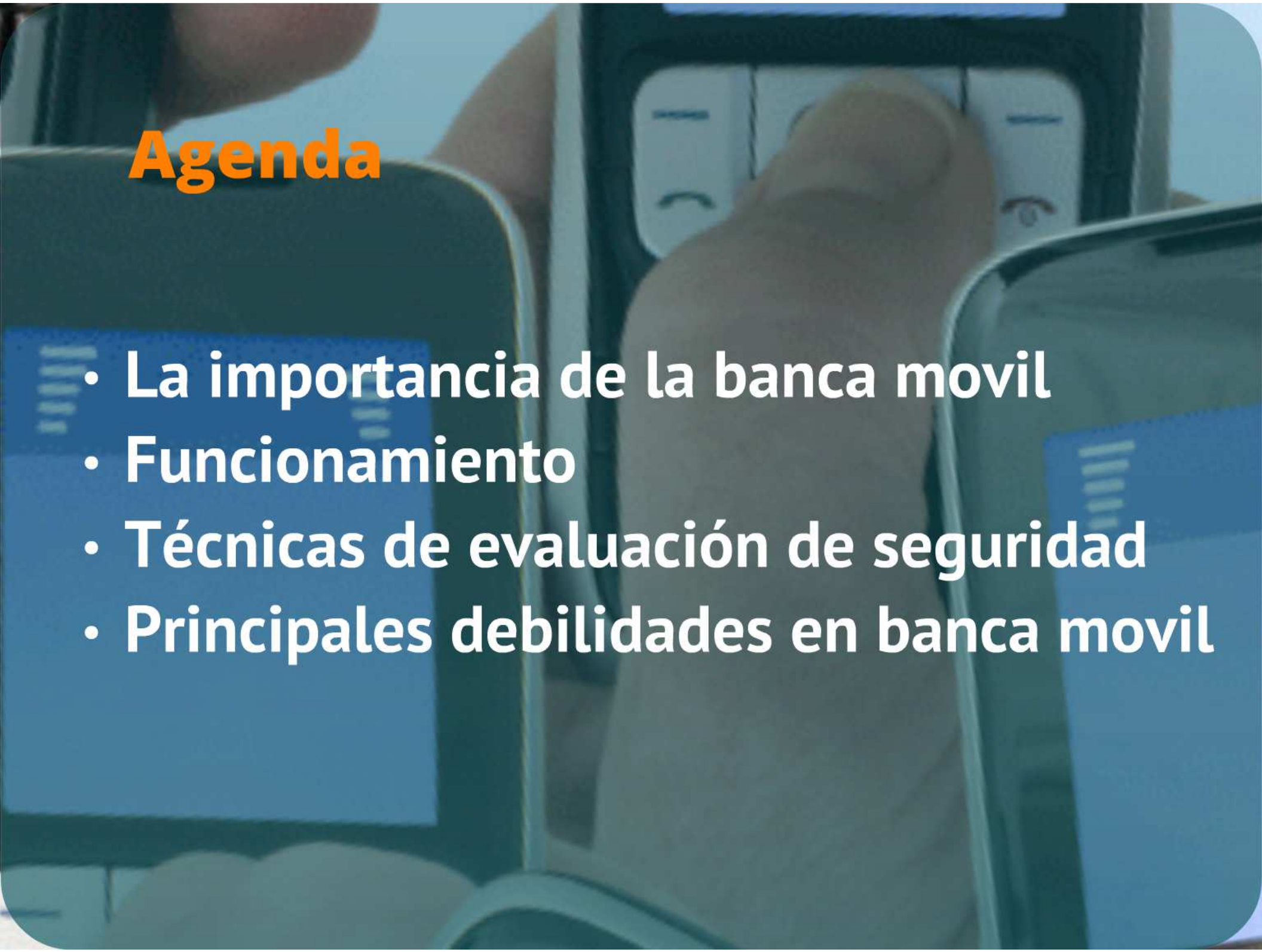
BANCA MOVIL:
Un analisis de seguridad

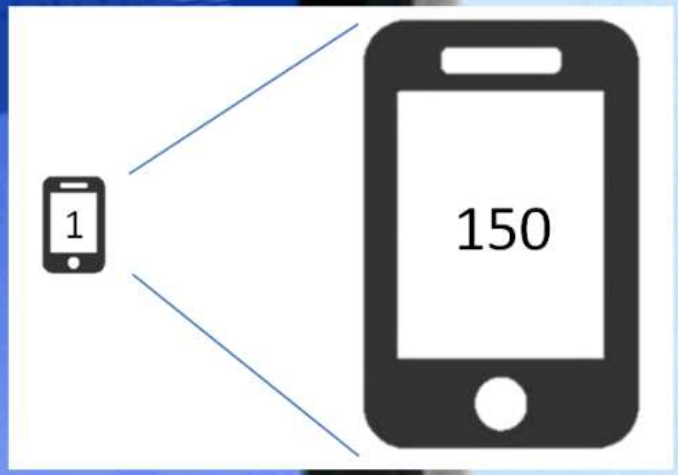
Nelson Boris Murillo Prieto

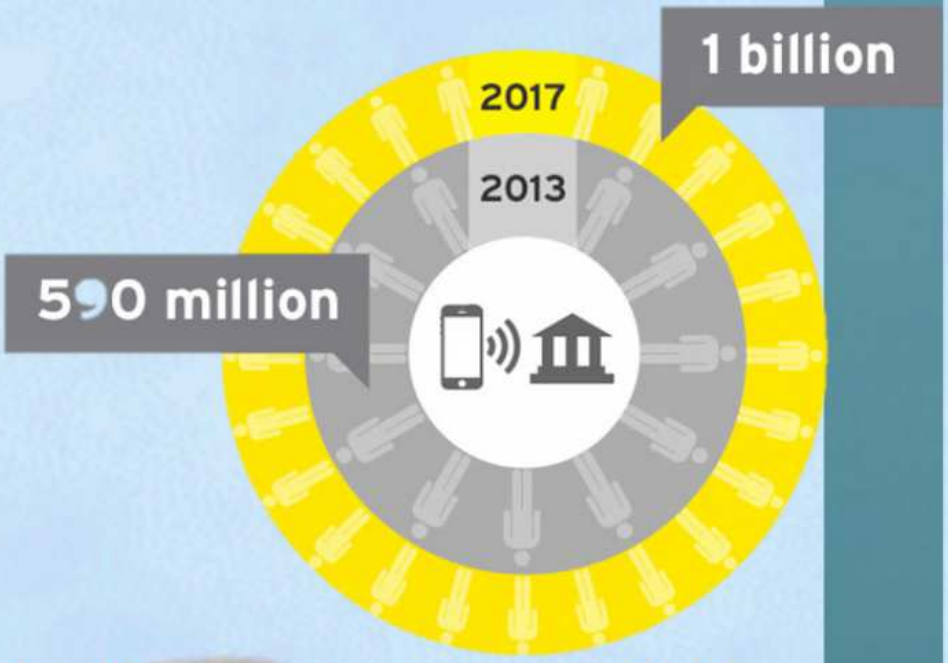


Agenda

- La importancia de la banca movil
- Funcionamiento
- Técnicas de evaluación de seguridad
- Principales debilidades en banca movil

En 2001 solo existía 1 método de pago móvil, hoy existen más de 150 solo en Estados Unidos

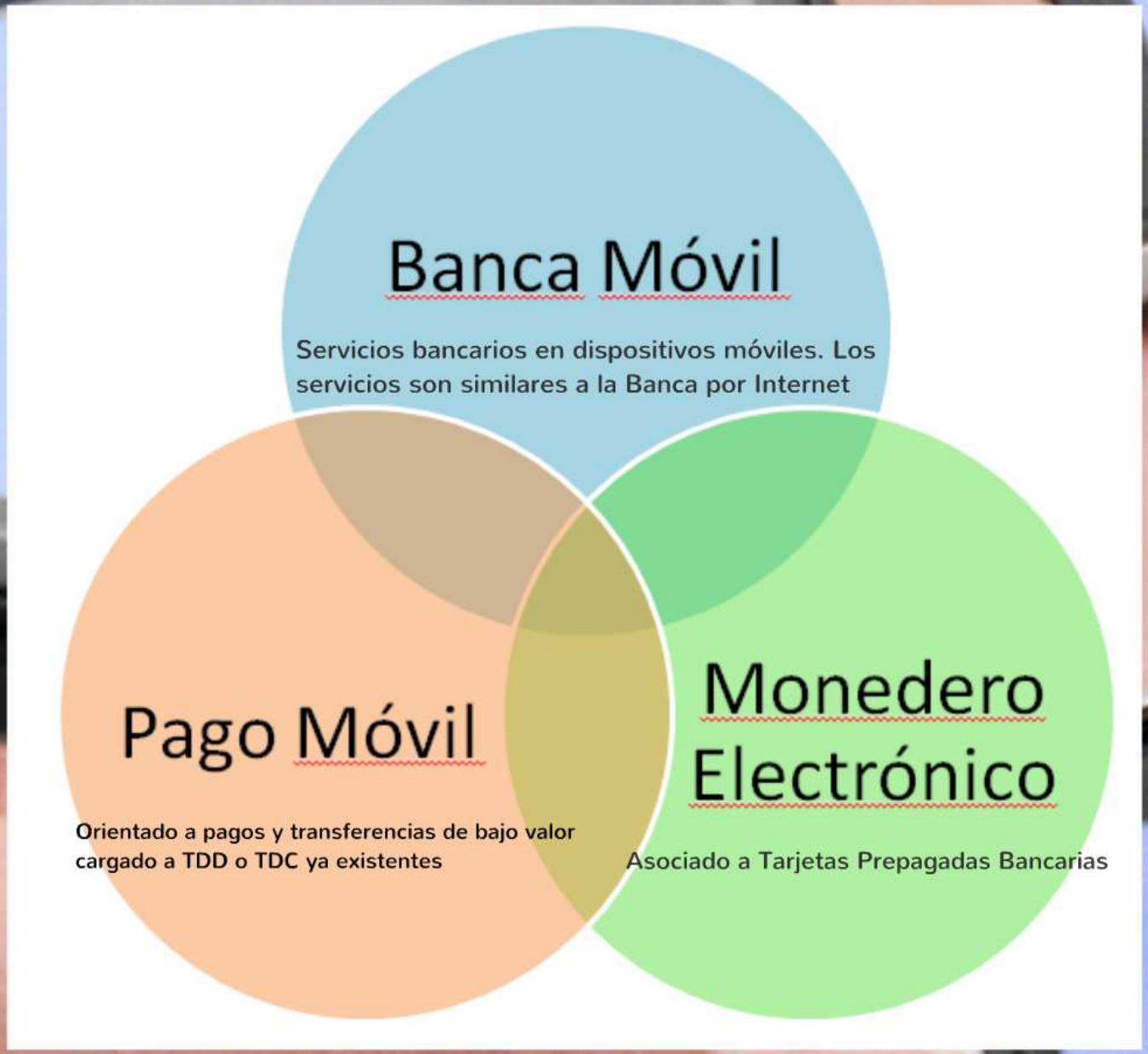




Crecimiento estimado de clientes de banca móvil


movil = barato
El costo de procesar una transacción desde un dispositivo móvil puede ser 50 veces menor a la banca tradicional

Mecanismos de transacciones moviles



Banca Móvil

Servicios bancarios en dispositivos móviles. Los servicios son similares a la Banca por Internet

Pago Móvil

Orientado a pagos y transferencias de bajo valor cargado a TDD o TDC ya existentes

Monedero Electrónico

Asociado a Tarjetas Prepagadas Bancarias

Bancos y consumidores en riesgo

La creciente complejidad en medios de pago, el lavado de dinero, el fraude y el riesgo de transferencias ilícitas crecen.

Los dueños de smartphones tuvieron un tercio más de posibilidades de ser víctimas de fraude y falsificación de identidad en el año pasado que los que no poseen smartphones

68% de los usuarios de smartphones que no utilizan aplicaciones financieras no las utilizan por miedo

Servidor

Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"

Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre

Herramientas/scripts
de análisis de servicios

Cliente

Herramientas para Pentest:
Decompilador

Comunicación

Observaciones comunes

- AAA insufici
- Manejo de
- SQL Injec
- Validaci
de par

MITM
metodos


String str1 = mUsername.getText().toString();
if (str1.length() == 0);
while (true)
iPhone
BlackBerry
symbian
Windows Phone

Servidor

Herramientas para Pentest:

Cercanas a la auditoria Web "tradicional"

Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre

BURPSUITE FREE EDITION

Herramientas/scripts de análisis de servicios

Webservice / Pagina Web

	A	B	C	D	E	F	G	H	I
1	07	45	77	85	23	23	24	23	24
2	94	78	83	68	75	75	44	75	44
3	75	09	93	16	16	16	51	16	51
4	63	40	65	39	39	39	92	39	92
5	20	75	13	38	38	38	58	38	58
6	85	54	38	45	45	45	76	45	76
7	74	51	77	86	86	86	07	86	07
8	18	42	85	61	61	61	54	61	54
9	76	96	98	03	03	03	12	03	12

Servidor

Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"

Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre

Cliente

Herramientas para Pentest:
Decompilador

Comunicación

Observaciones comunes

- AAA insufici
- Manejo de
- SQL Injec
- Validaci
de par

MITM
metodos

Cliente

Herramientas para Pentest:

Decompilador

Android -> Java

iOS -> Objetive C

```
private static final int ABOUT_ID = 101;
private static final int ERROR_DIALOG_ID = 2;
public static final String EXTRA_ADD_ACCOUNT = "add_account";
public static final String EXTRA_START_INTENT = "start_intent";
private static final boolean IS_TAG_DEBUG_LOGGABLE = false;
private static final int PROGRESS_LOGIN_DIALOG_ID = 1;
private static final String SAVE_ERROR_MESSAGE = "error_message";
private static final String TAG = "LoginActivity";
private boolean mAddAccountMode;
private AppSession mAppSession;
private AppSessionListener mAppSessionListener;
private String mErrorMessage;
private EditText mPassword;
private EditText mUsername;

private void login()
{
  String str1 = mUsername.getText().toString();
  if (str1.length() == 0);
  while (true)
```

ridad

Servidor

Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"

Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre

Cliente

Herramientas para Pentest:
Decompilador

Comunicación

Observaciones comunes

- AAA insuficientes
- Manejo de sesión
- SQL Injection
- Validación insuficie
de parámetros
- Errores a nivel
lógica de la ap

- MITM
- Uso de metodos
inseguros
- Uso de canal no cifrado
- Cifrado débil

miento de
del

Herramientas para Pentest:

Proxy/Web Proxy

Comunicación

eguridad

o


Servidor
Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"
Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre
BANK
BURPSUITE
Webservice / Pagina Web
Cliente
Herramientas para Pentest:
Decompilador
Android -> Java
iOS -> Objetive C
iPhone
symbian
Herramientas para Pentest:
Proxy/Web Proxy
BURPSUITE
Comunicación
Observaciones comunes
• Almacenamiento de datos sensibles del
• MITM
• Uso de metodos inseguros
• Uso de canal no cifrado
• Uso de cifrado débil
• ...Heartbleed
• AAA insuficientes
• Manejo de sesión
• SQL Injection
• Validación insuficiente de parámetros
• Errores a nivel de lógica de la aplicación

Servidor

Herramientas para Pentest:

Cercanas a la auditoria Web "tradicional"

o

re

Herramientas/scripts de análisis de servicios


Cliente
Herramientas para Pentest:
Decompilador
Android -> Java
iOS -> Objetive C
Herramientas para Pentest:
Proxy/Web Proxy
Comunicación
Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre
Webservice / Pagina Web
Servidor
Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"
BANK
Herramientas/scripts
de análisis de servicios
Observaciones comunes
• Almacenamiento de datos sensibles del cliente
• Visualización de información sensible de la aplicación en el código
• Malware
• MITM
• Uso de metodos inseguros
• Uso de canal no cifrado
• Uso de cifrado débil
• ...Heartbleed
• AAA insuficientes
• Manejo de sesión
• SQL Injection
• Validación insuficiente de parámetros
• Errores a nivel de lógica de la aplicación

INSERT DEMO HERE

- Adquisición de los instaladores
- Backup de las aplicaciones
- Copia a maquina
- Decompilación
- Ingeniería inversa


Cliente
Herramientas para Pentest:
Decompilador
Android -> Java
iOS -> Objetive C
Herramientas para Pentest:
Proxy/Web Proxy
Comunicación
Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre
Webservice / Pagina Web
Servidor
Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"
BANK
Herramientas y scripts de análisis de servicios
Observaciones comunes
• Almacenamiento de datos sensibles del cliente
• Visualización de información sensible de la aplicación en el código
• Malware
• MITM
• Uso de metodos inseguros
• Uso de canal no cifrado
• Uso de cifrado débil
• ...Heartbleed
• AAA insuficientes
• Manejo de sesión
• SQL Injection
• Validación insuficiente de parámetros
• Errores a nivel de lógica de la aplicación

INSERT DEMO HERE

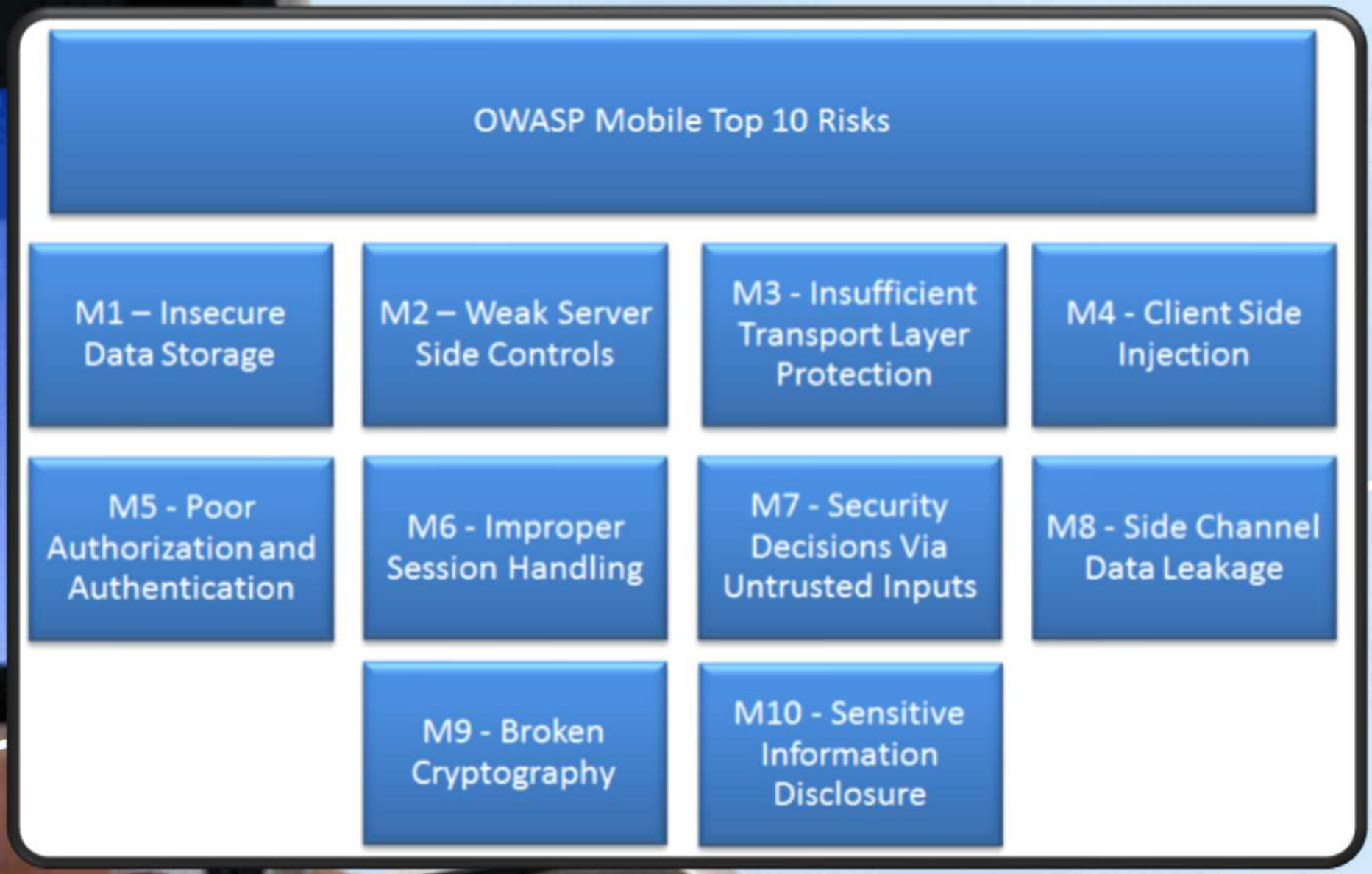
- Utilización de proxy
- Carga de certificado
- Navegación


Cliente
Herramientas para Pentest:
Decompilador
Android -> Java
iOS -> Objetive C
iPhone
BlackBerry
symbian
Windows Phone
Herramientas para Pentest:
Proxy/Web Proxy
BURP SUITE
FREE EDITION
Comunicación
Verificación de estado
Transferencias
Pago de servicios
Pago de tarjetas de cre
Webservice / Pagina Web
Servidor
Herramientas para Pentest:
Cercanas a la auditoria Web "tradicional"
BANK
BURP SUITE
FREE EDITION
Herramientas/scripts
de análisis de servicios
Observaciones comunes
• Almacenamiento de datos sensibles del cliente
• Visualización de información sensible de la aplicación en el código
• Malware
INSERT DEMO HERE
• MITM
• Uso de metodos inseguros
• Uso de canal no cifrado
• Uso de cifrado débil
• ...Heartbleed
INSERT DEMO HERE
• AAA insuficientes
• Manejo de sesión
• SQL Injection
• Validación insuficiente de parámetros
• Errores a nivel de lógica de la aplicación
INSERT DEMO HERE

INSERT DEMO HERE

- Configuración del servicio
- Test de autenticación
- Fuzzing de parámetros
- Lógica de aplicación

OWASP

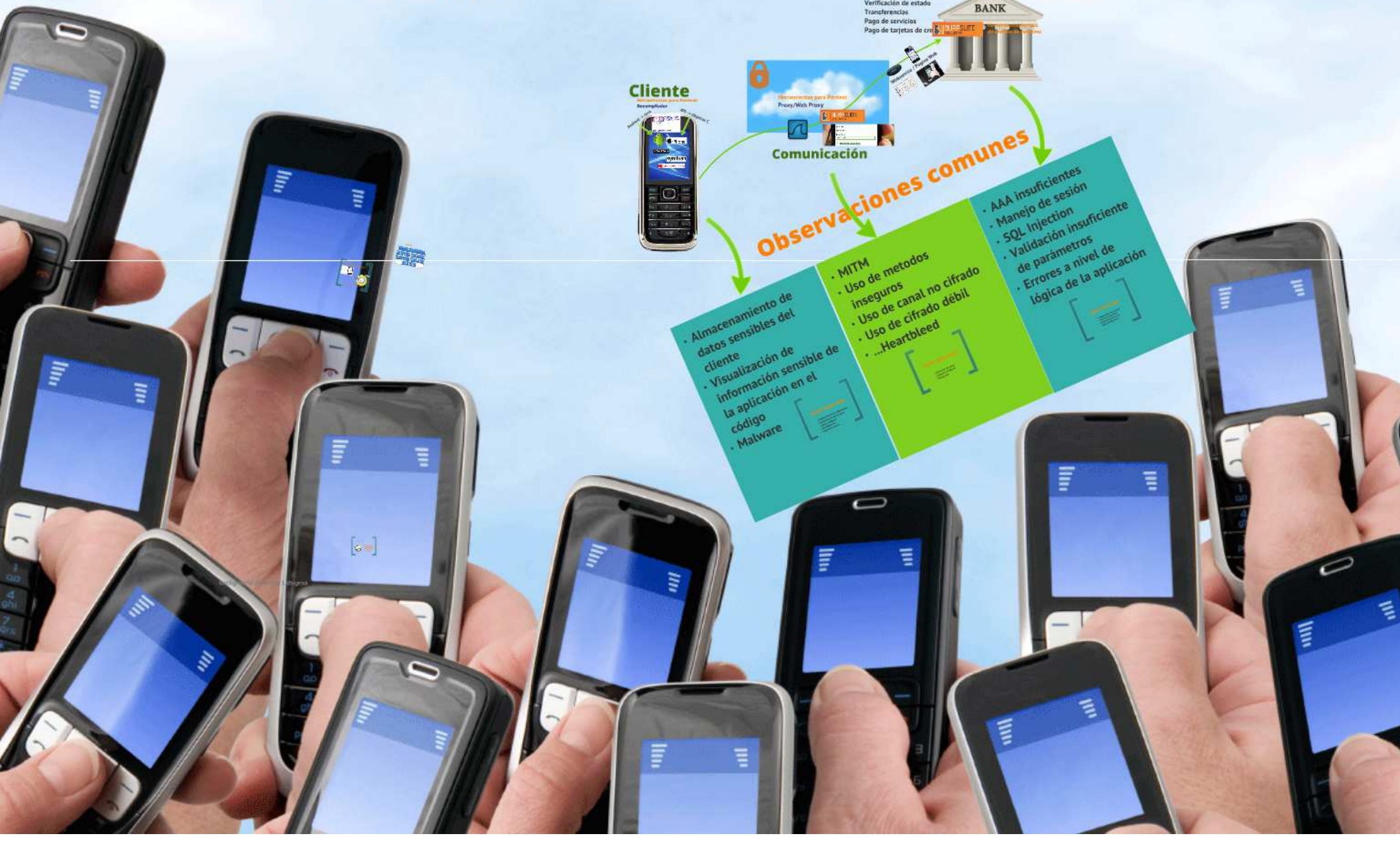

OWASP Mobile Top 10 Risks
M1 – Insecure Data Storage
M2 – Weak Server Side Controls
M3 - Insufficient Transport Layer Protection
M4 - Client Side Injection
M5 - Poor Authorization and Authentication
M6 - Improper Session Handling
M7 - Security Decisions Via Untrusted Inputs
M8 - Side Channel Data Leakage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

Conclusiones

- **El uso de la banca movil tiene un crecimiento exponencial**
- **Se requieren medidas de seguridad que permitan confiar en la aplicación (banco y cliente)**
- **Existe bastante oportunidad de mejora en las aplicaciones móviles**
- **Los controles adicionales “tradicionales” (ej. token) permiten disminuír el impacto de las vulnerabilidades demostradas.**
- **Estamos realmente seguros?**

BANCA MOVIL:
Un analisis de seguridad

Nelson Boris Murillo Prieto



alwa