AGENDA

1. Quick look at Stats for Sub-Saharan Africa
2. What Defines Secure M-Commerce Solutions?
3. Secure M-Commerce Through Mobile User Authentication and Fraud Prevention
   • Mobile App Security
   • Mobile Environment Security
   • Mobile-Friendly User Authentication
4. Conclusion / Questions
QUICK LOOK AT STATS FOR SUB-SAHARAN AFRICA

— KETAN DHOLAKIA, CISM, CRISC
MANAGING PARTNER, MACLEAR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2007

MORE EMPOWERED
“Some seven African countries are in the top 10 fastest growing economies in the world. If you look at countries like Mozambique, Angola, Ethiopia, Zambia, Togo – all of those markets have shown exceptional growth and real stability and with that you almost get a new investment climate for these countries. This allows you to have a new emerging middle class and with that comes a very vibrant entrepreneurship culture; businessmen or ladies who want access to technology and to innovate.”

Telecoms.com
Despite such a modest smartphone user base, mobile usage habits in Africa are on the whole relatively mature. Having been excluded from the PC revolution by price and lack of fixed connectivity, many African nations are not only mobile first, but essentially mobile only markets.

From Somalia to Kenya, mobile phone users are able to pay for petrol, bills and groceries using their mobile handsets, and m-learning is emerging as an affordable option for education in many regions—a scenario that leading operators and handset manufacturers are striving to now recreate in mature markets.

Telecoms.com
IN MID 2013, THERE WERE 253 MILLION UNIQUE MOBILE SUBSCRIBERS IN SUB-SAHARAN AFRICA.
SERVICE INNOVATION ACROSS A RANGE OF ACCESS TECHNOLOGIES

Voice:
- Interactive Voice Response (IVR)
  - National Farmers Information services. (Kenya)

Message:
- SMS
  - Manobi Agriculture (Senegal)
- USSD
  - HIV-911 (South Africa)
  - Tata Telecom m Krishi (India)
- MMS

Browse:
- WAP
  - Killimo Salama (Senegal)
- Web
  - M-FARM (Kenya)

Apps:
- Embedded
  - Nokia Life Tools, Africa
- Java (J2ME)
  - Esoko (Africa)
- Android
  - Infonet Blorvision (Kenya)

Source: GSMA Intelligence
Sometimes I send money to my parents. With the mobile money it goes right away to the person, but through the bank I think that it takes two or three days.”

Male, 25, Ghana

Source: M-Commerce in Sub-Saharan Africa, Ericsson Consumer Insight Summary Report, August 2012
POWER TO THE CONSUMER

Figure 3: Top 10 mobile features used weekly in Sub-Saharan Africa

- 44% Listen to music
- 44% Use social networks
- 44% Take photos or videos
- 38% Play games
- 38% Use instant messaging
- 35% Use bluetooth
- 34% Use calendar
- 26% Send/receive emails
- 72% Send/receive SMS

Source: Ericsson ConsumerLab Analytical Platform 2013
Base: Mobile users in Sub-Saharan Africa (Nigeria, Ghana, South Africa, Kenya, Senegal, Cameroon)

ISACA
Trends in digital payments

Convergence
Numerous form factors
Enablement

Bluetooth 4.0

ISACA
Evolution of mobile contactless (NFC) payments

- 2005: Visa Contactless is introduced
- 2006: Chase introduced the Blink Card
- 2007: Visa introduces the Minicard
- 2008: Launch of Visa payWave
- 2009: The Visa payWave keyfob is launched
- 2010: Visa introduces the Mini SD card for iOS, Blackberry and Android
- 2011: Visa moves to the Cloud
- 2012: Visa payWave preloaded on secure element embedded in Samsung devices
WHAT DEFINES SECURE M-COMMERCE SOLUTIONS?

— TIMO HEIKKINEN, CISA, CGEIT
SENIOR AUDIT SPECIALIST, NORDEA
HELSINKI, FINLAND
ISACA MEMBER SINCE 1999

MORE VALUABLE
WHAT DEFINES SECURE M-COMMERCE SOLUTIONS?

It is no secret that the Internet and the emergence of mobile or m-Commerce have thoroughly revolutionised traditional commerce. Developments in wireless and mobile network technologies are ensuring that this revolution continues.

*The constant state of change means that new vulnerabilities will continue to provide opportunities for hackers and fraudsters and security will continue to be a top priority for mobile enterprises, mobile service providers and mobile app developers alike.*
WHAT DEFINES SECURE M-COMMERCE SOLUTIONS?

It is useful to consider secure m-Commerce solutions as incorporating the managerial and technological procedures and processes that are applied to mobile commerce to provide the following properties:

1. Confidentiality
2. Authentication
3. Integrity
4. Authorisation
5. Availability
6. Non-repudiation

These six areas form the basis of all secure m-commerce solutions.
WHAT DEFINES SECURE M-COMMERCE SOLUTIONS?

**Confidentiality** states that all information must not be divulged to unauthorized persons, devices or processes. It has two types: forward and backward confidentiality.

**Authentication** means that each of the communicating partners are able to identify each other. The purpose of authentication is to ensure that each party to a transaction is 100% verified, trusted and is not an impostor.

**Integrity** maintains the protection of data and makes sure it is not altered, corrupted or changed in any way during transmission by outside unauthorized parties. The successful assurance of in-process integrity during an m-Commerce transaction greatly adds to the overall security.
WHAT DEFINES SECURE M-COMMERCE SOLUTIONS?

**Authorisation** steps to verify that the user is allowed to make purchases must also be facilitated.

**Availability** is where the authorised user has reliable and timely access to personal information so that he/she can adequately perform transactions. Unlike wired services, mobile unavailability of services is a big problem, if not handled properly.

**Non-repudiation** is basically the assurance that a user cannot deny that they have carried out a transaction. With m-Commerce transactions, a digital signature is commonly used to ensure that down the line a person cannot later deny that they did not carry out a given transaction.
To be effective, the security architecture should be capable of providing multiple levels of security services across all of these areas.

Each area may require many policies and procedures, as well as hardware and software tools in some cases, to protect transactions that are processed, stored and transmitted in secure m-Commerce systems.
KEY CHALLENGES

• Mobile commerce (m-commerce) relies on client/server architecture that requires a new breed of fraud prevention solutions that secure the endpoint application.

• Solutions that worked well to identify and verify user PCs, such as device fingerprinting, are not nearly as effective for mobile applications, so enterprises need to compensate and rely on other fraud prevention techniques.

• Enterprises face a confusing plethora of options and point solutions for mobile fraud prevention.
SECURE M-COMMERCE THROUGH MOBILE USER AUTHENTICATION AND FRAUD PREVENTION

— THOMAS BORTON, CISA, CISM, CRISC
DIRECTOR OF IT SECURITY AND COMPLIANCE, COST PLUS
SAN FRANCISCO, CALIFORNIA, USA
ISACA MEMBER SINCE 2004
SOME KEY FACTS

The volume of mobile payments is substantially increasing, and Gartner forecasts that the worldwide mobile payment market will have nearly a half billion users with nearly three quarters of a trillion U.S. dollars in value in 2017, representing double digit compound annual growth rates from 2012 through 2017.

Gartner clients have reported a few types of mobile fraud attacks, including:

- Theft of user credentials used to access mobile applications and then criminal use of those credentials to hijack customer accounts via PC based applications that share the same credentials for user access

- Hijacking and diverting of SMS messages sent to user mobile devices for user authentication or verification of transactions initiated on PCs
The main requirement of defense against mobile fraud is to fortify the application on the endpoint, where the OS and platform may be weak, and the users may be clueless as to any mobile threats against them.

Everything else involves successive layers of server defenses that are likely to be robust against basic attacks when adjusted to score fraud behaviors involving mobile transactions.

For example, new rules and statistical models are needed to evaluate payments made from a mobile wallet.
Almost all these reported attacks have targeted online banking accessed via Android OS based devices.

It's just a matter of a couple of years before these mobile scams become more prevalent and before fraudsters start targeting other mobile OSs.

Gartner's strategy for fighting fraud includes a five layered approach and is based on the fact that determined criminals circumvent most fraud prevention and authentication methods, so the more layers that surround key assets, the harder it will be for fraudsters to penetrate sensitive applications.

Mobile commerce demands new types of user authentication and endpoint centric fraud prevention solutions. We outline three categories of applications and services that help enterprises secure mcommerce.
THREE BROAD CATEGORIES OF INNOVATION TO SECURE M-COMMERCE

1. **Mobile app security**: Methods to secure the apps themselves against exploitation.
2. **Mobile environment security**: Defenses that address weaknesses in mobile platforms
3. **Mobile friendly user authentication**: Improvements in human interactions enabled on mobile devices so that users can be strongly authenticated

The solutions outlined below are usable in mcommerce environments (mainly business to consumer [B2C]) where endpoints are uncontrolled.

*For example, master data management and cloud security brokerage services are not discussed as security options, because these are only practical in a controllable enterprise business to employee setting.*
PRIORITIZE AND CHOOSE FROM AMONGST THE THREE CATEGORIES FOR SECURING YOUR MCOMMERCE

Enterprises should analyse and choose at least one solution from each of these three categories to secure the mobile application, the environment supporting it and authentication of the users.

Priority should be given to mobile application security and user authentication, and lastly to securing the mobile environment.
Mobile App Security

The goal of mobile app security is to prevent apps from being corrupted.

There are three approaches that can be adopted in all use cases.

The first is to add self defense to mobile apps, the second is to use post compile enhancements, and the third is to only use clean sources for apps.

- Self defending mobile apps can be created by means of good coding practices, as well as postproduction remedies.
- If apps do not contain measures for self defense, then it is easy for hackers to modify apps by injecting malware or even replacing apps with rogue ones.
MOBILE APP SECURITY

RECOMMENDED PRACTICES FOR DEVELOPERS

• Use of static and dynamic software testing tools to scan for weaknesses (sample vendors: Veracode and Coverity)

• Use of software development kits (SDKs) that integrate technical defenses to secure the apps (sample vendors: Arxan, Sencha and Metaforic)

• Compiling to work inside containerization environments (sample vendor: Good Dynamics)
• Finished apps can be fortified after compilation, if there is no efficient way to recompile them.

• Several methodologies exist to modify runtime apps by adding tamper tests, license management, certificate checking and local file encryption.
MOBILE APP SECURITY

RECOMMENDED PRACTICES FOR FINISHED APPS

• Use of app wrapping tools for individual apps (sample vendor: Mocana)

• Use of app wrapping tools for entry into containerization environments (note that containerization environments are generally only available to enterprise employees whose mobile devices can be managed) (sample vendors: Good [AppCentral] and Symantec [Nukona])
MOBILE APP SECURITY

• Strict policies for sources for clean apps is a successful strategy, because users are restricted from side loading unknown apps by default.

• In a B2C setting, this cannot be enforced. However, if the original app was written with Anti-tampering and a digital signature, users can be encouraged to install only from authorized sources.
MOBILE APP SECURITY

RECOMMENDED PRACTICE

• Allow only apps installed from curated public app stores, such as iTunes or Google Play.

• Where appropriate, distribute apps through a private curated store, such as Appthority.

• Test for identity factors that will only be present in an authorized distribution.
• Additionally, if the mobile application uses a mobile browser, then it is possible to deploy more secure mobile browsers on demand.

• These browsers are stripped down so that unnecessary functions and capabilities, such as plugins or storage of data in memory cache after a user logs off, are disabled, and all that the users can do with that secure browser is interact with the service providers' sites.

Sample vendors: Quarri Technologies and Wontok
MOBILE ENVIRONMENT SECURITY

— NATHAN ANDERSON, CISA, CRISC
INTERNAL AUDIT DIRECTOR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2010

MORE CAPABLE
The goal of mobile environment security is to prevent devices from being corrupted.

**App store scanning**

- This category entails the scanning of app stores for malicious applications that use an enterprise brand, usually for unauthorized financial gain.
- These malicious applications can be downloaded by innocent end users who do not realize the app's intent is to take over their device and accounts.
- The app store scanners scan hundreds or thousands of app stores, typically the most widely accessed stores by the general consumer population.
- These services are by no means foolproof, and there have been instances where malware gets into app stores that is not caught by the scanners.
- It is always preferable for app providers to use measures and app stores under their control.

*Sample vendors: RiskIQ; WMC Global; Webroot; App Authority; RSA, The Security Division of EMC; and TrendMicro (BitDefender)*
The goal of mobile environment security is to prevent devices from being corrupted.

Checking for Unsecure Devices

• Even if the company doesn't provide an agent for consumers using its mobile application, there are APIs that can and should be queried.

• It's possible for the server and the app, for example, to refuse to run on a jailbroken device.

Sample vendors: InAuth, IBM/Trusteer Versafe and Webroot
MOBILE ENVIRONMENT SECURITY

The goal of mobile environment security is to prevent devices from being corrupted.

Mobile Antimalware

• This is not a substitute for good app design, nor for other aspects of mobile environment security. It is often not effective against new threats and can be resource intensive for a mobile device.
• However, it should be considered in B2C applications where there are limits on managing and controlling the end user’s mobile device and if perceived as critical to app adoption.
• These solutions seek to protect user interactions with mcommerce services from mobile malware, such as keystroke logging, SMS diversion or other types of mobile attacks.
• They employ a wide range of defensive measures that check for unusual mobile application behavior.
• If an application is suspected of being infected, the enterprise is alerted and can then decide how to proceed – whether to disable user access, lower the privileges on the session or force the user to disinfect his or her mobile device.

Sample vendors: IBM/Trusteer Versafe and Webroot
MOBILE-FRIENDLY USER AUTHENTICATION

— NATHAN ANDERSON, CISA, CRISC
INTERNAL AUDIT DIRECTOR
CHICAGO, ILLINOIS, USA
ISACA MEMBER SINCE 2010

MORE CAPABLE
MOBILE-FRIENDLY USER AUTHENTICATION

• Mobile devices enable many different factors to be leveraged for mcommerce user authentication.

• On the other hand, several PC based methods that are commonly used in B2C applications, notably secret questions and answers, are kludged (and somewhat unsecure) when used on mobile devices.

• Enterprises should take advantage of improved human interfaces enabled on mobile devices so that users can be strongly authenticated.
Biometric authentication

- Mobile devices provide rich opportunities to engage in biometric authentication, because their form factors have built-in features that enable biometric capture – that is, a microphone for voice, and a camera for retina or fingerprint capture.

- However, mobile biometric authentication is still emerging and has not been deployed in large scale applications.

- Users should proceed with caution and engage in proof of concept pilots before committing to implementations.
MOBILE-FRIENDLY USER AUTHENTICATION

• Behavioral authentication is a type of biometric authentication that garners considerable interest among Gartner clients examining mobile user authentication methods. (It also can be used to strengthen user authentication for PC based applications.)

• Behavioral authentication is invisible to the user, and measures and records the user’s keystroke and typing rhythms, mouse and screen interface movements (for example, how a user enlarges images on a smartphone), and effectively creates a "bioprint" for that user. This bioprint can be used to authenticate the user during repeated logins to a service.

• It can also be used to detect the "humanness" of an application session (to detect a scripted attack) or remote control of a user account from the user's mobile account. This can be achieved, since the bioprint is transmitted to the server with delays and spurts that indicate the user is actually logging in from somewhere other than the device the user is purporting to be using.

Sample vendors: Multiple biometric factors – Daon and Mobeel Voice – Agnitio, Nuance, Behavioral, BioCatch, NuData, AdmitOne Security, Deepnet Security/TypeSense, bioChec, Trustable Passwords, ID Control, BehavioSec, Delfego and Intensity Analytics
Public key infrastructure (PKI) for SMS messages

- This method secures two way user authentication or transaction verification using PKI and x.509 electronic certificates deployed to the user's mobile device.

- It also provides mutual authentication of the user's device and the enterprise server.

- This method is effective for securing mobile and regular ecommerce.

Sample vendors: Entersekt and CA
MOBILE-FRIENDLY USER AUTHENTICATION

PKI and soft onetime passwords (OTPs)

• These methods include OTP generators that are downloaded to the user's mobile device.

• Communications between the server and device are typically secured through PKI and mobile resident certificates. Although OTPs are used to authenticate users with dynamic passwords, they also serve as strong mobile device identifiers after the software that generates them is downloaded by the user.

• The generated OTP can be passed back to the server application, without active user involvement, and can be totally transparent while still very effective.

Sample vendors: CA, Entrust, RSA and Symantec
Device identification

- Gartner has identified five methods of endpoint or device identification that are helpful as a factor to be used during user authentication.
- (For a full analysis of these methods. The most effective method for catching fraudsters using PC platforms is via browser mining with JavaScript – where the JavaScript program on the enterprise server home page (and any other pages that a user interacts with) collects as many attributes as possible from the user’s mobile browser so that it can be "fingerprinted" for future reference.
- Gartner clients report about a 15% fraud detection lift for Web based applications accessed via desktops and PCs.
- However, server based device identification (using a JavaScript) is generally much less effective in mobile computing, because there are not enough differentiating elements that the server can grab from the device.

Sample vendors: iovation, ThreatMetrix, IBM/Trusteer, 41st Parameter, Entrust, CA and RSA
Mobile device combined with user attributes for stronger authentication

In this category, mobile device information is combined (or bound) with user attributes to enable stronger (than password) user authentication.

The information that can be combined, but is not limited to:
MOBILE-FRIENDLY USER AUTHENTICATION

Mobile device information

- The mobile device itself, as known from its hardware resident or subscriber identifiers (for example, International Mobile Station Equipment Identity, MAC address, International Mobile Subscriber Identity and SIM card)
- The mobile phone number and its status
- The carrier network
- The mobile device's location

User attributes

- A biometric factor belonging to the user (such as voice, iris scan or fingerprint) captured through the mobile device microphone or camera
- A password entered by the user
- Financial transaction information associated with the device and its owner (as recorded from past interactions; only provided by Early Warning for now)
MOBILE-FRIENDLY USER AUTHENTICATION

- Vendors are using their various capabilities to combine device information with user attributes for user authentication.

- The user’s authentication credential can be securely shared across organizations that subscribe to the same service.

- In fact, the Fast IDentity Online (FIDO) Alliance was established to standardize on the sharing of authentication based on mobile device and user attributes (such as biometrics) across organizations and is sponsored by Internet companies, such as PayPal, Google and Microsoft.

Sample vendors: Duo Security, Authentify, TeleSign, Nok Nok Labs and Early Warning
CONCLUSION

— ROSEMARY AMATO, CISA
DIRECTOR, DELoitTE
AMSTERDAM, THE NETHERLANDS
ISACA MEMBER SINCE 1998

ACCOMPLISH MORE
CONCLUSION

- There are numerous endpoint centric (Layer 1 in Gartner's Five Layer parlance) point solutions and services that enterprises can adopt to secure mcommerce.

- Over time, the market will consolidate so that enterprises won't have to work with so many separate vendors to gain the fraud protection they require.

- Recommendation for now, is that enterprises should prioritize requirements and choose at least one solution from each of the three categories to help ensure that the mobile application is as secure as possible, user authentication is strengthened using mobile-friendly methods, and the environment surrounding the mobile application is secured.

- Priority should be given to mobile application security and user authentication, and lastly to securing the mobile environment, because that is the least manageable and predictable component in B2C mcommerce.
For example, and at a minimum, Gartner recommends that B2C mcommerce application service providers:

- Fortify the application using SDKs that secure the application.
- Check for jailbroken devices, and do not run sensitive applications on them.
- Evaluate and implement behavioral user authentication in applications where extra authentication should be invisible to the users, either because of user experience or security needs.
- Evaluate and implement user authentication that leverages the mobile device as a second factor in applications where it's acceptable to impose extra security requirements on the end user.
## BEST PRACTICES FOR RISK MANAGEMENT

### Many data elements are combined...

<table>
<thead>
<tr>
<th>Consumer transaction history</th>
<th>Device fingerprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone area code</td>
<td>Product type</td>
</tr>
<tr>
<td>Refund history</td>
<td>Geo-location match</td>
</tr>
<tr>
<td>Recent txn velocity</td>
<td>Consumer time on file</td>
</tr>
<tr>
<td>Merchant industry</td>
<td>IP address</td>
</tr>
<tr>
<td>Purchase amount</td>
<td>Carrier</td>
</tr>
<tr>
<td>Time stamp</td>
<td>Country</td>
</tr>
</tbody>
</table>

### ...to assess risk and rewards...

- Transaction risk level
- Consumer risk level
- Consumer lifetime value

### ...and to take action

- Bar user
- Block transaction
- Review transaction
- Reverse transaction
- Warn merchant
- Monitor consumer
- Allow transaction
QUESTIONS