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

Michael Paik, Jay Chen, Lakshminarayanan Subramanian
New York University
CTED
Counterfeiting

• Counterfeiting is a widespread problem in a variety of products.
Drug Counterfeiting

The percentage of drugs on shelves that is counterfeit is as high as 60% in Southeast Asia\(^1\) and 80% in the Ukraine\(^2\)

1. USP  2. NAFDAC
Motivating Problem

Counterfeit drugs, particularly in the developing world, have a cost in lost lives and livelihoods above and beyond economic cost.
Existing Approaches

Recognizable Packaging

Special Packaging

Holograms
Existing Approaches
Holograms worked well until...
Reformulated Problem

Static checks are broken - how do we track and trace medication as it goes through the supply chain between the manufacturer and the end user?
Straw Man: RFID

Proposed for the US ePedigree initiative

- Cost: $0.15 per tag and up

- Requires new, unfamiliar hardware at every point a tag would be verified, e.g. every point of sale

- Doesn’t solve the problem of tracking scans without existing infrastructure

1. rfidjournal.com
Intuition

- Use existing infrastructure, hardware, and know-how:
- GSM networks, mobile phones, and SMS/GPRS
Mobile Handsets

- Easily portable
- Self-contained power
- Physically robust
- Familiar usage metaphor
- Inexpensive
Epothecary

- Uses camera phones to scan unique glyphs affixed to units at each level of packaging and tags representing transacting parties.
- Uses SMS or GPRS as available to convey scan information back to a central authority.
Protocol: Prerequisites

• Each participant in the supply chain receives
  – An ID card with a unique glyph
  – A password
  – A preconfigured phone with random symmetric encryption key, itself encrypted with the provided password
Protocol: Transactions

• At each transaction, the purchaser enters his password and scans
  - His own ID glyph
  - The seller’s ID glyph
  - The glyph of the unit being sold
Protocol: Communication

- Scanned glyphs are appropriately concatenated and encrypted with the symmetric key using a standard stream cipher.

- The application chunks this message and optionally GPS location data into one or more SMS messages and sends them to a trusted third party, e.g. national regulatory body.
Protocol: Verification

- The third party
  - Checks that the top-level inventory glyph is known to belong to the seller
  - Returns
    - Metadata about the item being sold
    - Glyphs affixed to constituent units
    - Optionally, descriptive metadata of the seller
Protocol: Verification

- The purchaser
  - Checks provided metadata against item being purchased
  - Checks glyphs affixed to constituent units and scans these tags

- If the glyphs match the expected values, the application sends an ACK to the third party indicating a successful transaction
Protocol: Auditing

• The third party
  – Registers the change in ownership of the item sold if it receives the ACK, or
  – Flags the item for investigation if a NAK is returned or an ACK is not returned
Protocol: Consumer

• Party selling to end user scans
  – His own ID glyph
  – Glyph of the item being sold

• This information is sent to the third party, which marks them as sold
Protocol: Consumer

• The third party returns a summary with a uniformly random reference number
  – e.g. 412565

• The consumer can SMS this reference number to some public-facing number for verification
  – e.g. 9999
Protocol: Consumer

- Verification includes all relevant metadata:
  - Ampicillin
  - 500mg
  - 50 tablets
  - Sold by John Doe
  - 8 March 2011 13:23PM
The Loose Pill Problem

Many consumers cannot afford to buy an entire bottle or box of meds at once but must rather buy each day’s dose that day.

How do we protect these people?
The Loose Pill Solution

Epothecary tracks metadata about medication sold, including packed quantity. A small change to the protocol prevents sellers from refilling genuine packages of meds with counterfeits.
Protocol: Consumer (Revised)

- Party selling to end user scans
  - His own ID glyph
  - Glyph of the item being sold
- Seller enters quantity sold
- This information is sent to the third party, which marks them as sold
The Loose Pill Solution

Epothecary does per-package accounting on the server side, and once the expected quantity is exhausted, will cause transactions to fail.
Key Insights

Epothecary knows who owns any unit at any given time

Inserting counterfeits into the supply chain requires collusion of valid counterparties

Epothecary tags are, on net calculation, far more expensive to reproduce than to
What Does It Get Us?

• Fine-grain track and trace of sold pharmaceuticals
  - Easy recall of expired, bad drugs

• Cheap, readily available equipment
  - Allows for simple automatic use of phones as bookkeeping devices (if desired)
What Does It Get Us?

• Strong assurances to the consumer of the authenticity of drugs purchased through a participant in the system
• Greatly speeds tracking of problems in the supply chain
• Ability not only to detect counterfeits at the end of the chain but to detect where in the chain they were inserted
And the Counterfeiters?

- Counterfeiters rely on economies of scale to make counterfeiting worthwhile.
- Uniformly random tags cannot be predicted in advance, particularly not the constituent tags, and cannot be ordered in bulk ahead of time - economies of scale are lost.
And the Counterfeiters?

- Counterfeits cannot be created *ex nihilo* as tags not in the system will be detected immediately.
- A set of tags may be copied and one set of fake drugs sold, but any second sale will be detected immediately.
- Must buy/steal one to sell one - drastically increases effort and reduces profitability.
Numbers

Conservatively estimating 1 minute to unpack a unit, copy its tag, affix it to a counterfeit and replace the genuine item with the counterfeit...

~348 person-hours for 144 crates, 20736 boxes
The Inevitable Question

How does this compare to System X*?

* Disclaimer: Any analysis based only on publicly available information about existing pilot efforts as of the end of 2010.
The Inevitable Question

<table>
<thead>
<tr>
<th></th>
<th>Epothecary</th>
<th>System X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loose Pill Solution</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Track &amp; Trace</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>“Secure” Design</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Spoofing Resistant</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>DoS Resistant</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Sustainable Revenue Model</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Auditing</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Thank You
Spoofing

• Requires at minimum
  – Buyer ID glyph
  – Telephone number of buyer’s phone
  – Password
  – Symmetric key

• Basically guarantees duress or collusion, either of which is quickly detected