Desarrollo seguro de Aplicaciones Web basado en OWASP

Por: Carlos Carreño,

OCP, ScrumMaster, Solution Architect

Email: ccarrenovi@Gmail.com

Unidad 8 Mobile Security

- La Dimension de la Problematica
- OWASP Top 10 Mobile.

Autor: ccarrenovi@Gmail.com

La Dimension de la Problematica

570 millones: Usuarios de móviles

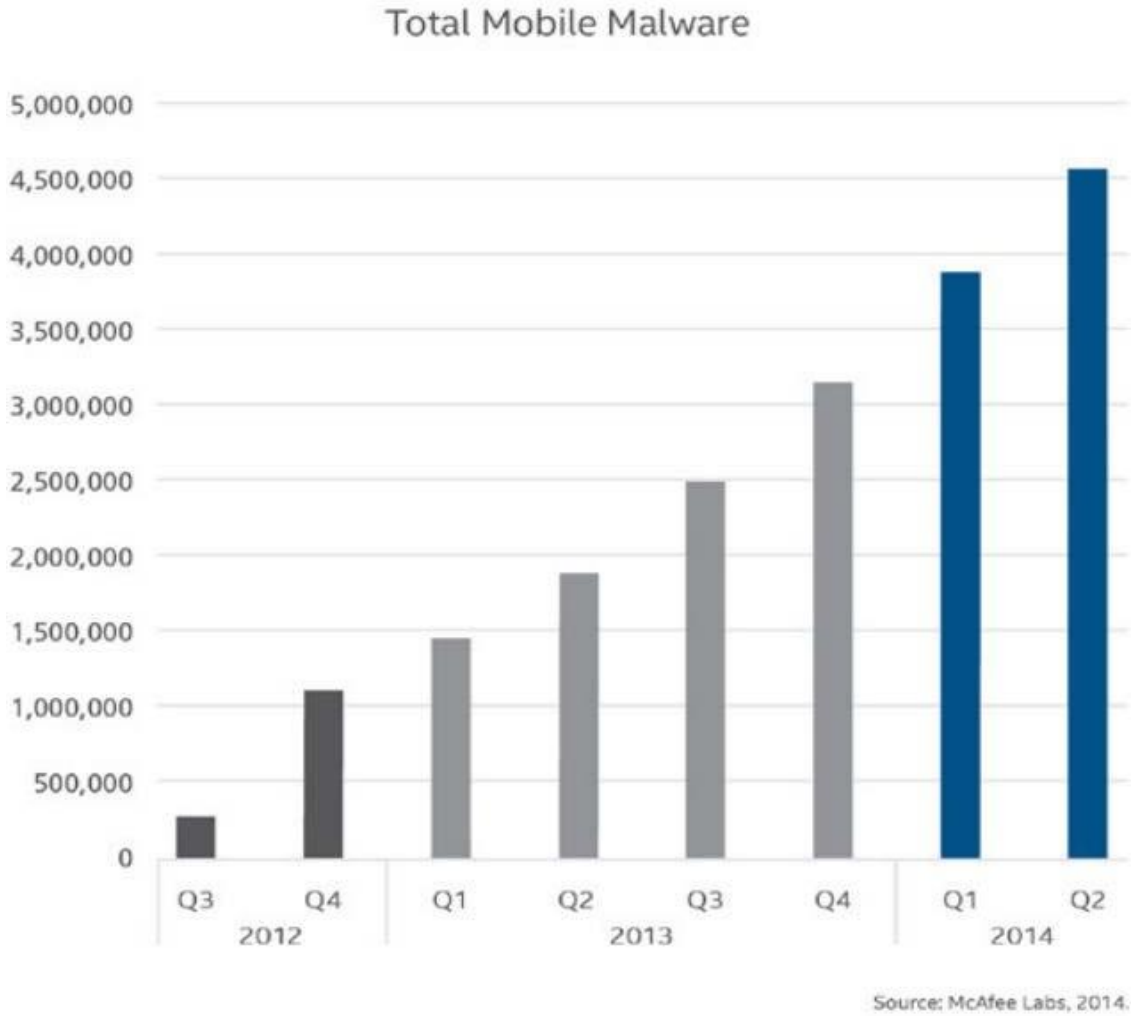
366 millones: Acceso a un baño

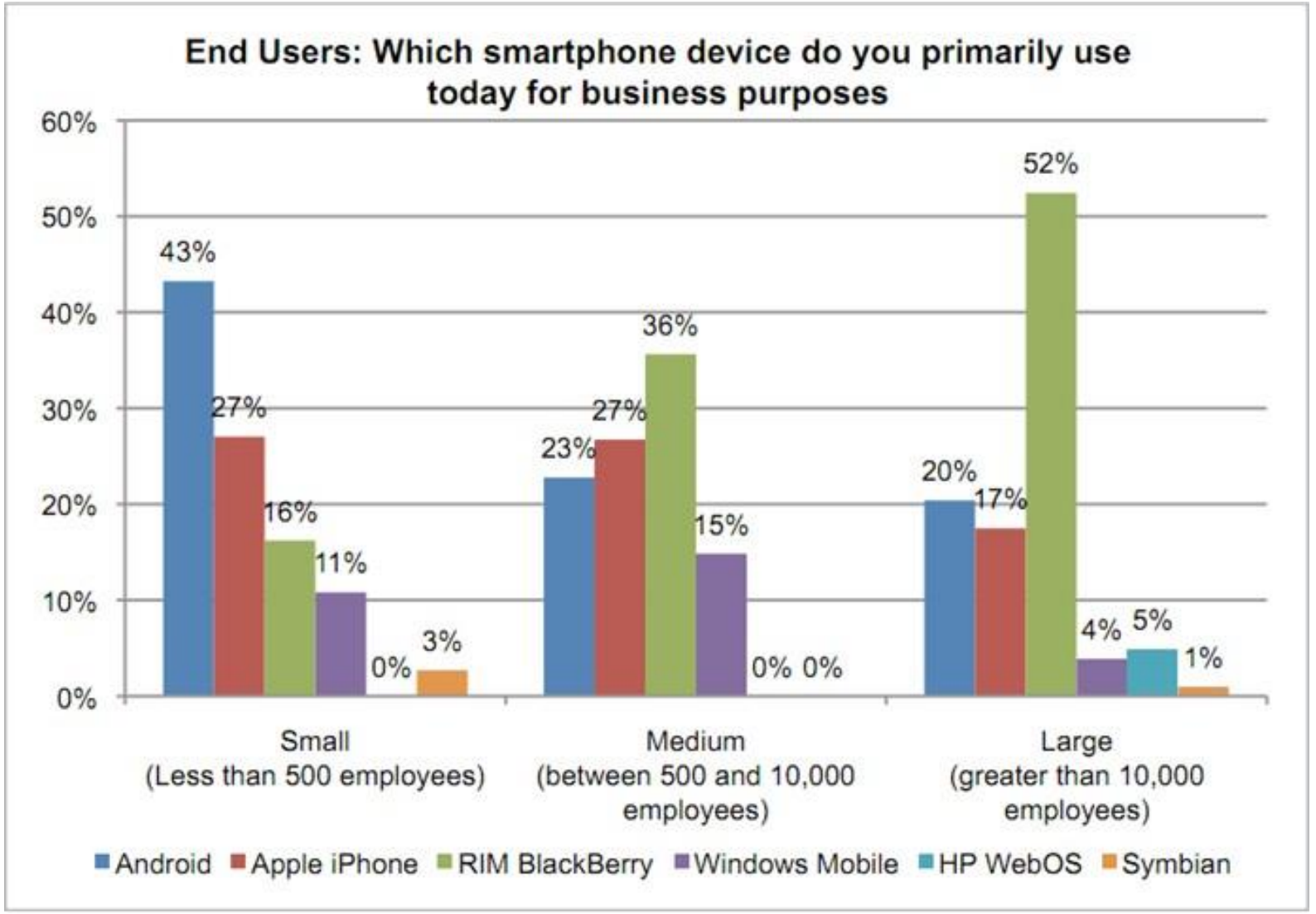
2000 millones: Descargas de Angry Birds

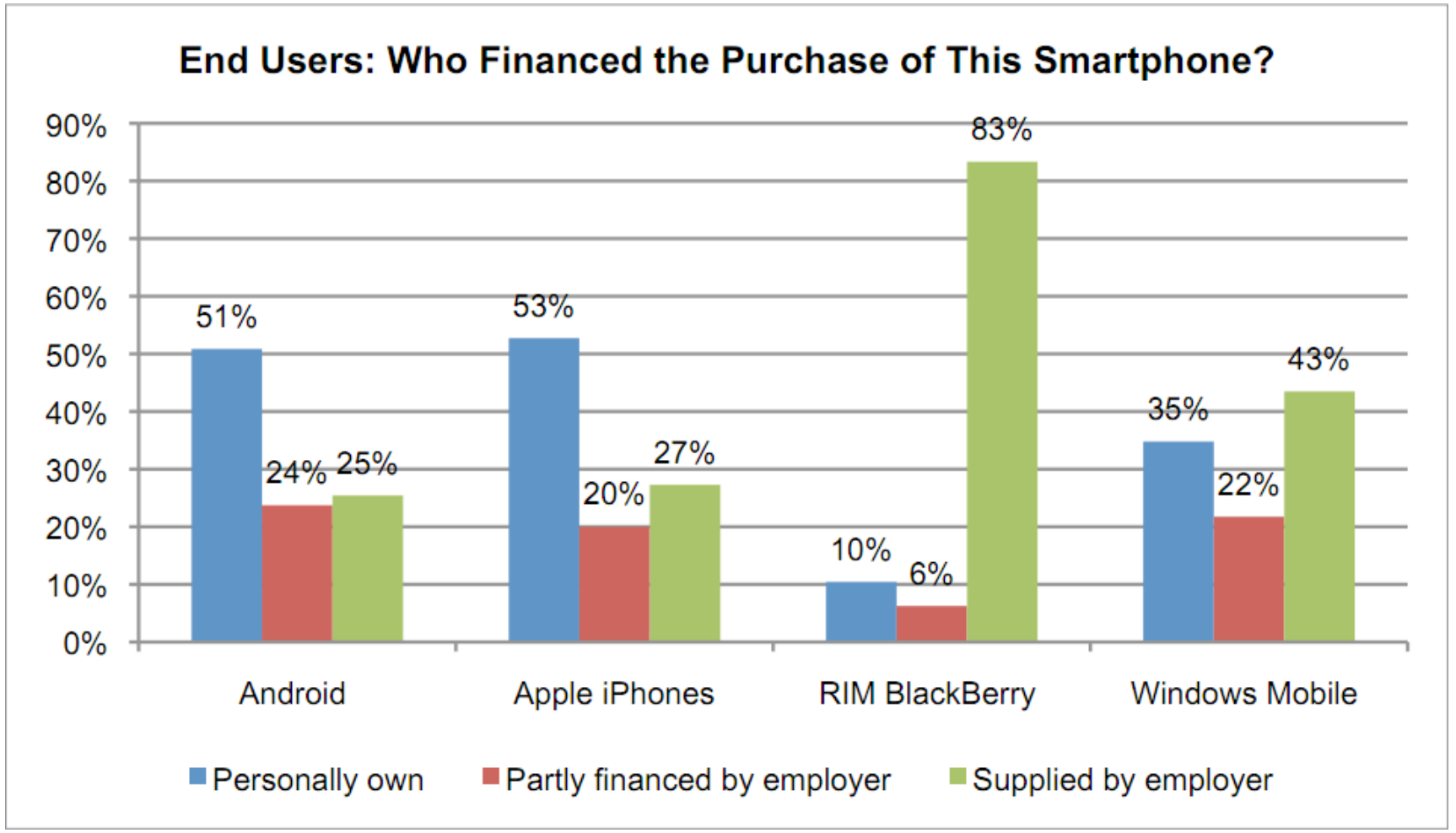
Tráfico de internet móvil > PC

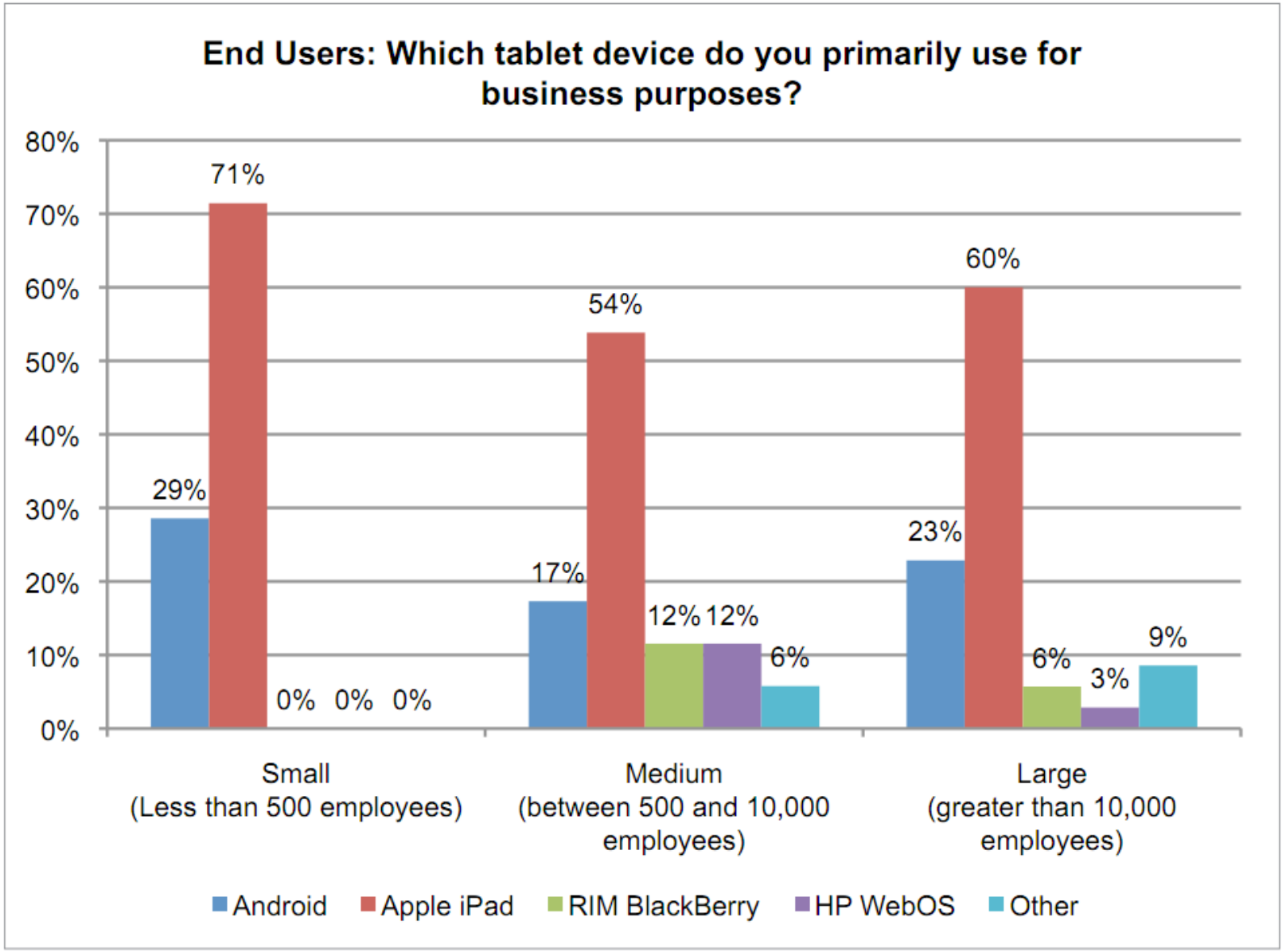
+2 Billones de dispositivos conectados,

En el 2020 habrá más de 60 Billones

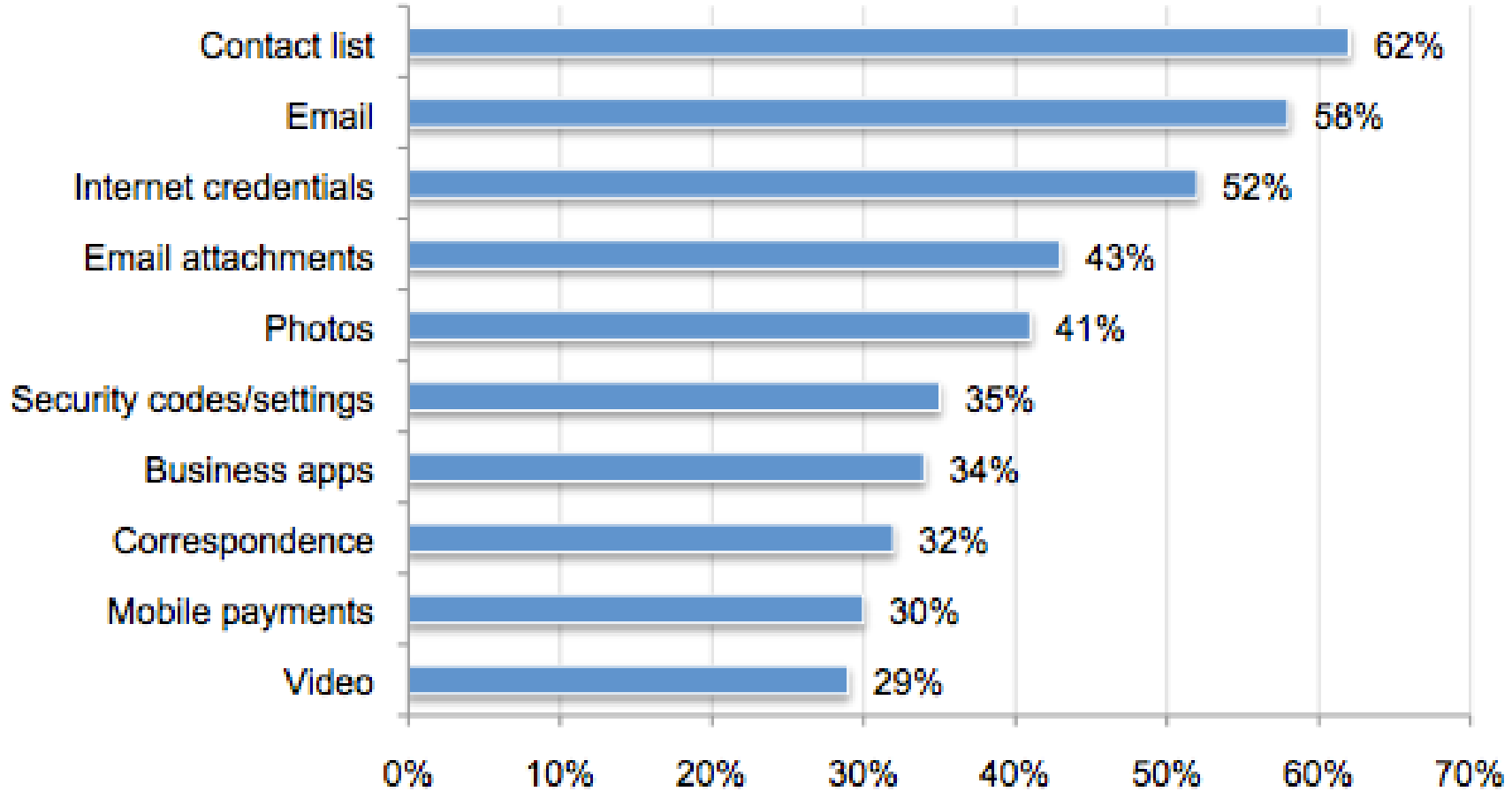

Total Mobile Malware
5,000,000
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Q3
Q4
Q1
Q2
Q3
Q4
Q1
Q2
2012
2013
2014
Source: McAfee Labs, 2014.


End Users: Which smartphone device do you primarily use today for business purposes
60%
50%
40%
30%
20%
10%
0%
43%
27%
16%
11%
0%
3%
23%
27%
36%
15%
0%
0%
20%
17%
52%
4%
5%
1%
Small (Less than 500 employees)
Medium (between 500 and 10,000 employees)
Large (greater than 10,000 employees)
Android
Apple iPhone
RIM BlackBerry
Windows Mobile
HP WebOS
Symbian


End Users: Who Financed the Purchase of This Smartphone?
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
51%
24%
25%
53%
20%
27%
10%
6%
83%
35%
22%
43%
Android
Apple iPhones
RIM BlackBerry
Windows Mobile
Personally own
Partly financed by employer
Supplied by employer


End Users: Which tablet device do you primarily use for business purposes?
80%
70%
60%
50%
40%
30%
20%
10%
0%
71%
29%
0% 0% 0%
54%
17%
12% 12%
6%
60%
23%
6%
3%
9%
Small (Less than 500 employees)
Medium (between 500 and 10,000 employees)
Large (greater than 10,000 employees)
Android
Apple iPad
RIM BlackBerry
HP WebOS
Other

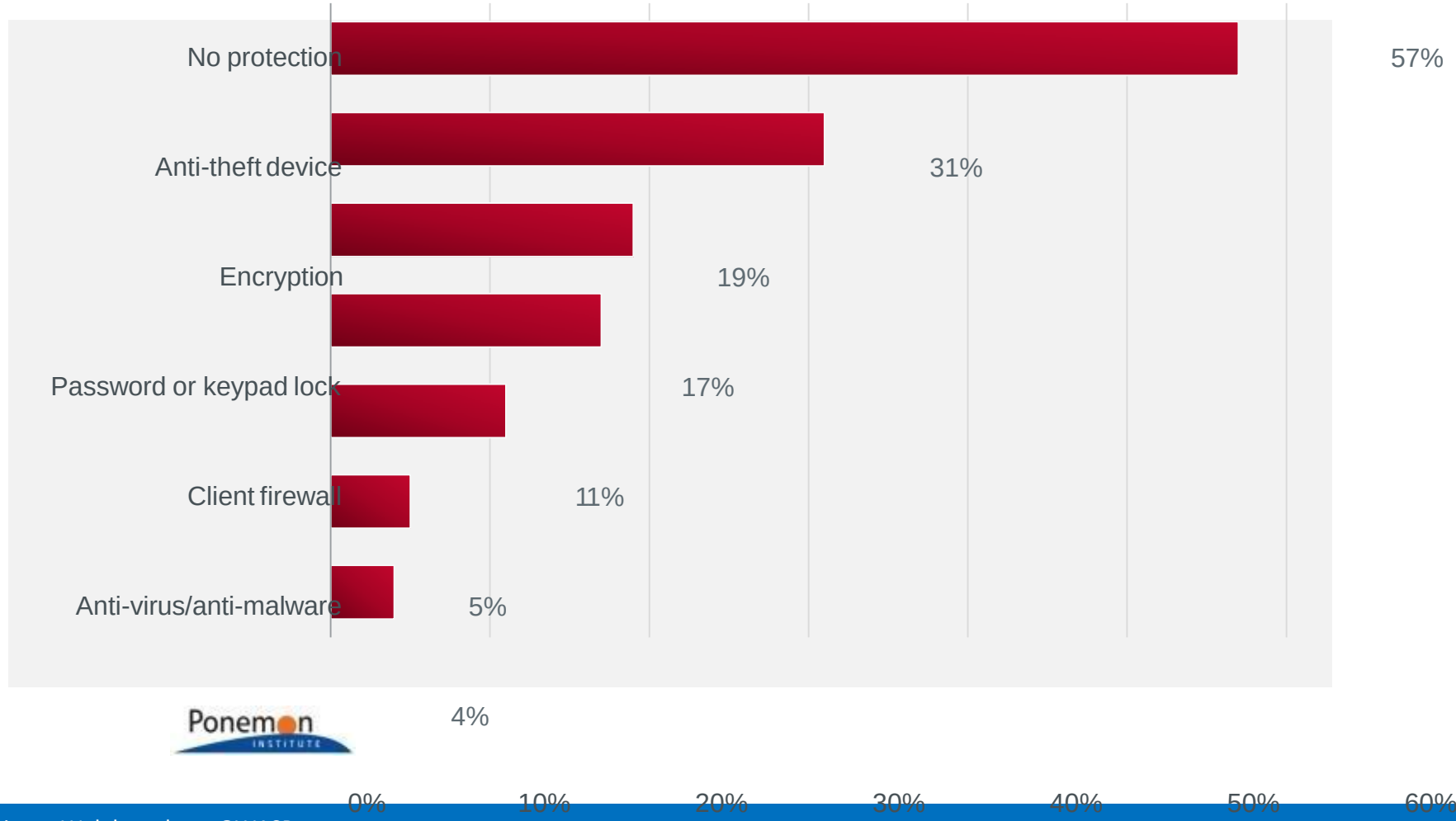
Bar Chart 8. What business information is at risk because of smartphone loss?



	PC	Móvil	Similitud
AMENAZAS	• Malware, Virus, Phishing, Stolen Data, Trojans, DoS, Social Engineering	• Similar al PC + • Pérdida de dispositivo, eavesdropping, fraude SMS	= +
VECTORES	• Browser, Bluetooth, Wi-Fi, Cellular Network, Cross Channel, Email	• Similar al PC + • SMS, MMS, App downloads	= +
ENTORNO	• Homogenous OS environment • Largely local computing centric	• Fragmented OS environment • Cloud-centric, tethered to OS provider	≠

Los desafíos en los ambientes móviles motivan a un cambio en el enfoque

Protección en dispositivos perdidos



Autor: ccarrenovi@Gmail.com

La mobilidad trae nuevos riesgos

Web 2.0, Apps 2.0, Mobility 2.0…Enterprise 2.0

60,000 Nuevas piezas de Malware/día

Zeus Malware apunta a mobile phones via SMS

Costo de la información de un laptop: $25-50K

80% de los usuarios concientes de la pérdida de Información

OWASP top 10 Mobile

- M1 – USO INADECUADO DE LA PLATAFORMA
- M2 – ALMACENAMIENTO DE DATOS INSEGUROS
- M3 – COMUNICACIÓN INSEGURA
- M4 – AUTENTICACIÓN INSEGURA
- M5 – CRIPTOGRAFÍA INSUFICIENTE
- M6 – AUTORIZACIÓN INSEGURA
- M7 – CALIDAD DEL CÓDIGO EN EL LADO DEL CLIENTE
- M8 – ADULTERACIÓN DEL CÓDIGO
- M9 – INGENIERIA INVERSA
- M10 – FUNCIONALIDAD EXTRAÑA

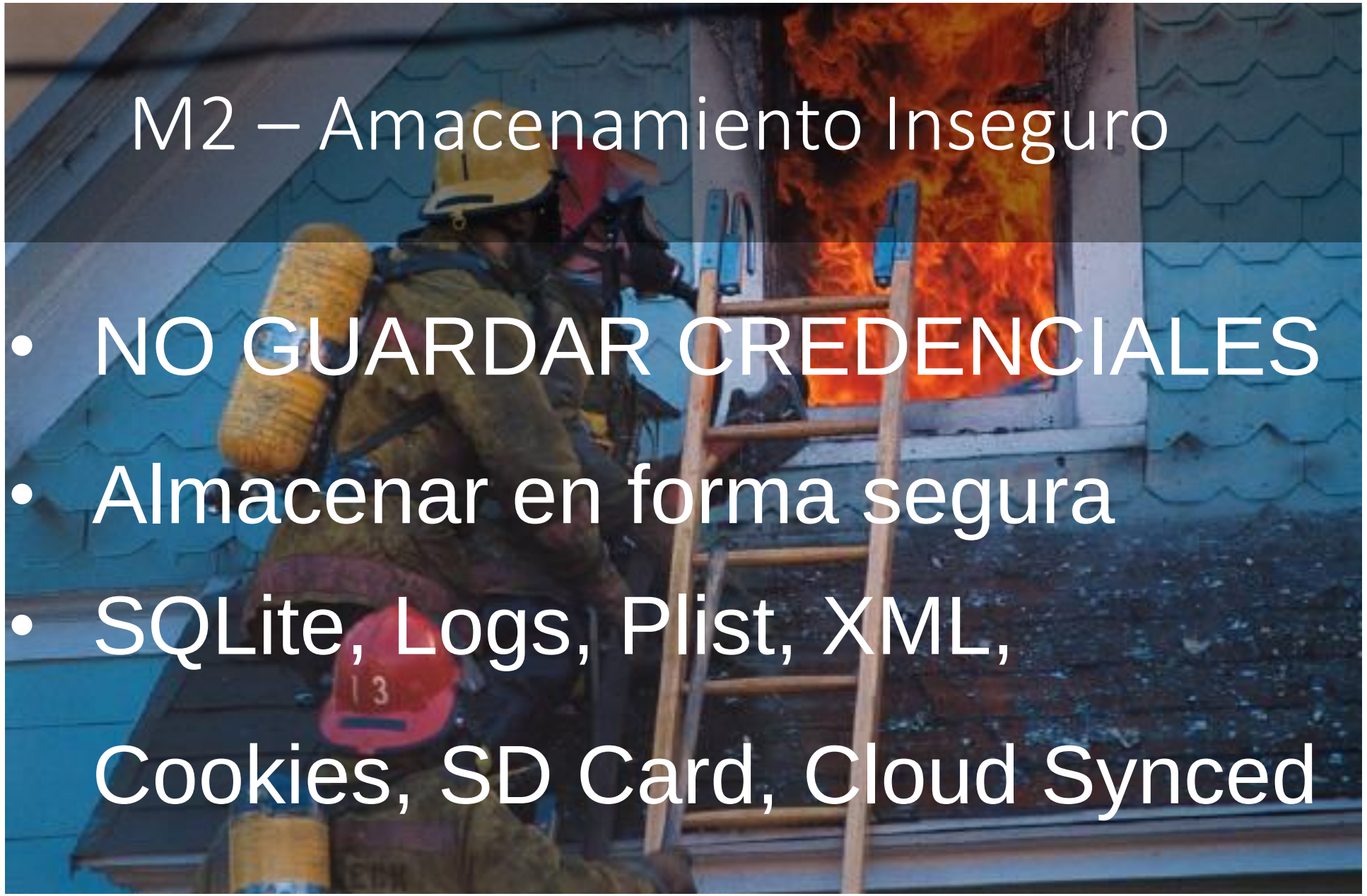
Autor: ccarrenovi@Gmail.com

M1 – Controles Débiles en el Servidor

- Riesgos del OWASP TOP 10
- SQL Injection, CSRF, etc
- Prácticas de Desarrollo de Software Inseguro

Autor: ccarrenovi@Gmail.com

M2 – Amacenamiento Inseguro



- NO GUARDAR CREDENCIALES
- Almacenar en forma segura
- SQLite, Logs, Plist, XML, Cookies, SD Card, Cloud Synced

M3 – Transmisión insegura

- Aplicar SSL/TLS
- Utilizar algoritmos seguros
- Certificados confiables
- Alertar al usuario

M4 – Fuga de Información no intencional

- Modelado de amenazas de OS, platfoms & frameworks
- Cache de datos, logs, cookies
- Desconocidos para el Developer

M5 – Autorización y Autenticación

- No autenticar solo a nivel local
- Cifrar datos locales
- Rember-me
- 4-digit PIN

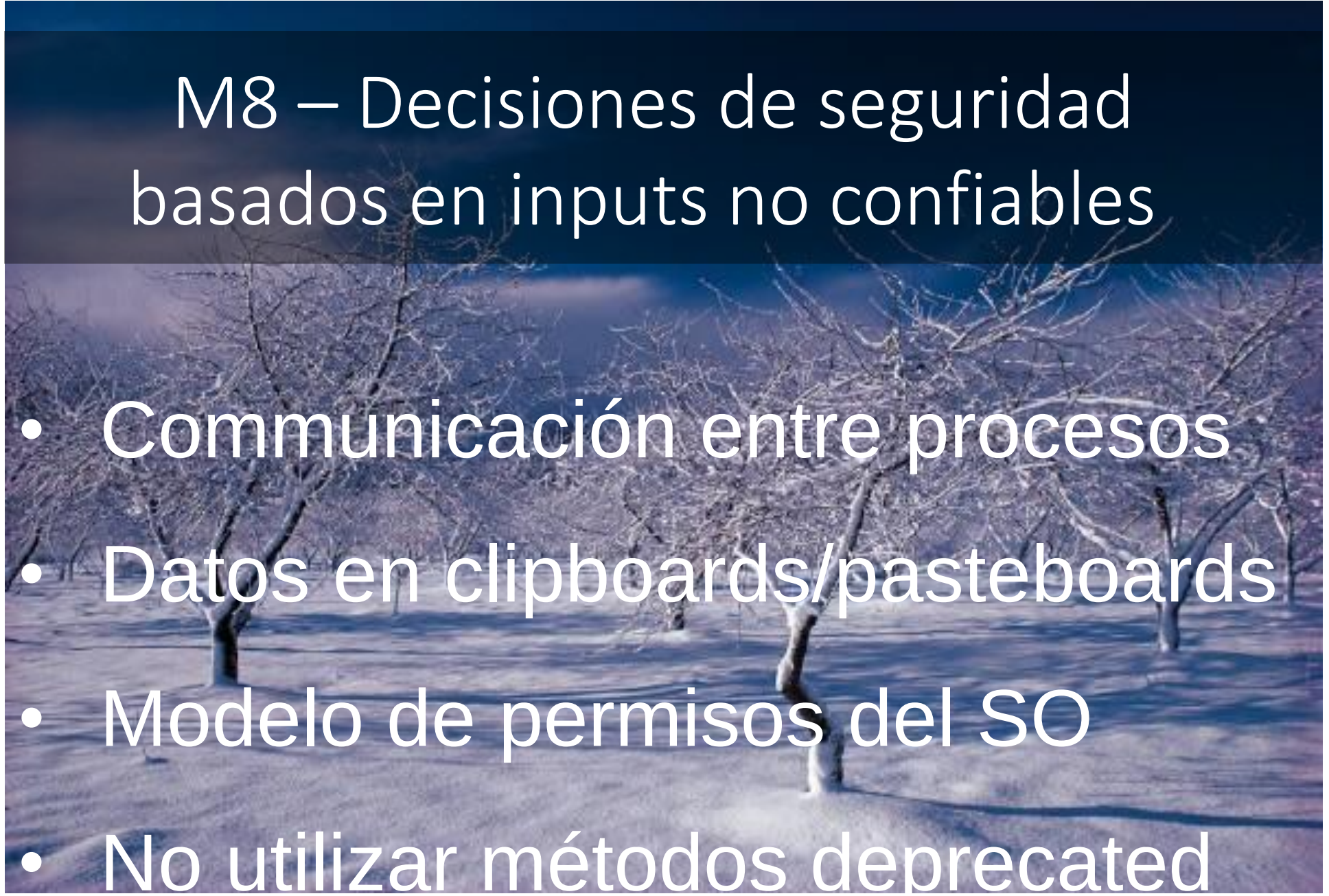
M6 – Criptografía Insegura

- Procesos de Cifrado/Descifrado
- Algorítmos débiles
- Key Management

M7 – Inyección del lado del Cliente

- SQLite Injection
- Sniffing (intent) en Android
- Inyección de Javascript
- Local File Inlclusion (NFSFile, Webviews)

M8 – Decisiones de seguridad basados en inputs no confiables



- Communicación entre procesos
- Datos en clipboards/pasteboards
- Modelo de permisos del SO
- No utilizar métodos deprecated

M9 – Manejo de Sesiones

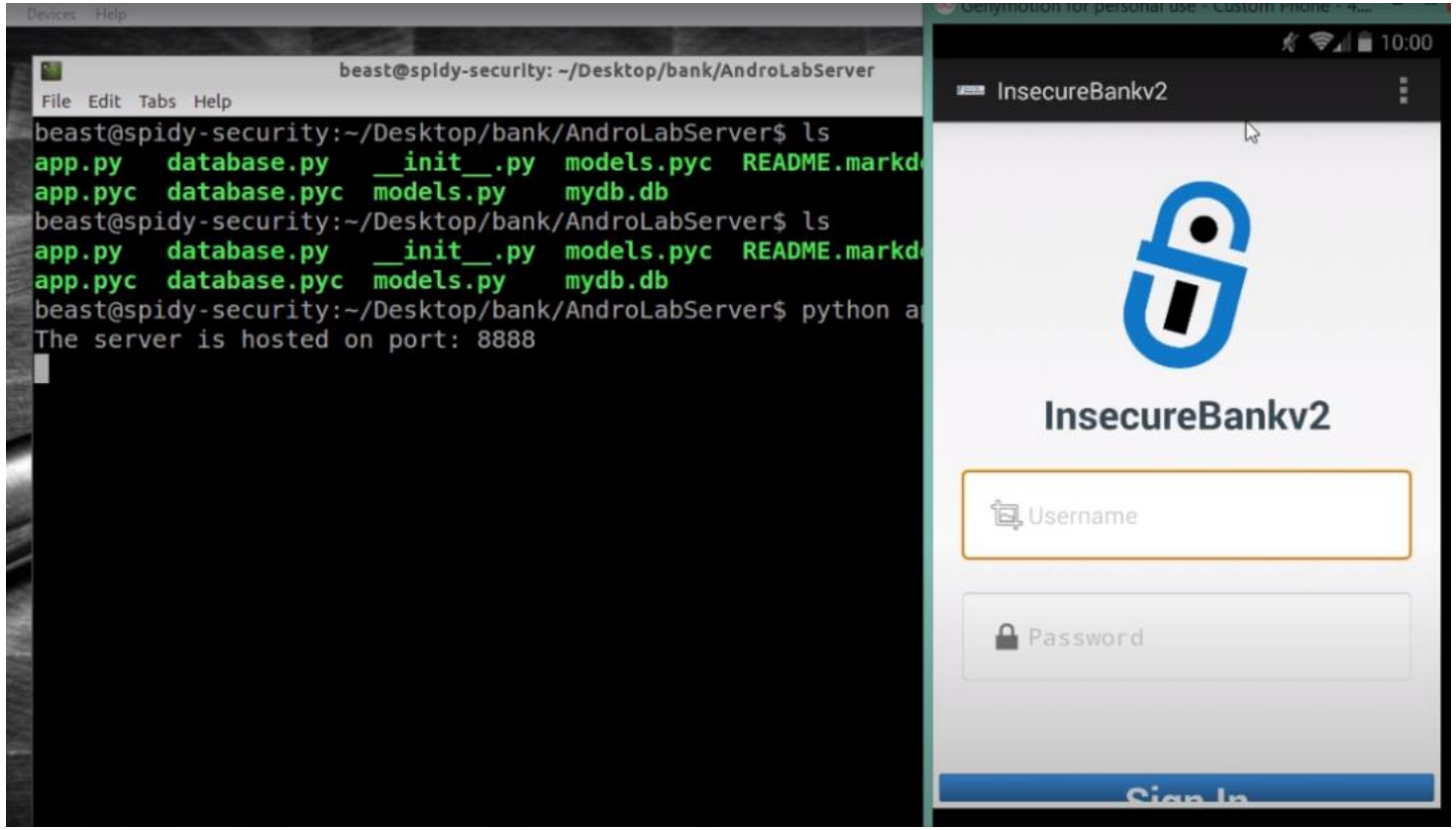
- Sesión del lado del cliente
- Timeout de sesiones inadecuado
- Sesión basada en cookies
- Creación insegura de tokens

M10 – Protección de Binarios

- Prevenir Reversing
- Monitorear Integridad de la App
- Detectar Jailbreak / Rooted

Laboratorio

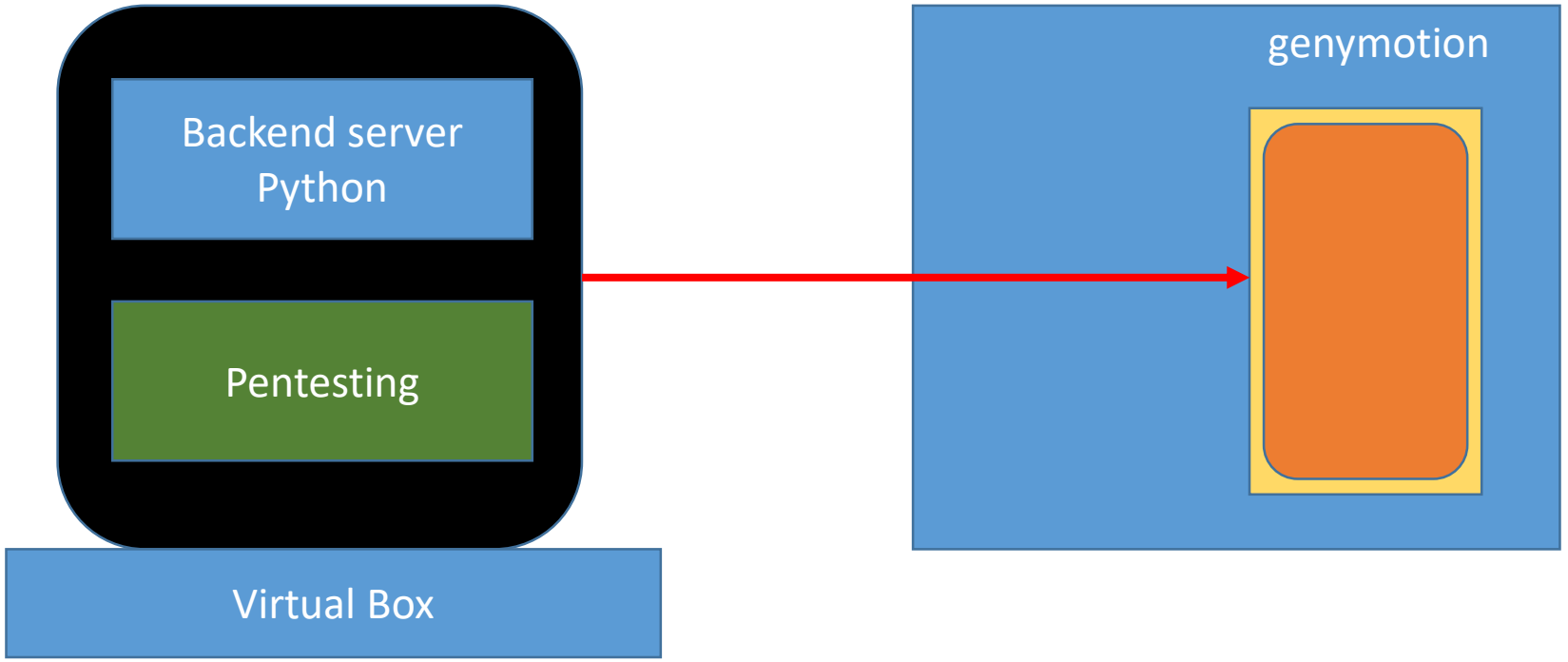
- Lab Pentesting con Android-InsecureBankv2



Autor: ccarrenovi@Gmail.com

Escenario Mobile Pentesting

Ubuntu 18.04 desktop o superior/Kali



Windows

Autor: ccarrenovi@Gmail.com