Combating counterfeit products with RFID

Dr. Florian Michahelles
fmichahelles@ethz.ch
Department of Management, Technology and Economics,
ETH Zurich, Switzerland

Auto-ID Labs and M-Lab
Fakes often have to cross national borders…
...and there are many creative ways...
…which are hard to detect…
…and require experience.
Physical inspections triggered by experience-based risk analysis

HEAD

1) Company
2) Nationality
3) Flight Number
4) Date of departure (is not always the arrival date!)
5) point of lading
6) point of unlading
Physical inspections triggered by experience-based risk analysis
Physical inspections triggered by experience-based risk analysis
Physical inspections triggered by experience-based risk analysis
Physical inspections triggered by experience-based risk analysis
Physical inspections triggered by experience-based risk analysis
Distribution Channels for Counterfeit Products

Trademark Owner (Manufacturer of original products) → Outsourced manufacturer

Licit distribution channel

Parallel trading, Product diversion, Factory overrun

Theft

Shrinkage, Product diversion etc.

Distribution channels for parallel traded goods

Illicit distribution channel

Customs

End-user / Consumer

Flow of goods
• By definition, the problem is hidden and difficult to measure
• ICC estimated the overall cost of counterfeiting in the world about 5-7% of world trade (International Chamber of Commerce, 1997)
  – Often quoted but very unreliable number
• OECD has recent, more accurate estimate that counterfeiting and piracy is likely to account for less than USD 176 billion, or 2% of international trade
  – Result is extrapolated from detection statistics
Drivers and enablers of illicit trade

- Advances in manufacturing technology
- Increased international trade
- Growing professionalism
- Internet as distribution channel (Lacking regulations, no liability of service providers)
- Emerging markets (China)
- Low political will to help: Anti-counterfeiting has low overall priority
- Parallel trade is legal
- Low risks and high returns (*Law of greed*)

*Illicit trade is mostly beyond the control of individual companies*
Illicit trade in…
IT Industry

- Software industry suffers from product piracy
- Example cases of product counterfeiting
  - Re-labeling of 233 MHz Intel Pentium II processors to 266 MHz (1998)
  - Counterfeit electronic devices such as cell phones or MP3-players can contain fake or modified chips
  - Millions of counterfeit mobile phone batteries per year (e.g. Nokia)
  - Replacing branded parts (e.g. memory chips) of computer packages by non-branded ones
• Profit margins very slim, aftermarket
• Expensive parts that are easy to copy and frequently used are most often targeted by counterfeiters
  – filters, spark plugs, headlamps, bumpers, side mirrors, brake pads
• Counterfeits manufactured in e.g. in Asia, East-Europe
• Internet, free garages, non-certified retailers are most important distribution channel of counterfeit parts
Illicit trade in...
Pharmaceutical Industry

• Production of counterfeit drugs is relatively easy:
  – Technology is easily available, global distribution, valuable brands
• Distribution through Internet or by injection to licit distribution channel
• Re-packaging can open door for counterfeits
• Parallel trade and diversion
• Patient safety is companies priority
Illicit trade in…
Aerospace Industry

- Counterfeit airplane spare parts endanger passenger safety
- Almost all parts in airplane hold certificate of authenticity and a lifecycle report
- Problem mechanism
  - Refurbished parts are often reused in different aircrafts
  - Counterfeits are sold as refurbished parts
  - Complex spare parts can contain counterfeit parts
Illicit trade in…
Luxury Goods Industry

- Luxury brands communicate exclusiveness, higher quality
- Problem is counterfeit products from low to high quality
- Most counterfeit luxury products are of low-quality, sold outside authorized distribution channels
- Consumer survey shows that
  - almost as many consumers buy a counterfeit product than an original one
  - those who have bought counterfeits are actually more likely buy also original products
Illicit trade in…
Consumer Goods and Retail Industry

- Counterfeit consumer goods include textiles, sportswear, food, furniture etc.
- In some cases counterfeit products can even be found in retail stores
- Counterfeit products are mixed with parallel traded goods
Impact of illicit trade

Impact on companies

- **Counterfeiting is theft from the brand owner**
- **Direct impact contains**
  - Counterfeits substitute (partly) original products
  - Liability claims such as warranty
  - Increased workload for monitoring, preventing, and intervening
- **Indirect impact:**
  - Decreased brand value (e.g., exclusiveness) and goodwill
  - Risk factor from liability
  - Decrease return on investment (ROI) of marketing and RnD

Impact of illicit trade on consumers and societies

- **Impact on consumers**
  - Counterfeit product can be perceived as *good bargain* by consumers
  - Safety and health of consumers can be endangered
- **Impact on societies**
  - IPR infringements discourage innovation decreasing economic growth
  - Counterfeiters do not pay taxes and are not model employers
What does that mean for anti-counterfeiting?

- Counterfeiting and illicit trade form serious and variable problems among different industries

- Quantity of counterfeit products is increasing and quality is improving

- Technical anti-counterfeiting system should increase the risk profile of counterfeit players

- Core of the solution is product authentication, it depends on the case how and by whom this should be done
• The Problem of Counterfeits
• Promises of RFID technology
• Towards an Anti-Counterfeiting Solution
• Current Projects
• Outlokk & Implications
Low cost minicomputers ...
... with mobile communication capabilities ...
Recent advances in miniaturization, …
… finally help to link real world things at low cost to homepage(s),…
The Problem of Counterfeits
Promises of RFID technology
Towards an Anti-Counterfeiting Solution
Current Projects
Outlook & Implications
Towards an Anti-Counterfeiting Solution

- Our approach: Authentication of products
  - Distinguish genuine from fake goods
  - Easy-of-use, broaden the user base
  - Long-lasting
  - Reliability

Source: Mikko Lehtonen, Auto-ID Labs St. Gallen/ETH Zurich
Mechanisms of illicit trade

Licent Supply Chain

- Manufacturing of genuine goods
- Transportation
- Sales Point
  - Retail stores
  - Authorized dealers
  - Maintenance points
  - Service points
  - Internet

Illicit Supply Chain

- Product Acquisition
  - Factory overrun
  - Theft
  - Diversion
  - Manufacturing of fakes

Original products enter gray market

- Fakes (and originals) (re-)enter the licit SC
  - Street and bazaars
  - Flea market
  - Shops and boutiques
  - Internet
  - Private events

Original Good
High-Quality Fake
Low-Quality Fake

Source: Mikko Lehtonen/Tobias Ippisch, Auto-ID Labs St. Gallen/ETH Zurich
Use Cases of Product Authentication

Licit Supply Chain  
Illicit Supply Chain

- Manufacturing of genuine goods
- Product Acquisition
  - Factory overrun
    - Theft
    - Diversion
  - Manufacturing of fakes
- Distribution
- Sales Points/End Points
- Usage (End-User/Consumer)

- Original Good
- High-Quality Fake
- Low-Quality Fake

SToP
Use Cases of Product Authentication

- Product authentication is a tool that can be used to find counterfeit products

- This tool can be used to achieve following goals

1. Prevent counterfeits from entering the licit distribution channel
2. Help customs to detect infringing products
3. Keep sales-points and end-points clean from counterfeits
4. Enable authentication of products that are in use
5. Enable after sales services to authenticate products
Principle anti-counterfeiting solutions under study

Unique serial numbering

- The EPC Number dissected (96 bit version)
  
  21 203D2A9 16E8B8 719BAE03C

  - Header 8 bits
  - EPC Manager 28 bits (> 268 Million)
  - Object Class 24 bits (> 16 Million)
  - Serial Number 36 bits (< 68 Billion)

Source: Auto-ID Lab

Track and trace based plausibility checks

- Combination of measures
- Integrated into product
- Use physical properties

Product verification with RFID

Object-specific features

[Source: Alex Illic]
Unique serial numbers on item or case level

- Unique serial numbers stored on RFID transponders
  - Lowest cost
    - per feature
    - per check
  - Reasonable level of security
  - Reasonable complexity
  - Foundation for further solutions
  - Ready-to-implement solutions are available
Unique serial numbers stored on RFID transponders

Infrastructure overview

- Lowest cost
  - per feature
  - per check
- Reasonable level of security
- Reasonable complexity
- Ready-to-implement solutions are available
- Foundation for further solutions
User management

- Opening the system for a larger number of users increases usability.
- However, this allows for attacks: Problems may arise if illicit actors retrieve valid numbers.

- Customs and supply chain partners
  - enabled to conduct bulk checks
  - access control

- Public access
  - restricted number of requests per time → avoid denial of service-attack
  - authentication of the requesting party:
    - User registration.
    - No registration, but answer provided by email
    - Using authentication of the requesting system, e.g., caller ID from cell phone
  - Reward the check, and place it as service

→ Approaches not restricted to RFID
Using trusted address services

- The lean "hard wired" solution is not feasible in m to n environment

- An external, trusted address service is necessary if
  - The web page is not a desired entry point
  - Test equipment is not under control of the brand owner, or
  - Many brand owners use the same application and numerous service addresses

- A standardized directory service, e.g. ONS proposed by EPCnetwork, would be required

- Link address is crucial for security
  - Only for registered manufacturers
  - We suggest an additional manufacturer registration process
Plausibility checks based on track and trace

• Record of past and possible future owners or locations
• Illicit trade can be detected using business logic
• Promising for highly regulated industries
• Provides numerous additional benefits

• Requires the cooperation of numerous supply chain organizations:
  ➔ Technical challenges
    – Access rights
    – Business logic
    – Data exchange formats
    – Standardization
  ➔ Organizational challenges
    – Different interests
Track & Trace

• **Pros:**
  – Cloned tags are easier to detect
  – “Ok” to implement in a simple supply chain

• **Cons:**
  – Requires network access to authenticate tag/product
  – Gets complex in non-predetermined supply chains (access rights, ...)
  – Requires standardized network infrastructure
  – Business partners might not be willing to share these data
  – Tag-cloning not completely eliminated

• **Our recommendation in the context of anti-counterfeiting**
  – Important approach for the pharmaceutical industry
  – Only powerful if all partners use it
  – Don’t wait for ready solutions, use the unique serial approach instead
Crypto tags

- **Pros:**
  - Cloning attacks become unfeasible

- **Cons:**
  - Tags are still expensive and not standardized
  - Extra time required for challenge/response protocol
  - Read range is limited
  - How to deal with recycled tags?

- Will become more important in the future
- Only for very expensive and security relevant parts, e.g. in the aviation industry

![Diagram for RFID cost drivers]

- **Tag Channel Server**
  - ID
  - $A = f(K, RAND)$
  - $B = f(K, RAND)$
  - $A = B$?
Object Specific Security

- The previous approaches concentrate on preventing cloning attacks
- RFID is a tagging technology
  - It is still the transponder you authenticate
  - Care must be taken to ensure a genuine tag cannot be removed and reapplied to an illicit product

- Goal: integrate RFID-tag into the product
  - Incorporate RFID tags during manufacturing
  - "passport approach": store object specific features
    - weight
    - shape
    - surface

Source: Protexxion, Bayer Technologies
Object Specific Security

- Approach: tag-product integrity by storing a “fingerprint” on the tag
Requirements: secure against attacks

Source: Mikko Lehtonen, Auto-ID Labs St. Gallen/ETH Zurich]
Empowering the end-user: The Auto-ID Product Check

Phase 1
- PDA
- CF-Card RFID Reader

Phase 2
- Cell-phone
- NFC Reader

Phase 3
- Cell-phone
- NFC/EPC Reader
- EPC Network

Auto-ID Product Check
- Verify Product
- Secure Authentication: Valid product

Company: Duracell
Product: Ultra M3

More information about this demo
Agenda

• The Problem of Counterfeits
• Promises of RFID technology
• Towards an Anti-Counterfeiting Solution
• Current Projects
• Outlook & Implications
The Auto-ID Labs architect the Internet of Things. Their research is global, relevant (partner of EPCglobal), long-term, and cross-discipline.
The Auto-ID Labs architect the Internet of Things. Their research is global, relevant (partner of EPCglobal), long-term, and cross-discipline.
Research:
Mission 1 – RFID as a tool against Counterfeiting

“The Special Interest Group Anti-Counterfeiting will identify the true potential that RFID / EPC technology offers to combat counterfeiting”

Research topics of the Anti-Counterfeiting Initiative:
- Business Impact
- Network Issues
- Shortcomings of the EPC Network, e.g. Security
- Cross Industry Requirements
• **SToP overview:**
  
  - EU 6\textsuperscript{th} Framework Programme
  - Specific Targeted Research Project (STREP)
  - Duration: 1 Nov 2006 – 30 Apr 2009 (30 months)
  - Budget
    
    - Total: 4,888,448 EUR
    - European Community: 2,780,000 EUR

  - SAP, Univ. St. Gallen, Spacecode, Oria Computers,
  - Novartis, Richemont, Airbus, Bundesdruckerei
Expected outcome of StoP

- extend of Counterfeits
- impact of Counterfeits
- industry sector specific solutions
BRIDGE RFID Platform

WP5 Business application Anti-Counterfeiting
WP6 Business application Drug Pedigree
WP7 Business application SCM Textile Industry
WP8 Business application Manufacturing
WP9 Business application Reusable Assets Mgt.
WP10 Business application Products in Service
WP11 Business application Item Level Tagging

BRIDGE RFID Platform WP1-4
BRIDGE in a nutshell

- BRIDGE is an Integrated Project (IP)
- The duration is 3 years, starting in June 2006
- 30 partners with a balance representation of GS1 MOs, Labs, Users and Solution Providers
- The total “real cost” is €14,3M. The grant from the European Commission is €7,5M. The difference is covered by the participating companies
<table>
<thead>
<tr>
<th>GS1</th>
<th>Labs</th>
<th>Users</th>
<th>Sol. Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>GO</td>
<td>Cambridge</td>
<td>Carrefour</td>
<td>BT</td>
</tr>
<tr>
<td>France</td>
<td>St Gallen</td>
<td>Benedicta</td>
<td>SAP</td>
</tr>
<tr>
<td>UK</td>
<td>Fudan</td>
<td>Kaufhof</td>
<td>AIDA</td>
</tr>
<tr>
<td>Germany</td>
<td>UPC Barcelona</td>
<td>Gardeur</td>
<td>Caen</td>
</tr>
<tr>
<td>Spain</td>
<td>TUG Graz</td>
<td>Nestlé</td>
<td>Confidex</td>
</tr>
<tr>
<td>Poland</td>
<td></td>
<td>Sony</td>
<td>Cetecom</td>
</tr>
<tr>
<td>China</td>
<td></td>
<td>El Corte Inglès</td>
<td>Rafsec</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Verisign</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Melior</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unisys</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Domino</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>JJ Assoc.</td>
</tr>
</tbody>
</table>
Counterfeiting and illicit trade

Technological countermeasures

Consumer education

Private investigations

Legal measures, law enforcement

D5.1 Problem Analysis

D5.2 Requirements Analysis

D5.3 Business Case

D5.4 Development of Infrastr.

D5.5 Evaluation

D5.6.1 Application guidelines

D5.6.2 Implementation roadmap

WP4 - Security requirements, WP2 - Requirements for look-up service

BRIDGE RFID Platform
Research:
Mission 2 – RFID in new industries

• establishing RFID standards in new industries:

  • Automotive
  - Customer Focus
    - Customization
    - Real-time information about product
  - Outsourcing
    - Accurate data
    - Real-time information
  - Demand Chain
    - Handling efficiency
    - Accurate data
    - Real-time information
  - Total Quality Management
    - Handling efficiency
    - Accurate data
  - Mass Customization
    - Unique identification
    - No manual handling

• Ski Industry
  - Bulk Reading
    - Yes
    - No
  - Retail Compatible
    - Yes
    - No
  - Robust Integration
    - Yes
    - No
  - Read Tag through Ski Base
    - Yes
    - No
  - Hard to Destroy
    - Yes
    - No
Research:
Mission 3 – Enhancing the EPC network

• transforming EPC into a trusted network
  – suitable network for secure track and trace
  – cost-efficient measurement against counterfeiting

• preparing EPC for the future
  – integration of sensors on tag
  – sharing of sensor data across the network
  – data access

• developing/enhancing ONS
  – P2P approaches
  – OpenSource EPC network
• The Problem of Counterfeits
• Promises of RFID technology
• Towards an Anti-Counterfeiting Solution
• Current Projects
• Outlook & Implications
Non-functional requirements of secure product authentication

- Availability: all genuine products must be tagged, the tags must work
- Trust in parties who authenticate products
- Data sharing policies (for track and trace based approach)
“Weak products authentication” with RFID

1. Putting an RFID tag on genuine products detects fakes that are not tagged
2. Verifying ID numbers detects fakes that don’t have valid IDs
3. Verifying the transponder ID number (EPC Class-1 Gen 2 tags) makes the genuine tags harder to copy
4. Verifying if the product has already been checked helps detecting some cloned tags

Not a 100% secure system, but increases the effort to clone a product. Good solution for short-term or for inexpensive products.
Long term goal: Product authentication in the EPC network

1. DS query (EPC – list[URIs])
2. Mutual authentication against CA; EPC-IS query (EPC – event)
3. Mutual authentication against CA; Item authentication protocol (EPC – Ch. – Resp. – Result) (EPC+feature – Result)
Implications and Long-Term vision…

Automated product authentication

Lower Costs per check

Frequency of checks

Number of faked products

Liability
Revenue
Reputation
Return

Patterns of illicit actors

Standard procedures to treat cases

Outsourcing (AC service provider)

Supply-Chain Visibility

Visibility of Greymarket/Parallel Trade

Standard procedures to treat cases
…calls for a comprehensive infrastructure of the internet of things.

Core Characteristics:

• look-up service
• quality of real-time
• trusted parties
• defined ownership of data
• scalable data access model
• life-cycle of data
Use Cases of Product Authentication

- Product authentication is a tool that can be used to find counterfeit products

- This tool can be used to achieve following goals

1. Prevent counterfeits from entering the licit distribution channel
2. Help customs to detect infringing products
3. Keep sales-points and end-points clean from counterfeits
4. Enable authentication of products that are in use
5. Enable after sales services to authenticate products
6. Help private investigators
Take home message

- There is no business model for anti-counterfeiting, it is not about ROI, but it is about
  - trust
  - customer safety
  - brand protection
  - countermeasures against future competitors