belongs to the user as advertised, a Public Key Infrastructure (PKI) Trusted Third Party (TTP) is often employed to validate identities. Analogously, the mobile shortcode is the public key, encapsulating the drug's pedigree. Upon submission of a valid private key (covert voucher code), a patient can unlock a drug's pedigree. As the auditing agency, the DRA serves as the TTP under this analog.

If a private key is compromised (for instance, by voucher theft), it can be revoked before the drug is authenticated, which will notify consumers of the impending risk. This adaptation of asymmetric encryption is both secure and practical. Asymmetric encryption is well-understood and hack-resilient. Developed over 30 years ago, the RSA algorithm follows asymmetric encryption and is used widely in commerce. Documents encrypted with RSA keys of reasonable length, 1024–2048 bits, are yet to be cracked. [12]

With the mobile authentication method has many advantages. Drug validation requests could be aggregated to isolate persistent negative responses, allowing law enforcers to conduct investigations on a product with timely intelligence. If a safety issue is discovered after products have left the factory, drug manufacturers can silently conduct DRA-sanctioned product recalls by having the SMS response direct consumers to exchange purchases. Aid agencies can track their drug donations via cascading authentication. Genuine drug manufacturers can deploy sales tracking and supply chain management software atop the aggregated data, allowing them to generate sales forecasts and respond rapidly to market trends. Using DRA-approved short marketing messages, such manufacturers could advertise their products while consumers are still at the point of purchase. A system giving manufacturers and distributors such a direct channel to individual consumers is yet to be widely realized even in the industrialized world.

One of the challenges such a scheme will have is the relatively low rate of education in developing nations. The Ghanaian 2000 census pegs the effective literacy level at just 46.9% [13]. Literacy will limit the variety of SMS responses that can be generated. However, just as illiterate people can get very comfortable doing basic arithmetic with currency, the vast majority of mobile phone users are literate in numbers. With education, illiterate consumers can learn to self-police their purchases, because they stand to lose the most from unknowingly ingesting counterfeit medication.

TABLE I.
RISKS AND SUGGESTED SOLUTIONS FOR A MOBILE-BASED ANTI-COUNTERFEIT SOLUTION

Risk	Mitigation
Counterfeiters will fake the codes or SMS responses.	• Use completely random codes that expire after a single use, as the phone industry currently does. • Conceal codes under opaque scratch-off protective layer. • Advocate for consumer involvement to ensure authentication is carried out. Only consumers can ensure codes are genuine. • Ensure a single, well-branded SMS shortcode is used for all authentications. If possible, the shortcode should be treated as a "911" emergency number for pharmaceuticals, mandated by telecom regulators.
Counterfeiters will hack code database.	• Require two independent interfacing devices that co-create codes. • Generate the codes offline, pass the codes through a cryptographic hash function after printing and securely upload the hashed codes. • Deploy hardware and software firewalls to protect servers. • House servers in a secure location, with secure access policies.
Printed labels can be peeled off genuine products and applied to fake drugs.	• Use tamper-evident labels. • Counterfeiter has to purchase coded genuine products. • Labor intensive task, not economically sound for very large batches.
Criminals will spam the free SMS number.	• Implement anti-spam solutions, such as throttled billing (a cap on free authentications per hour per number) and SIM blocking.
Criminals will steal the coded labels.	• House labels in a secure warehouse with inventory control. • Deactivate stolen codes in database. • Transport codes securely using existing currency transportation services.
SMS messages will be sent but the server's response won't be received by consumers	• This risk varies based on network operator service quality. Codes can be rendered inactive after 5 minutes of receiving an authentication query. Consumers can call-in as an alternative within 5 minutes of sending the code if they don't get a response by SMS. • SMS messages can also be sent with validity periods and delivery confirmation. Thus, if message delivery isn't confirmed within a short period of time, the SMS Center server may discard the message and a new message alerting consumers could be sent.

Other risks and suggested solutions are displayed in Table 1. It is important to note that the scratch-off top-up model has worked well for multinational phone companies in Africa's US$ 38 billion mobile services market (2007) for over a decade, successfully powering Africa's tremendous subscriber growth. [14]

A. SMS Transmission

Cell phone communications are standardized, with the most common standard being the Global System for Mobile Communication (GSM) specification. GSM allows for a voice communication on one channel and the control signals on another, which doubles as the SMS communication channel. Newer cell phones allow SMS transmission over additional channels, such as the General Packet Radio Service (GPRS) data channel.

SMS is a "store-and-forward" technology – messages are stored on a central server known as the Short Message Service Center (SMSC) and delivered to a mobile device when it is powered and within range. Message delivery is retried during a Validity Period (VP), and senders can request delivery confirmation. Mobile Network Operators (MNO) have commercial agreements that can allow trans-network two-way SMS.

Figure 1 shows the SMS authentication infrastructure envisaged for this Mobile application. Acronyms are as follows: ME: Mobile Equipment capable of communicating on a mobile network (e.g. cell phone). SIM: Subscriber Identity Module, a small chip with memory that provides the phone's unique identity/number. SME: Short Message Entity that combines ME and SIM – a functional device authorized to transmit SMS messages. BTS: Base Transceiver Station. BSC: Base Station Controller. HLR: Home Location Register that registers SIM location to appropriate cell tower, allowing for routing SMS messages from sender to receiver. MSC: Mobile Switching Center that registers and updates the SME on the network specified by the SIM. SMSC: Short Message Service Center, the server that processes incoming and outgoing text messages. ESME: Short Message Entity, hardware or software external to the MNO's network that is capable of communicating via SMS. ESME: Authentication System, the proposed design for authentication.

B. SMS reliability

Though SMS is not a real-time GSM service, it is typically considered reliable enough under normal network volume to support financial notification services. A real-life study with 59 million messages sent over three weeks showed a

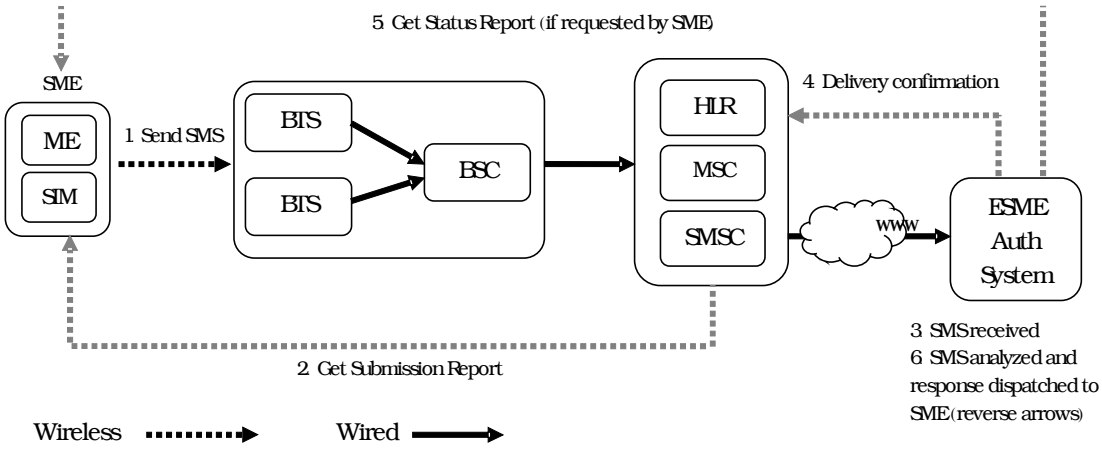

Figure 1. Overview of SMS authentication infrastructure showing a mobile originated (MO) SMS message. The process is reversed for mobile terminated (MT) messages. [16]

message delivery failure rate of 5.1% in normal network operation for a network operator with 20 million subscribers. Analogous transmission losses for Email are pegged at 1.57%. [15] The study's average throughput was 33 messages/ second, but messaging volume varies greatly across peak/non-peak hours. Researchers generally agree that SMS is as reliable as a typical commercial grade end-to-end communications system, but care must be taken in deploying a mission-critical system solely over SMS. In our design, we use extended SMS features like expressly-requested delivery reports and delayed single-use code expiration to boost service integrity.

Though a real-time service would be preferred for our mission-critical application, network operators are yet to open up real-time services like GSM's Unstructured Supplementary Service Data (USSD) for general use. On the other hand, SMS is now a widely-accessible network service, offered through the operator's Value Added Services (VAS) department. These solutions are typically implemented through special mobile numbers known as shortcodes – phone numbers of a shorter length, typically 4 to 6 digits, instead of the standard ITU-E.164 format that can be twice as long. Shortcodes also allow for regular SMS service, as well as premium SMS, in which users pay above the normal tariff for text messaging, and reverse-billed SMS, in which users pay nothing for sending SMS messages to a particular number and the shortcode lessee pays for the SMS messages on behalf of users.

C. Code Generation

The generation of authentication code is modeled after the highly successful top-up card industry for pay-as-you-go mobile phone subscriptions. Randomly-generated codes with a check-sum are securely provided to a trusted label printing service, with signed, encrypted messages using Pretty Good Privacy (PGP). The length of the authentication codes needed is adjusted to suit the volume of products to be authenticated, such that there is a negligible probability that a counterfeiter will be able to match a code by printing random codes onto fake products. With such a slim chance of success, it is economically impractical for counterfeiters to apply fake labels as long as a vast majority of consumers authenticate their drugs. Higher rates of consumer participation could be induced by allowing genuine manufacturers to provide incentives directly to consumers or pharmacists.

D. Code Processing

Figure 2 shows the system layout for an incoming SMS message. Each of the Compute Nodes (CN-1… CN-n) runs a distributed SMS authentication software based on the job scheduler in the Authentication Cluster (AC). Each compute node is responsible for:

1. Sanitizing the SMS authentication messages, removing any malicious code and rejecting malformed messages (without querying the SQL Server, preventing unnecessary system load)
2. Extracting the numeric authentication code from the text message
3. Validating the numeric code against the SQL Server database
4. Compositing the authentication response (appending the appropriate mobile marketing message) and requesting for a delivery confirmation status report in the text message metadata
5. Dispatching the final response to AC and updating the authentication record on the SQL Server when a delivery confirmation is received.

The AC then sends the SMS message to the SMSC for delivery to the SME through the MNO's network.

Additional CNs can be added for threat analysis and supply chain analytics computation.

Periodic authentication metrics are sent to the Front-end Report Cache (FRC). Generalized high-level metrics for le-

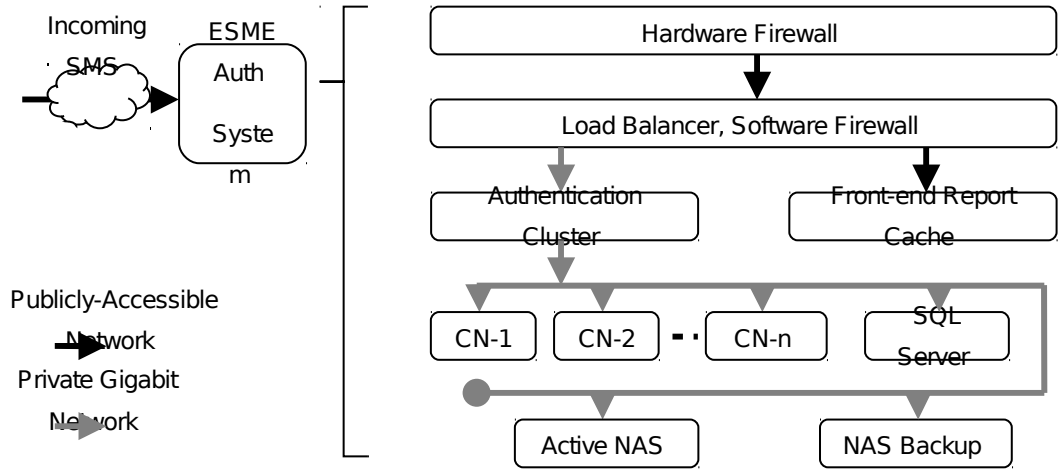

Figure 2. System layout for an incoming SMS message. Reverse the paths for outgoing messages.

gitimate brand owners and regulatory authorities can be accessed from the FRC and syndicated via RSS.

Future work will be done on a commercial cloud computing platform. Such providers allow for rapid addition of general purpose compute node via virtualization, and abstract away all hardware failures the typical system administrator has to worry about

IV. Alternative Technology Solutions

Traditionally companies have relied on unique (and sophisticated) tamper-proof packaging, but big-business counterfeiters have shown an ability to copy almost any package. Indeed, some counterfeiters can produce better packaging than legitimate brand owners since they spend less on the drug's active pharmaceutical ingredients. The alternative approach is to have a transparent and traceable path from consumer back to the drug-maker. In developed countries, RFID is thought to be the technology that will supply this. A viable alternative is 2D bar codes that contain a great deal of information, but require sophisticated readers. The US FDA is instituting an e-pedigree program that expects big pharma to use one of these technologies to protect consumers. However, in both cases the sophisticated technology is beyond the price range of customers and/or small businesses in developing countries, particularly in small towns. Possible alternative technologies can be grouped into three main categories: direct authentication; mass serialization track-and-trace; and forensic, chemical and physical tests. [17]

A. Direct Authentication

Direct authentication is a process by which a consumer can directly determine that a product is authentic. This may be merely by direct observation, or it may require a simple test. Of course, effectiveness requires a consumer culture of package inspection. *Advanced Product Design and Packaging* is used by many companies in an attempt to provide uniqueness. Unfortunately, counterfeiters are becoming more and more capable of copying even the most complex designs and packages. *Micron-sized Printing and Direct-write Technologies* are widely used on currency and checks, but these often require a form of magnification for good inspection, and counterfeiters can produce convincing replicas, unless a magnifying glass is at hand, *Holograms* were thought to have been effective, but today low-cost equipment for reproducing them is readily available, especially on the Internet. A variety of *Security Inks* [17] have been used, including Color Shifting, Thermochromatic, Photochromic, Reflective, Chemically-reactive, and Magnetic. Each of these has found some use, particularly in financial markets to protect individual documents, but these techniques are replicable by counterfeiters if the economic payoff is high enough. Nowadays, off-the-shelf software packages allow moderately skilled counterfeiters to replicate packaging from scratch. Furthermore, authentication devices may be expensive and/or require educated consumers, which is not appropriate to developing countries. After study, we deemed none of these technologies long-lasting and sufficiently guaranteed for pharmaceutical products.

B. Mass Serialization, Track and Trace

This is the class of technologies under which the proposed mobile phone authentication is placed. This section looks at alternative, and possibly competitive, technologies. The alternatives include *Static Markings and Product Codes* printed on the package. The US has a Universal Product Code (UPC); there are also the European Article Number (EAN) and the Japanese Article Number (JAN). However, counterfeit product manufacturers are now printing the static registration numbers on their packages in a very convincing manner – these codes provide minimal protection against counterfeiting.

Encrypted *Barcodes* represent a more viable alternative. More flexibility and information are available with 2D barcodes; even 3D barcodes are in the works, adding color. Encrypted 2D barcodes with open standards linked to a centralized database could be a potent solution against counterfeiting in the developed world. The European Federation of Pharmaceutical Industries and Associations (EFPIA) is scheduled to use GS1 codes represented as DataMatrix bar

codes for pharmaceutical products, starting with mandatory implementation in France by 2011. [18] However, barcodes are of little use without electronic point of sale systems, as is the case in smaller towns and villages in the developing world. Simple 1D barcodes can also easily be counterfeited by photocopy.

Radio Frequency Identification (RFID) Tags represent a third possible track-and-trace technology. They present contact-free radio communications, but require a reader. They are presently used for automating animal tracking, vehicular toll payment, wholesale and retail supply chain management and credit card payments. However today conventional tags have read error rates around 20%. [19] Chief concerns about RFID revolve around privacy, tag costs, complicated logistics and poor read rates.

The U.S. Food and Drug Administration (FDA) launched e-pedigree as a renewed effort to require drugs sold in the U.S. to contain complete pedigree information. RFID was designed to operate with EPC codes, which support item-unique coding. Thus, with a global mass-serialized RFID scheme, such as the Worldwide Track and Trace Bank (WTTB), products can be automatically tracked from raw materials to post-consumer waste. Such a system could also be used to fight product diversion and illegal parallel trade. [29] However, RFID tags can cost four times more than barcodes and the American pharmaceutical industry is not ready for a large-scale serialization deployment. While the U.S. State of California has aggressively pursued ePedigree implementation, the deadline has been pushed back from 2009 to 2011, and recently even further to 2015. [20] With that basis, it may take much longer before national RFID-based schemes are implemented across the developed world, and even longer for developing nations to benefit directly from such technology. One potential in developed countries for drug authentication is for RFID readers to be integrated with cell phones, so they could be used by consumers. The industry's response is, however, not encouraging – though the first radio frequency phone kit was released in 2004, [21] none others have apparently entered the market [22].

C. Forensic, Chemical and Physical Tests

Forensic tests are designed to provide conclusive evidence via sophisticated methods that can constitute evidence admissible in court. Chemical tests are the surest way of testing for sub-standard and counterfeit formulations and have to be regularly carried out by manufacturers and DRAs. Physical tests provide a cheaper, yet effective alternative by utilizing the oft non-conforming manufacturing environment for fake drugs as a means of discerning authenticity. However, none of these tests can easily be performed by a consumer. *Taggants* (such as in explosives) are micron-sized inert or rare elements, or fluorescent fibers within the product or package. The assurance of security lies in the difficulty of reverse-engineering taggant particles. Verification requires readers such as UV lamps or other equipment to decode proprietary spectral signatures.

Chemical-induced Color-based Detection determines with a high degree of certainty if a sample is truly as specified by a manufacturer. The tradeoff is typically high complexity, lack of equipment or trained professionals in deprived areas, cost and availability of supplies, and the need to tamper with medication. *Colorimetry* involves observing distinct color changes with specific reagents based on the presence of a specific active pharmaceutical ingredient. This test can provide a basic "yes/no" response that can screen samples for further testing, saving resources. [23] Unfortunately, counterfeiters are catching on to such tests by adding fractions of the recommended amounts of active ingredients to fake drugs.

Hardness and dissolution tests can be surprisingly effective and cheap. Though two pills may look alike, their dissolution profiles in some solvents show a marked difference. By recording the percentage of dissolved medication over time, researchers have been able to show high selectivity in determining drug genuineness of common anti-malarials. [24] The dissolution test takes time and the entire pill is often ruined; it is not commercially viable on single dosage drugs, but is valuable to DRA's. It also doesn't apply to liquid formulations – the common drug delivery medium for infants.

V. Conclusion

The prevalence of fake drugs is unacceptably high and technology is being implemented to ensure consumers that their purchases are genuine. The solution for the developing world must be consistent with the technology available to them. Using the omnipresent mobile phone to text message unique codes found on each package and obtain confirmation from an encrypted database is the most suitable solution. Preliminary tests have shown consumers willing and able to use this service.

This effort was supported in part by NCIIA (The National Collegiate Inventors and Innovation Alliance) and in part by Dartmouth College.

References

[1] Kirsty Barnes, *"Systech offers solution in counterfeit drug war,"* In-PharmaTechnologist.com, October 21, 2005. http://www.in-pharmatechnologist.com/Packaging/Systech-offers-solution-in-counterfeit-drug-war. Accessed on December 1, 2008.

[2] Transcript of interview, *"Cracking Down on Killer Drugs: Dora Akunyili and the Nigerian Success Story,"* American Enterprise Institute, April 14, 2008. http://www.aei.org/events/filter.all,eventID.1700/transcript.asp. Accessed on December 1, 2008.

[3] Nick Taylor,— *"Nigerian Counterfeit drug seizure",* In-PharmaTechnologist.com, May 29, 2008. http://www.in-pharmatechnologist.com /Processing-QC/Nigerian-counterfeit-drug-seizure. Accessed on December 3, 2008.

[4] Presentation at the *"FDA Anti-Counterfeit Drug Initiative Workshop Public Meeting"* by Thomas McPhillips, Vice President, U.S. Trade Group, Pfizer Inc. February, 2006. Accessible online: http://www.fda.-gov/oc/meetings/rfid/McPhillips.ppt

[5] Newton P. N., McGready R, Fernandez F, Green M. D., Sunjio M, et al. (2006) *"Manslaughter by fake artesunate in Asia—Will Africa be next?"* PLos Med 3(6): e197. DOI: 10.1371/journal.pmed.0030197

[6] Counterfeit Drugs – Guidelines for the development of measures to combat counterfeit drugs. Department of Essential Drugs and Other Medicines, World Health Organization, Geneva, Switzerland. http://whqlibdoc.who.int/hq/1999/WHO_EDM_QSM_99.1.pdf. Accessed January 11, 2009.

[7] Thomas Crampton, *"Wireless Technology Speeds Health Services in Rwanda,"* New York Times, March 5, 2007.

[8] Erik Hersman, "Big Surprises, Small Package," http://www.slideshare.net/whiteafrican/mobile-phones-in-africa-picnic-08-presentation?type=powerpoint. Accessed January 11, 2009.

[9] Ashifi Gogo, *"Engineering Solutions to the Problem of Counterfeit Medication in Developing Nations",* Ms Thesis, Dartmouth College, December 2008.
[10] The United States Central Intelligence Agency World Factbook: Ghana. https://www.cia.gov/library/publications/the-world-factbook/geos/gh.html. Accessed December 10, 2008.
[11] GSM Association Development Fund, *"Phones for Health,"* http://www.businessactionforafrica.org/documents/GSMAhealth.pdf. Accessed December 10, 2008.
[12] Wikipedia contributors, "RSA," Wikipedia, The Free Encyclopedia http://en.wikipedia.org/wiki/RSA. Accessed December 5, 2008.
[13] Ghana Investment Promotion Center Frequenty Asked Questions, http://www.gipc.org.gh/Pages.aspx?id=81Literacy. Accessed December 2, 2008.
[14] Portio Research Mobile Factbook 2008.
[15] Xiaoqiao Meng; Zerfos, P.; Samanta, V.; Wong, S.H.Y.; Songwu Lu, *"Analysis of the Reliability of a Nationwide Short Message Service,"* INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , vol., no., pp.1811-1819, 6-12 May 2007
[16] URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4215793&isnumber=4215582
[17] Adapted from Figs. 3.2 and 3.7 in Gwenael Le Bodic, Mobile Messaging Technologies and Services: SMS, EMS and MMS, Second Edition, John Wiley & Sons, 2005
[18] Anti-counterfeiting Packaging Technologies in the U.S. Pharmaceutical and Food Industries. BCC Research, Published August 2007. http://www.mindbranch.com/prod-toc/Anti-counterfeiting-Packaging-R2-1283. Accessed January 11, 2009.
[19] Thomas Völcker, *"Anti-Counterfeiting Technologies,"* Pharma Focus Asia, http://www.pharmafocusasia.com/manufacturing/anti_counterfeiting_technologies.htm. Accessed December 8, 2008.
[20] Wikipedia contributors, *"RFID,"* Wikipedia, The Free Encyclopedia http://en.wikipedia.org/wiki/RFID. Accessed December 5, 2008.
[21] Nick Taylor, *"Another delay knocks back ePedigree until 2015,"* PharmaTechnologist, October 13, 2008.
[22] *"Nokia Unveils the world's first NFC product - Nokia NFC shell for Nokia 3220 phone,"* November 2, 2004. http://press.nokia.com/PR / 200411/966879_5.html. Accessed January 11, 2009.
[23] *"Phone Finder"* search query. http://www.gsmarena.com. Accessed November 28, 2008.
[24] *Counterfeit Drugs – Guidelines for the development of measures to combat counterfeit drugs.* Department of Essential Drugs and Other Medicines, World Health Organization, Geneva, Switzerland. Http://whqlibdoc.who.int/hq/1999/WHO_EDM_QSM_99.1.pdf. Accessed January 11, 2009.
[25] Characterization of counterfeit artesunate antimalarial tablets from southeast Asia,
[26] Am J Trop Med Hyg Hall et al. 75 (5): 804 and Green M. D., Mount D. L., Wirtz R. A., White N. J. *A Colorimetric Field Method to Assess the Authenticity of Drugs Sold as the Antimalarial Artesunate.* Journal of Pharmaceutical and Biomedical Analysis 24:65-70, 2000, http://www.cdc.gov/malaria/travel/test.htm. Both accessed January 11, 2009.