NIGERIAN COMMUNICATIONS COMMISSION

Developmental Imperatives of Mobile Money and Implications on Security

Thabiso MOERANE

March 2012

Alcatel·Lucent

Summary

The proliferation of Mobile Money services, particularly "Person-to-Person Transfer Services" provide a foundation for Developing Countries to promote Financial Inclusion. Financial Inclusion requires a formal financial system that can be trusted by the users. Service Providers of Mobile Money services are, or at least should be, considered part of the formal financial system. This is because the operation of the formal financial system is profoundly important for economic growth and poverty alleviation. It influences how many people are hungry, homeless, and in pain. It shapes the gap between the rich and the poor. It arbitrates who can start a business and who cannot, who can pay for education and who cannot, who can attempt to realize one's dreams and who cannot (WEF, 2008)…

The challenge facing Mobile Money Service Providers in Developing Countries is finding a balance amongst dynamics that are seemingly in conflict:

"Affordability; Relevant Service; Customer Experience and Security…"

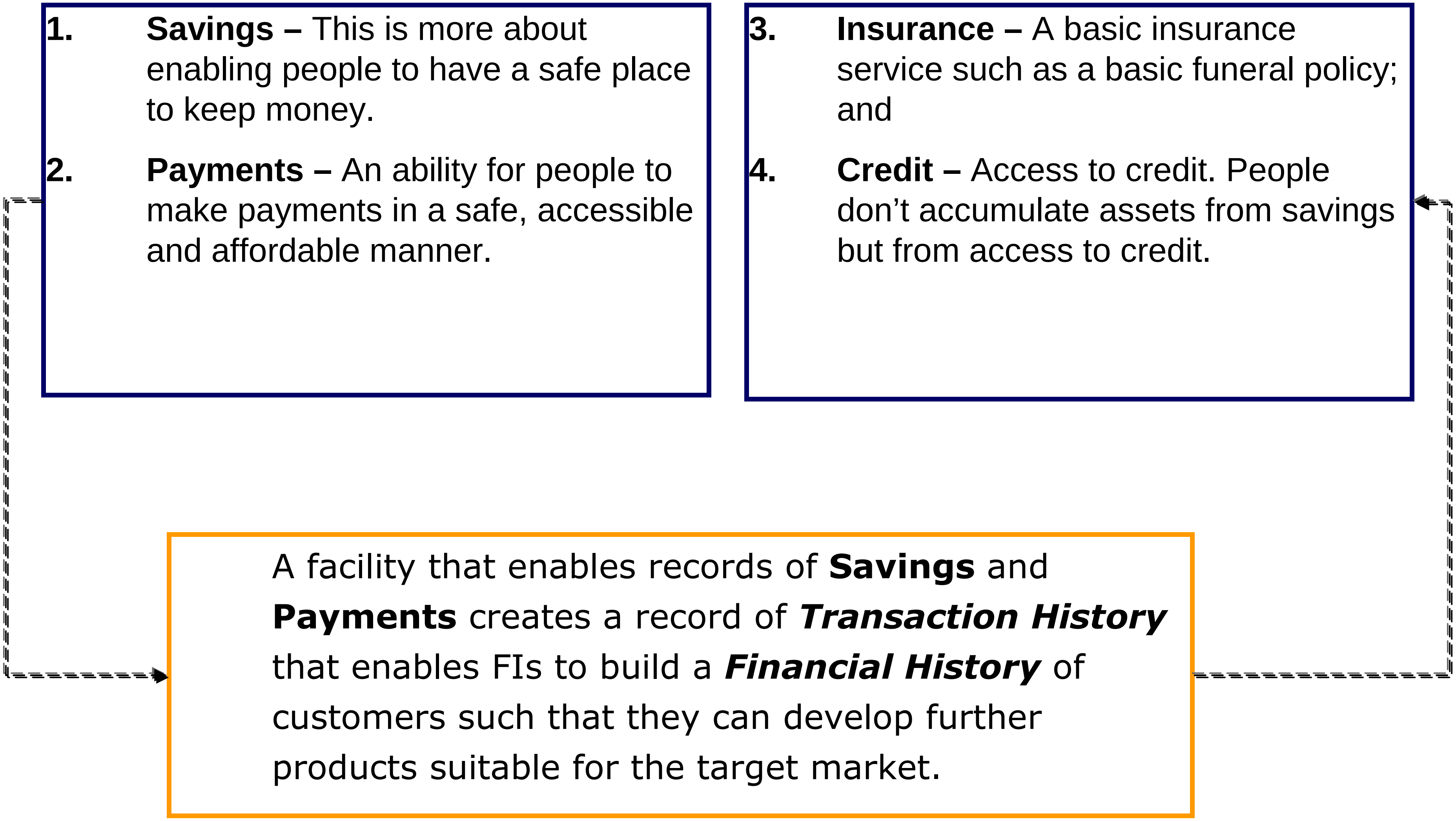
Contents

- Background
- Financial Inclusion: Main Requirements
- Nigeria Market Profile
- Mobile Banking/Payments Regulatory Framework in Nigeria
- Service Description
- Customer Experience
- Security
- Conclusion
- Questions

Financial Inclusion

Main Requirements

Minimum Services Required to Achieve Financial Inclusion



1. **Savings –** This is more about enabling people to have a safe place to keep money.
2. **Payments –** An ability for people to make payments in a safe, accessible and affordable manner.
3. **Insurance –** A basic insurance service such as a basic funeral policy; and
4. **Credit –** Access to credit. People don't accumulate assets from savings but from access to credit.

A facility that enables records of **Savings** and **Payments** creates a record of ***Transaction History*** that enables FIs to build a ***Financial History*** of customers such that they can develop further products suitable for the target market.

Socially Desirable Outcomes

Financial Development: The efficiency of the financial system as a payments mechanism and intermediation system is maximised and in turn, contribute to overall economic growth.

Financial Stability: The safety and soundness of the banking and payments system is not compromised.

Financial Integrity: The service should not compromise the financial system through abuse for criminal and terrorist financing purposes

Financial Inclusion: Financial Inclusion is delivering affordable financial services to the vast sections of the disadvantaged and low income groups.

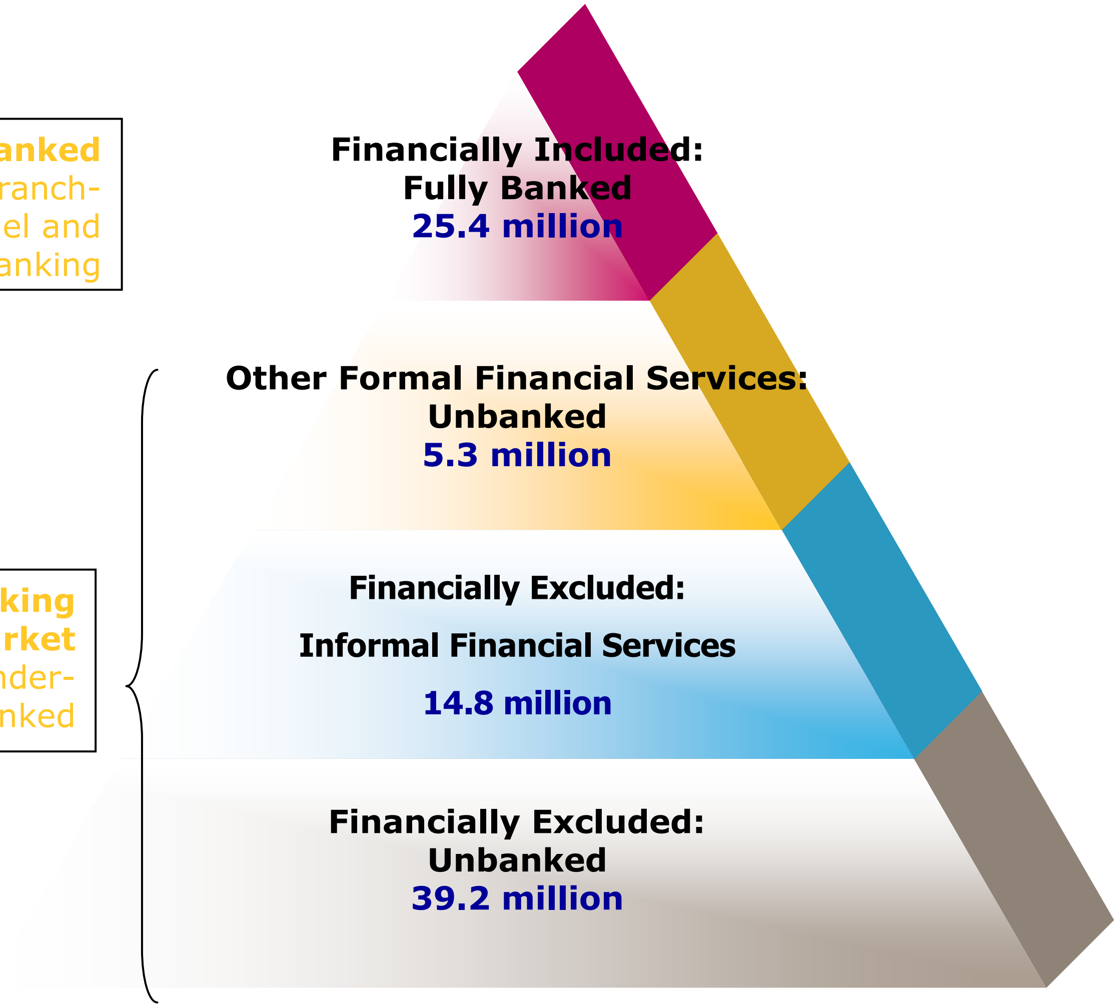
Consumer Protection: The customers must enjoy adequate protection as provided for by legislation

Nigeria Market Profile

Affordability and Market Size

Mobile Banking Target Market

Fully-Banked
Services by Branch-Centric Model and Internet Banking



Financially Included:
Fully Banked
25.4 million

Other Formal Financial Services:
Unbanked
5.3 million

Financially Excluded:
Informal Financial Services
14.8 million

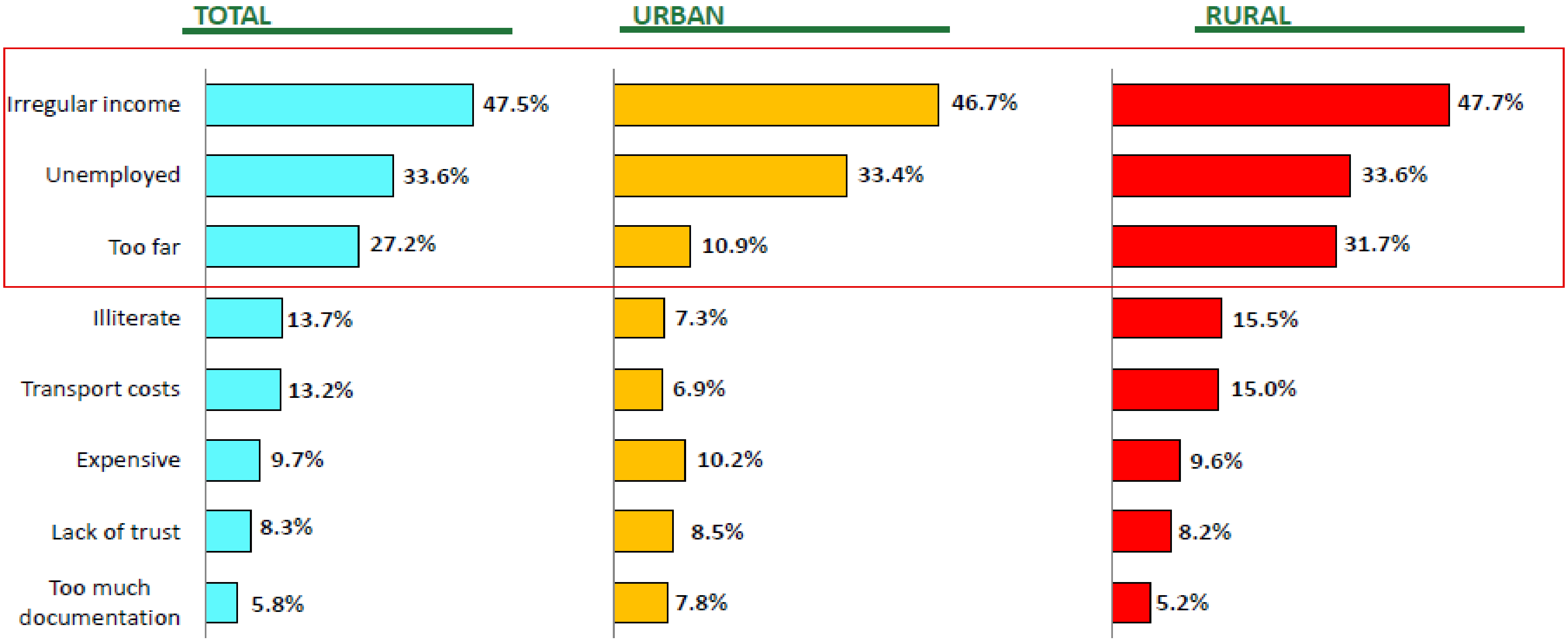
Financially Excluded:
Unbanked
39.2 million

Mobile Banking Target Market
Currently un/under-banked

Source: EFInA, 2010

Barriers to Banking in Nigeria

- The main barriers to banking in Nigeria are irregular income, unemployment and distance, particularly in rural areas



Source: EFInA, 2010

Nigeria Demographics: Affordability

Adult Population (18+ years)		**84,700,000**				
Affordability					****2%**	
Exchange Rate						*****151.774**
	Monthly Income Levels*	**Population***	**%age of Population***	**Maximum Income per Level***	**Affordable Bank Fees pm**	**Affordable Bank Fees pm**
LSM 1	Don't Know	18,125,800	21.4%			
LSM 1	No Income	9,232,300	10.9%	NGN 0	NGN 0	$0
	Sub-Total	**27,358,100**	**32.3%**			
LSM 1	<N250	1,694,000	2.0%	NGN 250	NGN 5	$0.03
LSM 2	N251-N1,000	3,472,700	4.1%	NGN 1,000	NGN 20	$0.13
LSM 3	N1,000-N2,000	6,437,200	7.6%	NGN 2,000	NGN 40	$0.26
LSM 4	N2,001-N6,000	8,385,300	9.9%	NGN 6,000	NGN 120	$0.79
LSM 5	N6,000-N13,000	10,248,700	12.1%	NGN 13,000	NGN 260	$1.71
Weighted Average Affordability		**30,237,900**	**35.7%**		**NGN 132**	**$0.87**
LSM 6	N13,001-N20,000	7,961,800	9.4%	NGN 20,000	NGN 400	$2.64
LSM 7	N20,001-N40,000	5,166,700	6.1%	NGN 40,000	NGN 800	$5.27
LSM 8	N40,001-N70,000	2,710,400	3.2%	NGN 70,000	NGN 1,400	$9.22
LSM 9	N70,001-N100,000	592,900	0.7%	NGN 100,000	NGN 2,000	$13.18
LSM 10	>N100,000	592,900	0.7%	NGN 100,000	NGN 2,000	$13.18
	Refused to Answer	10,164,000	12.0%			
		27,188,700	**32.1%**			
	Total	**84,784,700**	**100.1%**			

Sources: EFInA*; Finmark Trust**; Oanda***

Mobile Banking/Payments Regulatory Framework in Nigeria

In Compliance with the Central Bank of Nigeria (CBN) Regulatory Framework for Mobile Payment Services in Nigeria

Nigeria Regulatory Framework: Models & Services

Bank-Focused (Banks Only)	**Bank-Led (Consortium)**	**Non-Bank-Led**
Participants		
Initiating Bank	Initiating Bank/s	Corporate Organisation
ICT Partner/s	Partner Organisations	Partner/s
	•Scheme Operator/s	
	•MNOs	
	•Independent Operator/s	
Mobile Payment Scenarios		
Bank Account-Based	**Card Account-Based**	**System-Based (SVA)**
Services		
Provide all m-Payment services	Provide all financial services	Provide and manage technology
Facilitate International Remittances	Provide and manage technology	Provide Agent Network
	Provide Agent Network	Facilitate International Remittances
	Facilitate International Remittances	

Service Description

Mobile Payment Service

m-Commerce & m-Payments

- Mobile Money is NOT an end in itself but a means to an end, which is enabling m-Commerce by enabling m-Payments for services…
- Therefore, there are only two types of payments: Proximity and Remote…

Proximity Payments

- Cash-In/Cash-Out
- Retail Purchases
- Bill Payment through Retailer (Agent)
- Money Transfer through Retailer (Agent) – Domestic
- Pre-Paid Services: Top-Up through Retailer (Agent) – Airtime, Electricity, Water

Remote Payments

- Bill Payment
- Money Transfer – Domestic
- Pre-Paid Services: Top-Up – Airtime, Electricity, Water

The only difference between a proximity and a remote payment is that the proximity payment involves a retailer (who is either an agent or a merchant or BOTH) whereas a remote payment doesn't!

Customer Experience

THE CUSTOMER JOURNEY (m-Commerce):
TOUCHPOINT MAP

1 AWARENESS 2 INTERACT 3 AGREE/GET 4 CONSUME 5 USE 6 PAY 7 REWARD 8 LEAVE

1

AWARENESS

- Brand image: personality

2

INTERACT

- Service promise
- Selection and value

3

AGREE/GET

- Discover: easy to find, search, recommend (e.g. portal)
- Channels: store, portal, CSR
- Easy registration as customer
- Activate: easy to buy, quick and easy services delivery
- Personalize: bundle flexibility

4

CONSUME

- Perceived service quality
- Change, add, end services
- Simple and easy to modify account (e.g. add members modify privileges)

5

USE

- Problem, question, change interaction
- Self serve, CSR, IVR: portal, chat, phone, social
- Information availability
- Authority to fix

6

PAY

- Billing and reporting: paper, electronic
- Understand
- Self service
- Payment options

7

REWARD

- Loyalty program

8

LEAVE

- Easy and friendly
- Keep record for ease of return

Source: Alcatel Lucent, 2012

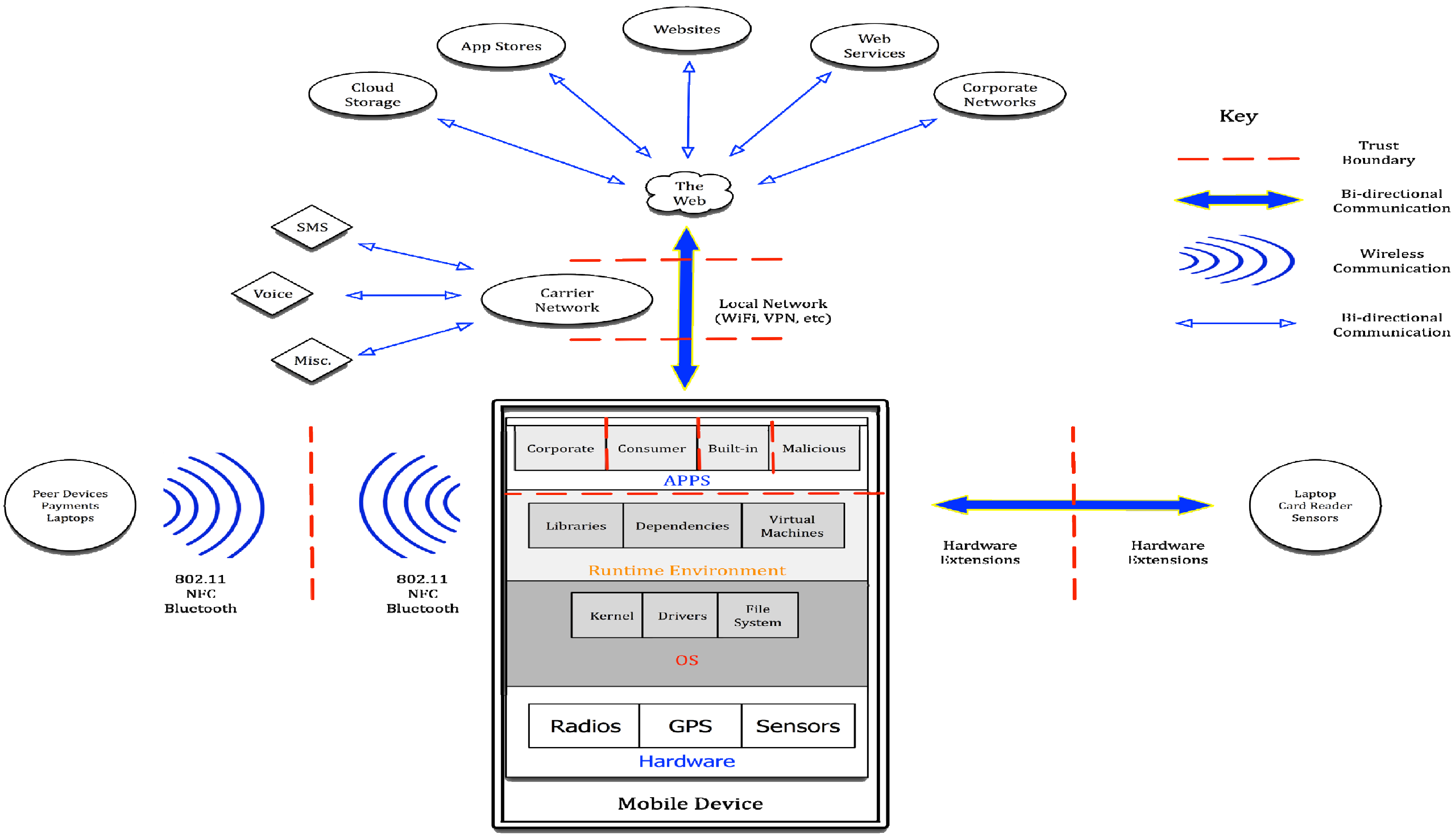
Security

Open Web Application Security Project (OWASP)

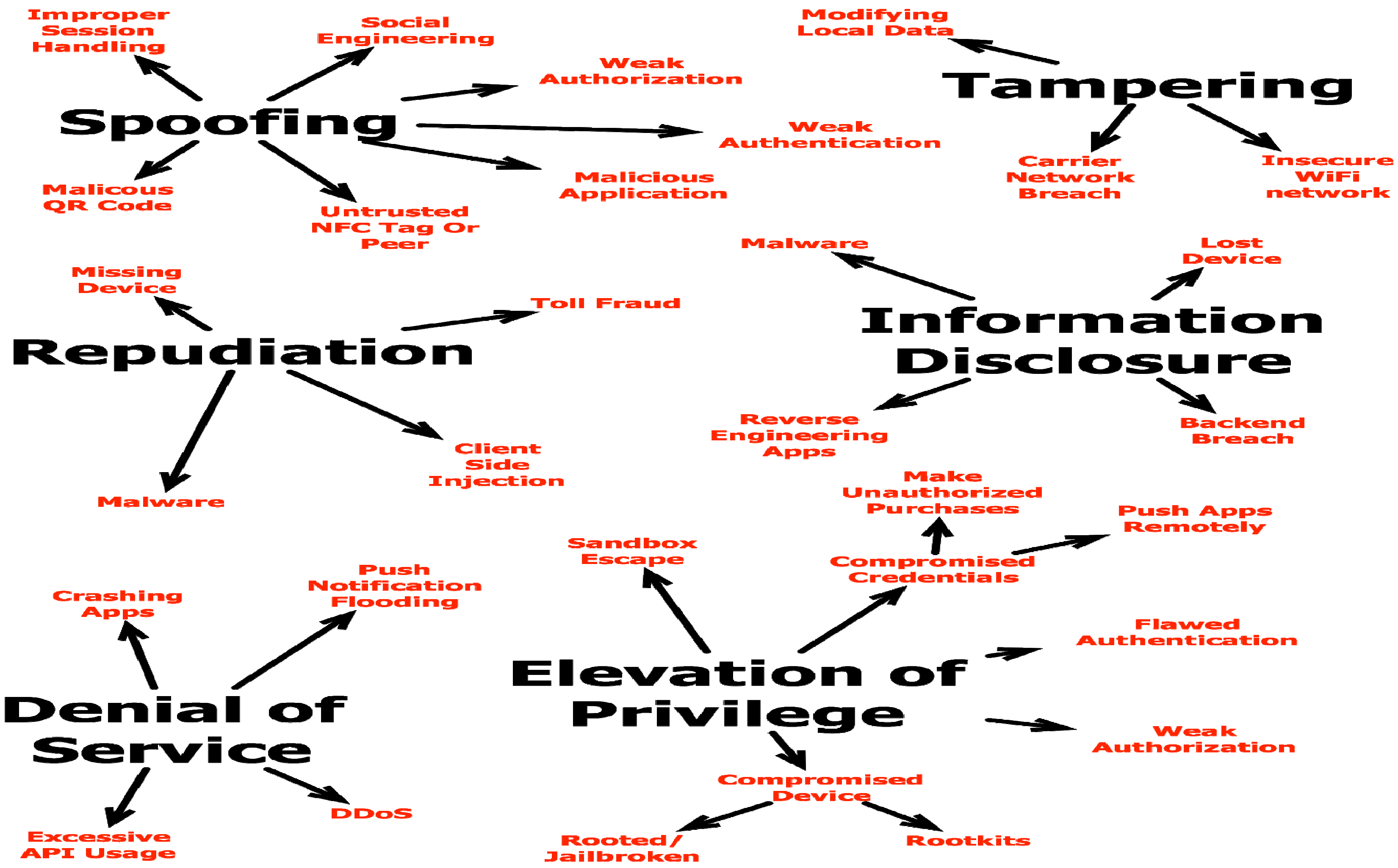
Top 10 Mobile Risks

Source: OWASP, 2011

Mobile Threat Model



Mobile Threat Model



Spoofing
- Improper Session Handling
- Social Engineering
- Weak Authorization
- Weak Authentication
- Malicious Application
- Untrusted NFC Tag Or Peer
- Malicous QR Code

Tampering
- Modifying Local Data
- Carrier Network Breach
- Insecure WiFi network

Repudiation
- Missing Device
- Toll Fraud
- Client Side Injection
- Malware

Information Disclosure
- Malware
- Lost Device
- Reverse Engineering Apps
- Backend Breach

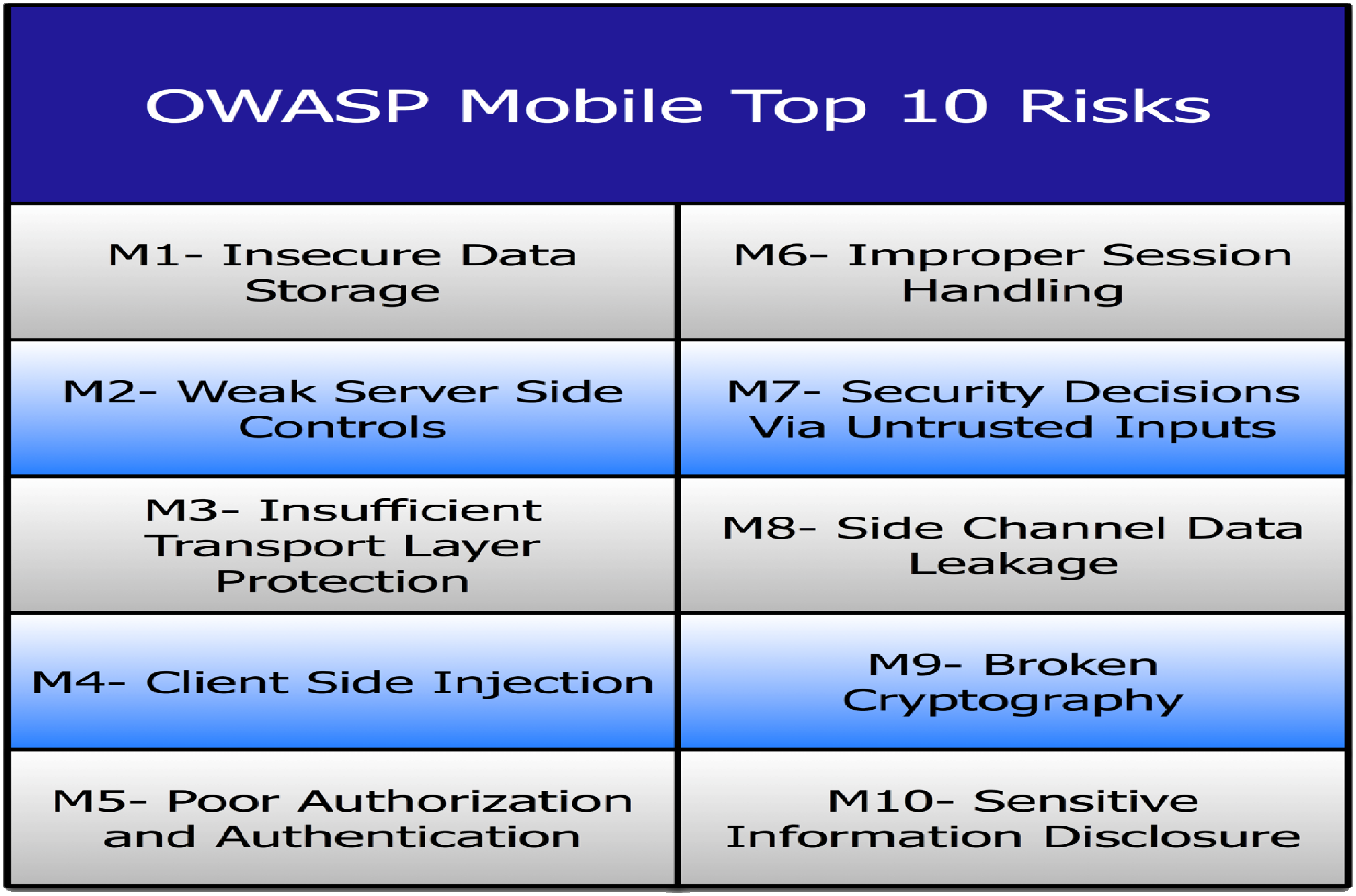
Denial of Service
- Crashing Apps
- Push Notification Flooding
- Excessive API Usage
- DDoS

Elevation of Privilege
- Sandbox Escape
- Compromised Credentials
  - Make Unauthorized Purchases
  - Push Apps Remotely
- Flawed Authentication
- Weak Authorization
- Compromised Device
  - Rooted/ Jailbroken
  - Rootkits

AT THE SPEED OF IDEAS™

Alcatel·Lucent

Top 10 Risks



OWASP Mobile Top 10 Risks	
M1- Insecure Data Storage	M6- Improper Session Handling
M2- Weak Server Side Controls	M7- Security Decisions Via Untrusted Inputs
M3- Insufficient Transport Layer Protection	M8- Side Channel Data Leakage
M4- Client Side Injection	M9- Broken Cryptography
M5- Poor Authorization and Authentication	M10- Sensitive Information Disclosure

M1- Insecure Data Storage

- Sensitive data left unprotected
- Applies to locally stored data + cloud synced
- Generally a result of:
  - Not encrypting data
  - Caching data not intended for long-term storage
  - Weak or global permissions
  - Not leveraging platform best-practices

Impact

- Confidentiality of data lost
- Credentials disclosed
- Privacy violations
- Non-compliance

M1- Insecure Data Storage
Prevention Tips

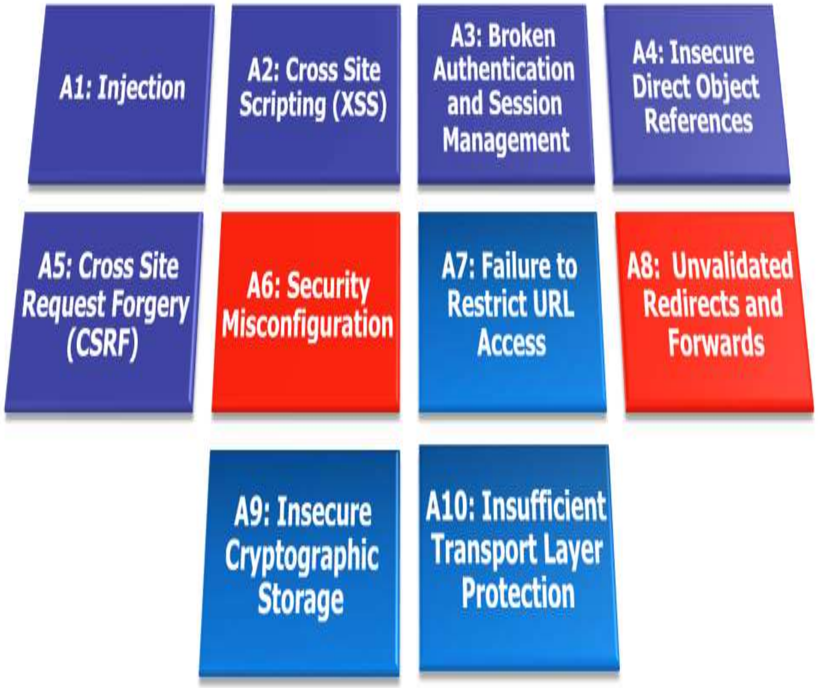
- Store ONLY what is absolutely required
- Never use public storage areas (ie- SD card)
- Leverage secure containers and platform provided file encryption APIs
- Do not grant files world readable or world writeable permissions

Control#	Description
1.1-1.14	Identify and protect sensitive data on the mobile device
2.1, 2.2, 2.5	Handle password credentials securely on the device

M2- Weak Server Side Controls

OWASP Top 10

•https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



A1: Injection

A2: Cross Site Scripting (XSS)

A3: Broken Authentication and Session Management

A4: Insecure Direct Object References

A5: Cross Site Request Forgery (CSRF)

A6: Security Misconfiguration

A7: Failure to Restrict URL Access

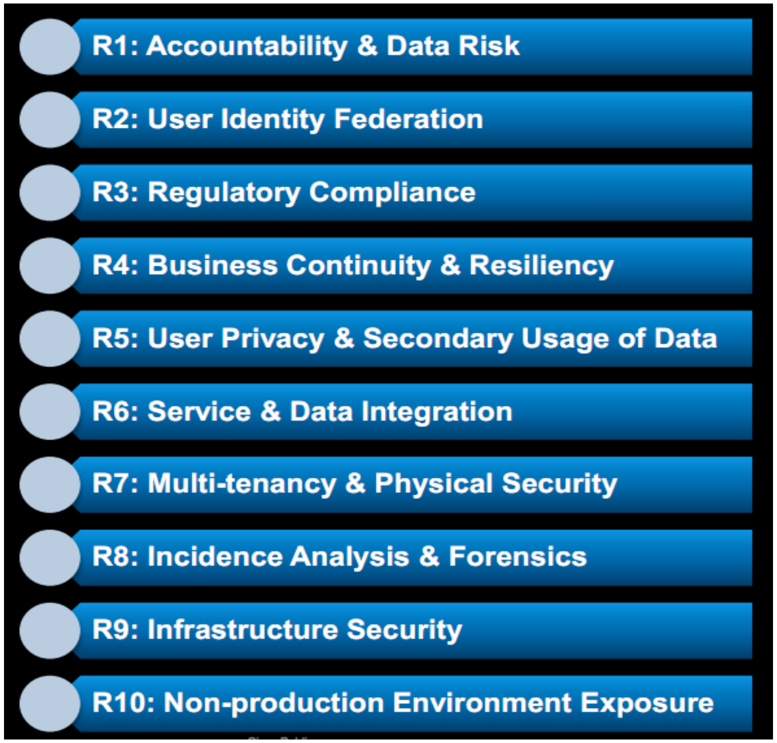
A8: Unvalidated Redirects and Forwards

A9: Insecure Cryptographic Storage

A10: Insufficient Transport Layer Protection

OWASP Cloud Top 10

https://www.owasp.org/images/4/47/Cloud-Top10-Security-Risks.pdf



R1: Accountability & Data Risk

R2: User Identity Federation

R3: Regulatory Compliance

R4: Business Continuity & Resiliency

R5: User Privacy & Secondary Usage of Data

R6: Service & Data Integration

R7: Multi-tenancy & Physical Security

R8: Incidence Analysis & Forensics

R9: Infrastructure Security

R10: Non-production Environment Exposure

M2- Weak Server Side Controls
Prevention Tips

- Understand the additional risks mobile apps introduce into existing architectures
- Leverage the wealth of knowledge that is already out there
- OWASP Web Top 10, Cloud Top 10, Web Services Top 10
- Cheat sheets, development guides, ESAPI

Control#	Description
5.1-5.8	Keep the backend APIs (services) and the platform (server) secure

M3- Insufficient Transport Layer Protection

- Complete lack of encryption for transmitted data
  - Yes, this unfortunately happens *often*
- Weakly encrypted data in transit
- Strong encryption, but ignoring security warnings
  - Ignoring certificate validation errors
  - Falling back to plain text after failures

Impact

- Man-in-the-middle attacks
- Tampering w/ data in transit
- Confidentiality of data lost

M3- Insufficient Transport Layer Protection *Prevention Tips*

- Ensure that all sensitive data leaving the device is encrypted
- This includes data over carrier networks, WiFi, and even NFC
- When security exceptions are thrown, it's generally for a reason…*DO NOT* ignore them!

Control#	Description
3.1.3.6	Ensure sensitive data is protected in transit

M4- Client Side Injection

- Apps using browser libraries
  - Pure web apps
  - Hybrid web/native apps
- Some familiar faces
  - XSS and HTML Injection
  - SQL Injection
- New and exciting twists
  - Abusing phone dialer + SMS
  - Abusing in-app payments

Impact

- Device compromise
- Toll fraud
- Privilege escalation

M4- Client Side Injection

Prevention Tips

- Sanitize or escape untrusted data before rendering or executing it
- Use prepared statements for database calls…concatenation is still bad, and always will be bad
- Minimize the sensitive native capabilities tied to hybrid web functionality

Control#	Description
6.3	Pay particular attention to validating all data received from and sent to non-trusted third party apps before processing
10.1-10.5	Carefully check any runtime interpretation of code for errors

M5- Poor Authorization and Authentication

- Part mobile, part architecture
- Some apps rely solely on immutable, potentially compromised values (IMEI, IMSI, UUID)
- Hardware identifiers persist across data wipes and factory resets
- Adding contextual information is useful, but not foolproof

Impact

- Privilege escalation
- Unauthorized access

M5- Poor Authorization and Authentication *Prevention Tips*

- Contextual info can enhance things, but only as part of a multi-factor implementation
- Out-of-band doesn't work when it's all the same device
- Never use device ID or subscriber ID as sole authenticator

Control#	Description
4.1-4.6	Implement user authentication/authorization and session management correctly
8.4	Authenticate all API calls to paid resources

M6- Improper Session Handling

- Mobile app sessions are generally MUCH longer
- Why? Convenience and usability
- Apps maintain sessions via
  - HTTP cookies
  - OAuth tokens
  - SSO authentication services
- Bad idea= using a device identifier as a session token

Impact

- Privilege escalation
- Unauthorized access
- Circumvent licensing and payments

M6- Improper Session Handling
Prevention Tips

- Don’t be afraid to make users re-authenticate every so often
- Ensure that tokens can be revoked quickly in the event of a lost/stolen device
- Utilize high entropy, tested token generation resources

Control#	Description
1.13	Use non-persistent identifiers
4.1-4.6	Implement user authentication/authorization and session management correctly

M7- Security Decisions Via Untrusted Inputs

- Can be leveraged to bypass permissions and security models
- Similar but different depending on platform
  - iOS- Abusing URL Schemes
  - Android- Abusing Intents
- Several attack vectors
  - Malicious apps
  - Client side injection

Impact

- Consuming paid resources
- Data exfiltration
- Privilege escalation

M7- Security Decisions Via Untrusted Inputs

Prevention Tips

- Check caller’s permissions at input boundaries
- Prompt the user for additional authorization before allowing
- Where permission checks cannot be performed, ensure additional steps required to launch sensitive actions

Control#	Description
10.2	Run interpreters at minimal privilege levels

M8- Side Channel Data Leakage

- Mix of not disabling platform features and programmatic flaws
- Sensitive data ends up in unintended places
  - Web caches
  - Keystroke logging
  - Screenshots (ie- iOS backgrounding)
  - Logs (system, crash)
  - Temp directories
- Understand what 3rd party libraries in your apps are doing with user data (ie- ad networks, analytics)

Impact

- Data retained indefinitely
- Privacy violations

M8- Side Channel Data Leakage

Prevention Tips

- Never log credentials, PII, or other sensitive data to system logs
- Remove sensitive data before screenshots are taken, disable keystroke logging per field, and utilize anti-caching directives for web content
- Debug your apps before releasing them to observe files created, written to, or modified in any way
- Carefully review any third party libraries you introduce and the data they consume
- Test your applications across as many platform versions as possible

Control#	Description
7.3	Check whether you are collecting PII, it may not always be obvious
7.4	Audit communication mechanisms to check for unintended leaks (e.g. image metadata)

M9- Broken Cryptography

- Two primary categories
  - Broken implementations using strong crypto libraries
  - Custom, easily defeated crypto implementations
- Encoding != encryption
- Obfuscation != encryption
- Serialization != encryption

Impact

- Confidentiality of data lost
- Privilege escalation
- Circumvent business logic

M9- Broken Cryptography

Prevention Tips

- Storing the key with the encrypted data negates everything
- Leverage battle-tested crypto libraries vice writing your own
- Take advantage of what your platform already provides!

Control#	Description
1.3	Utilize file encryption API’s
2.3	Leverage secure containers

M10- Sensitive Information Disclosure

- We differentiate by stored (M1) vs. embedded/hardcoded (M10)
- Apps can be reverse engineered with relative ease
- Code obfuscation raises the bar, but doesn't eliminate the risk
- Commonly found "treasures":
  - API keys
  - Passwords
  - Sensitive business logic

Impact

- Credentials disclosed
- Intellectual property exposed

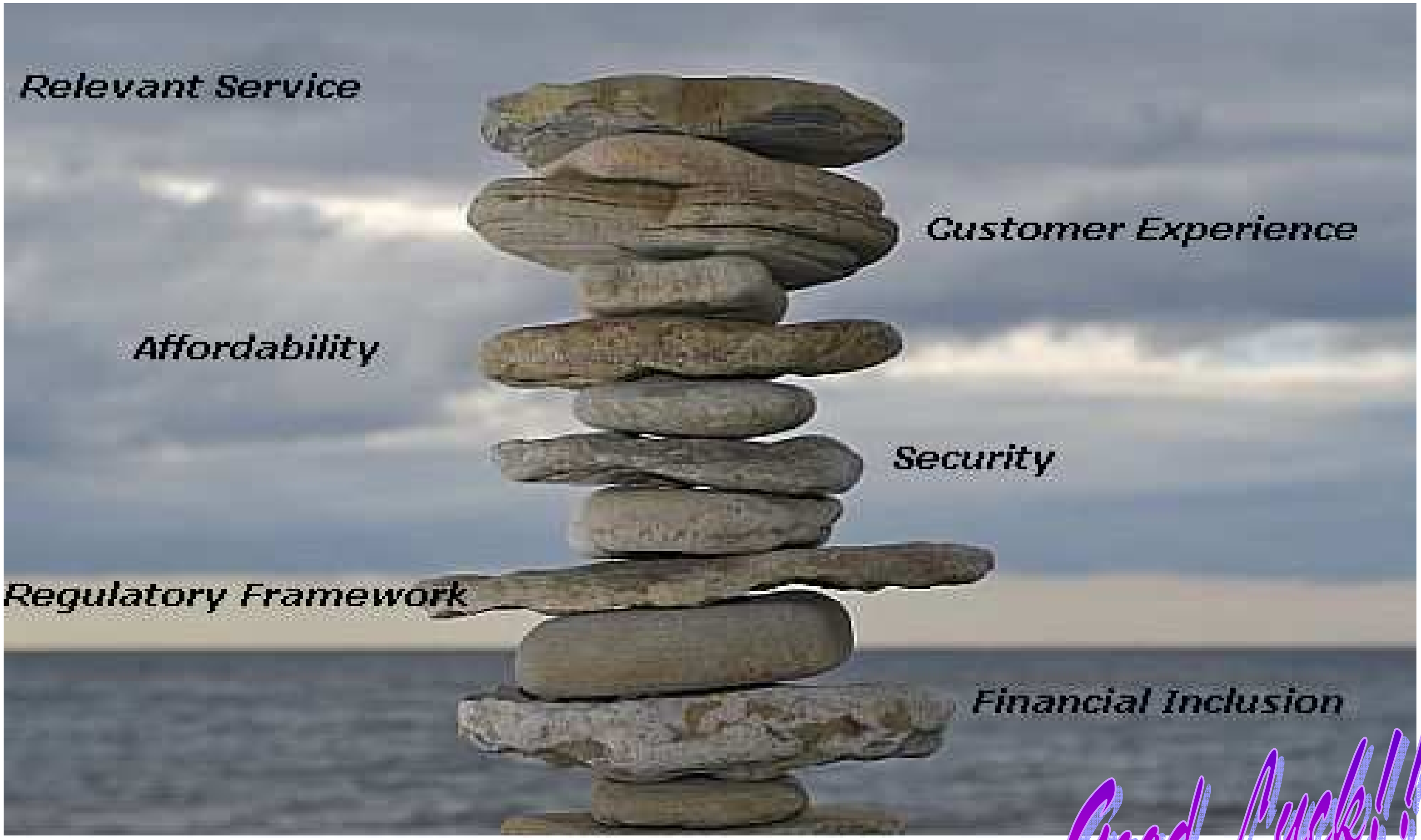
M10- Sensitive Information Disclosure
Prevention Tips

- Private API keys are called that for a reason…keep them off of the client
- Keep proprietary and sensitive business logic on the server
- Almost never a legitimate reason to hardcode a password (if there is, you have other problems)

Control#	Description
2.10	Do not store any passwords or secrets in the application binary

Conclusion

Mobile Money Service Provider Challenge: “Balance”



Good Luck!!!!

Thank you!!!

For more information please contact us:

Thabiso Moerane:
Mobile Commerce Ecosystem Leader
E-Mail: thabiso.moerane@alcatel-lucent.co.za
Tel: +27 (0) 12 648 3000
Cell: +27 (0) 83 960 6953
Fax: +27 (0) 86 502 1498
www.alcatel-lucent.com

AT
THE
SPEED
OF
IDEAS™