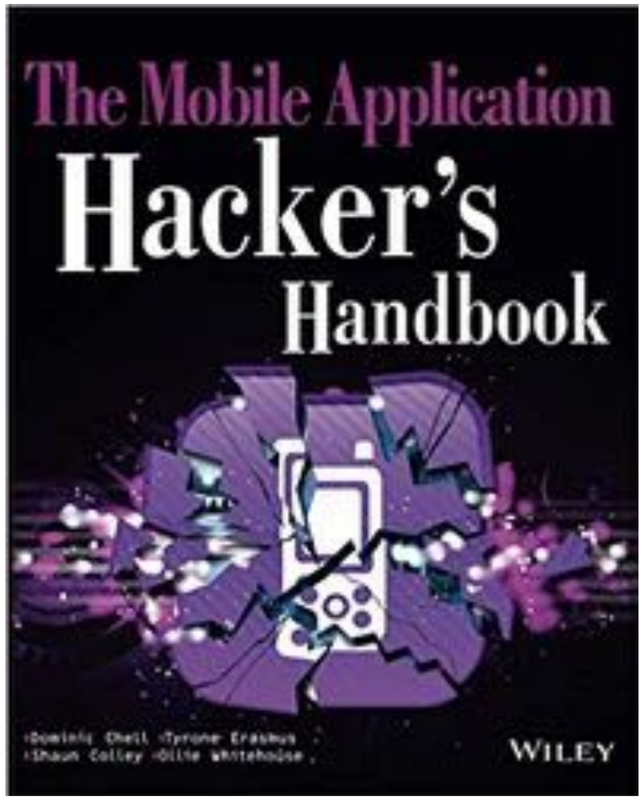
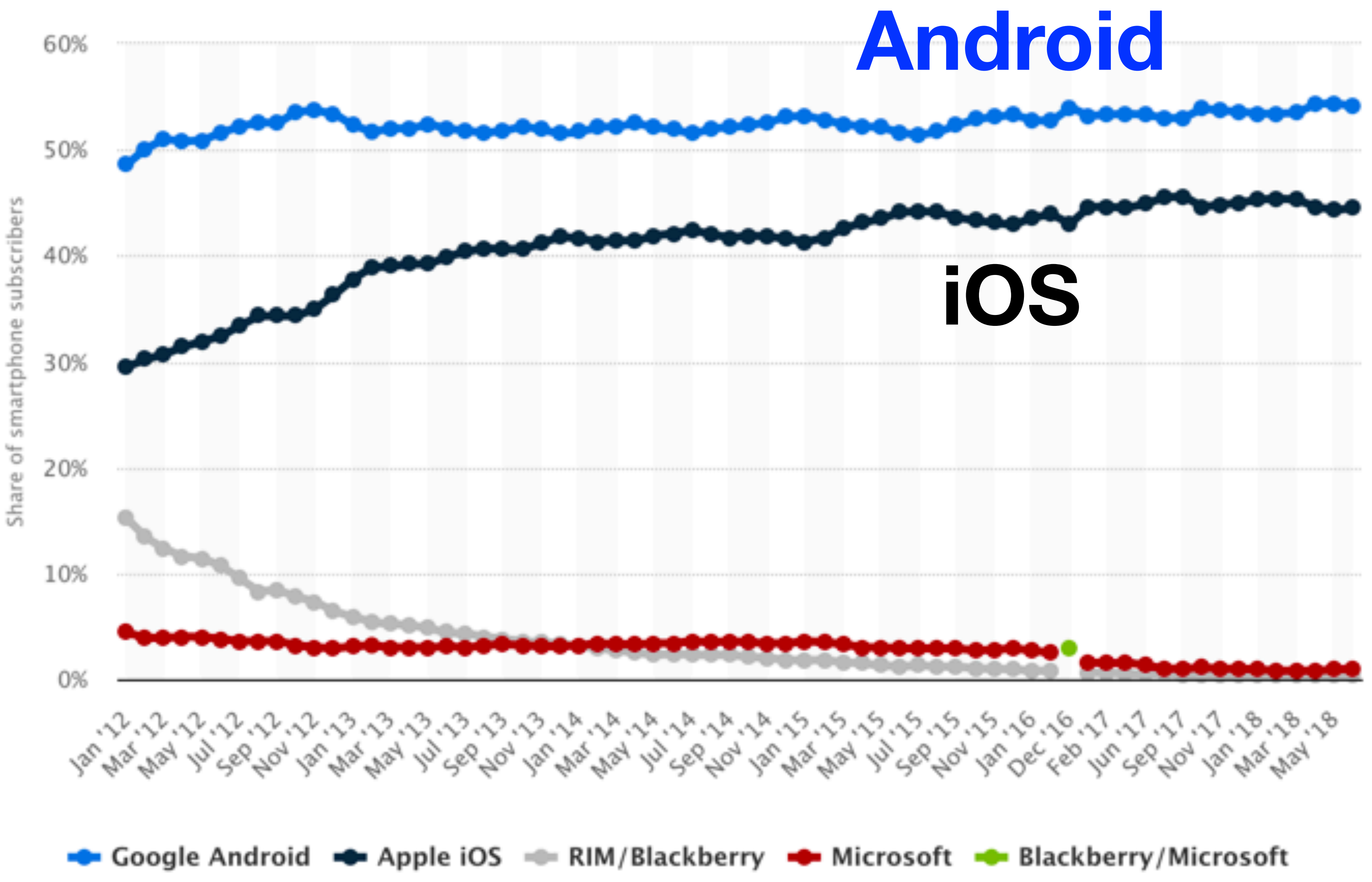
CNIT 128
Hacking Mobile Devices



1. Mobile Application (In)security

Mobile OS Market Share



- Link Ch 1a

Attack Surface

- Network communications
    - Often public Wi-Fi
- Device theft
    - Locally stored data
- Malicious apps on the phone
    - Often from Google Play
- Other input sources
    - NFC, Bluetooth, camera, microphonw, SMS, USB, QR codes

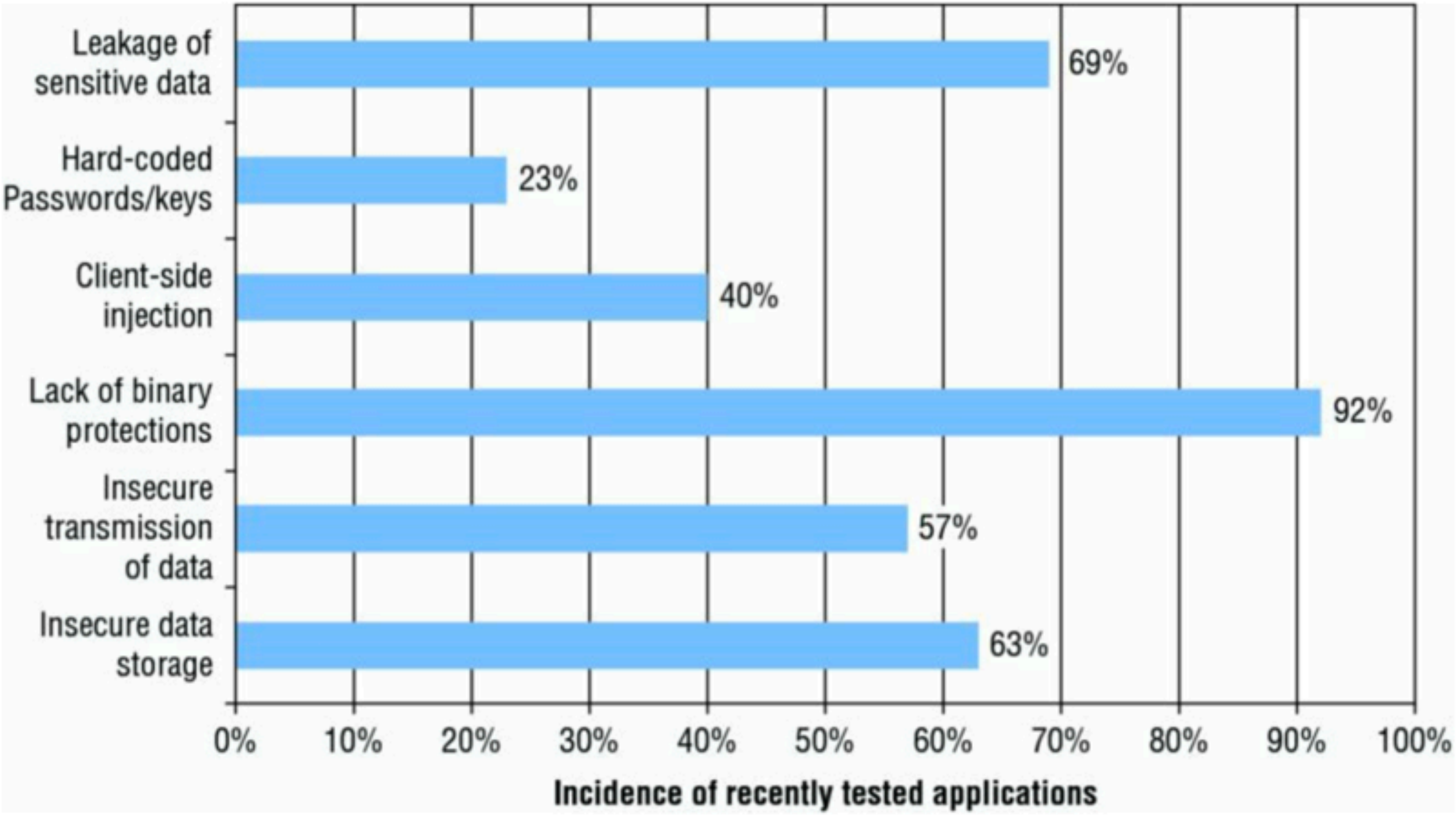
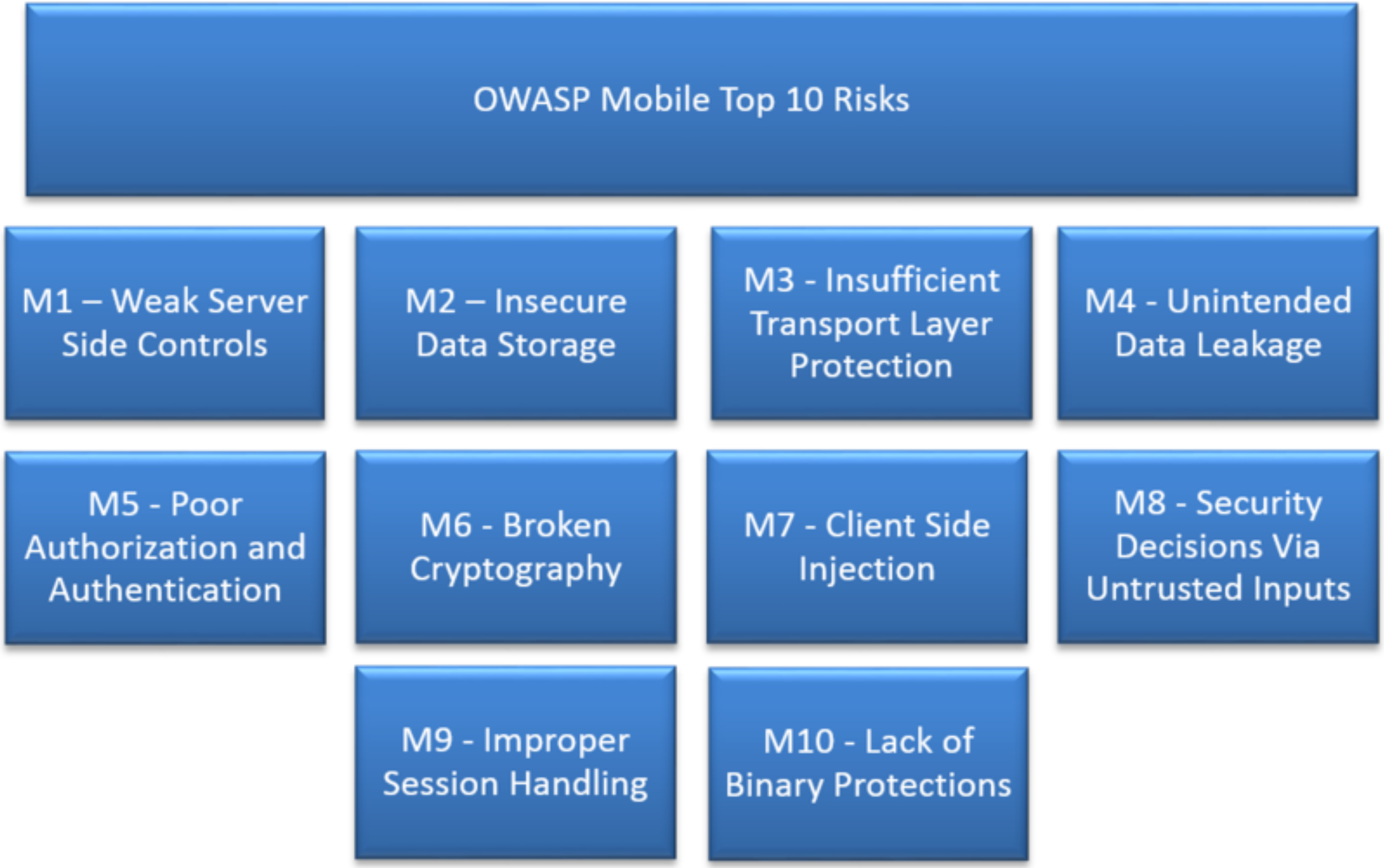


Figure 1.1 The incidence of some common mobile application vulnerabilities recently tested by the authors

Key Problem Factors

- Underdeveloped security awareness
  - By developers
- Ever-changing attack surface
- Custom development
  - In-house code mixed with libraries from many sources

OWASP Top Ten



OWASP Mobile Top 10 Risks

M1 – Weak Server Side Controls

M2 – Insecure Data Storage

M3 - Insufficient Transport Layer Protection

M4 - Unintended Data Leakage

M5 - Poor Authorization and Authentication

M6 - Broken Cryptography

M7 - Client Side Injection

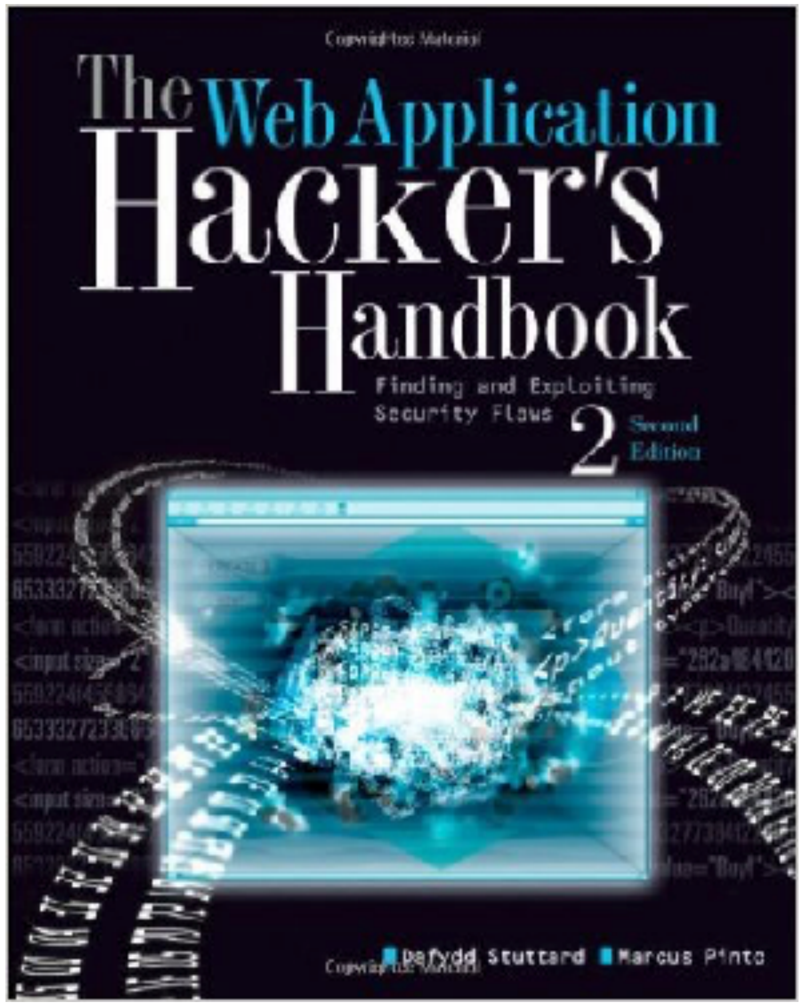
M8 - Security Decisions Via Untrusted Inputs

M9 - Improper Session Handling

M10 - Lack of Binary Protections

OWASP Top Ten

- **M1: Weak Server-Side Controls**
  - The most critical issue
  - Not a flaw on the phone
  - Server errors and misconfigurations
  - A whole class covers this: CNIT 129S: Securing Web Applications


The Web Application Hacker's Handbook
Finding and Exploiting Security Flaws
2 Second Edition
Dafydd Stuttard
Marcus Pinto

OWASP Top Ten

- **M2: Insecure Data Storage**
  - Plaintext or obfuscated
- **M3: Insufficient Transport Layer Protection**
  - Failure to validate TLS certificates
- **M4: Unintended Data Leakage**
  - In logs, cache, snapshots, etc

OWASP Top Ten

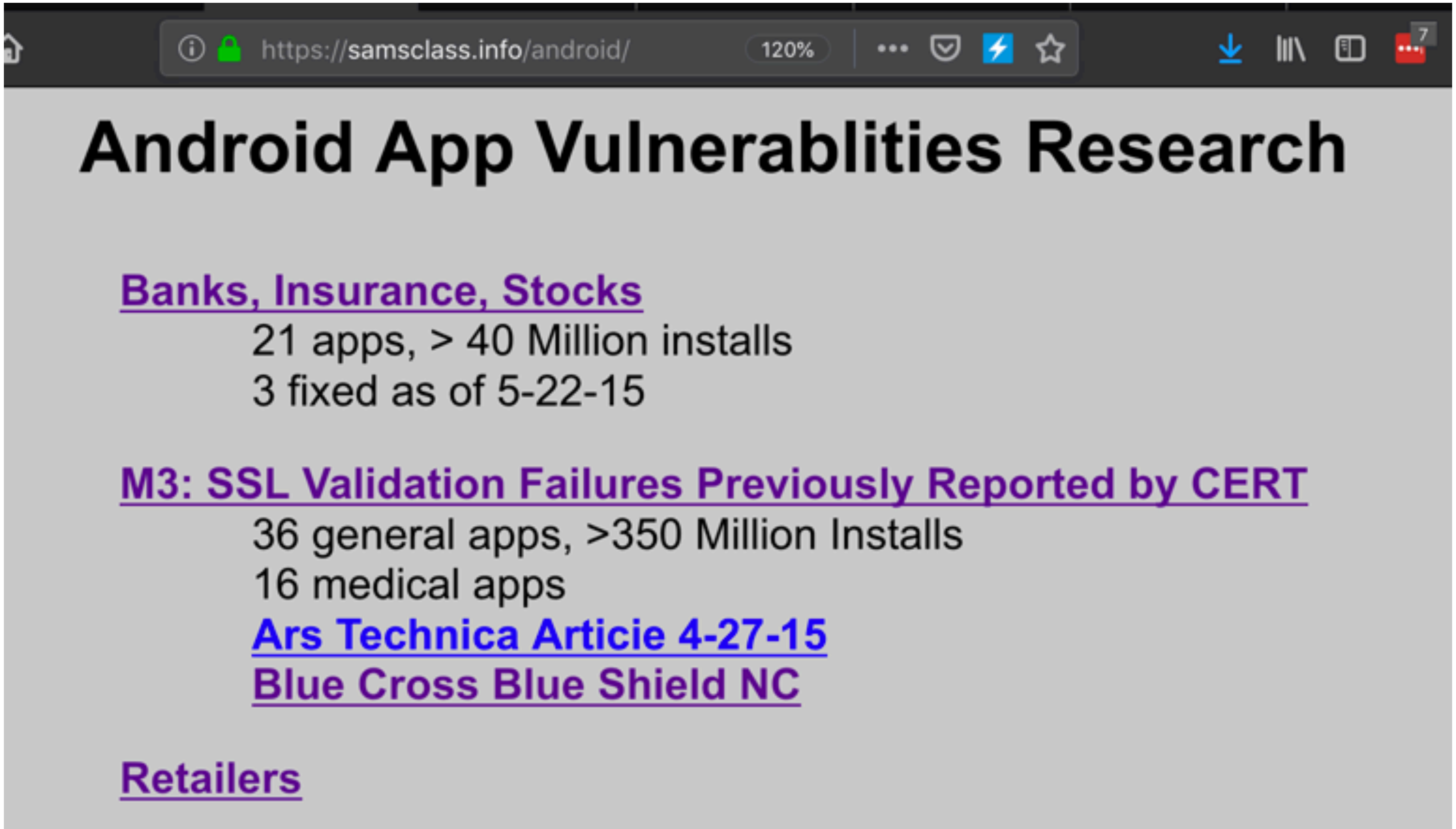
- **M5: Poor Authorization and Authentication**
  - Causes failures in access control
- **M6: Broken Cryptography**
  - Hard-coded key, or key stored on device
- **M7: Client-Side Injection**
  - App takes input from another app, server, etc.

OWASP Top Ten

- **M8: Security Decision Via Untrusted Inputs**
  - Often Inter-Process Communication (IPC)
- **M9: Improper Session Handling**
  - Exposing session tokens to adversary
- **M10: Lack of Binary Protections**
  - Allows reverse-engineering and modification of app

OWASP Mobile Security Tools

- **iMAS**
  - Framework to develop secure iOS apps
- **GoatDroid, iGoat, DV iOS**
  - Deliberately insecure apps for practice
- **MobiSec**
  - Mobile pentesting distribution, like Kali
- **Androick**
  - For Android forensics



Android App Vulnerablities Research

Banks, Insurance, Stocks

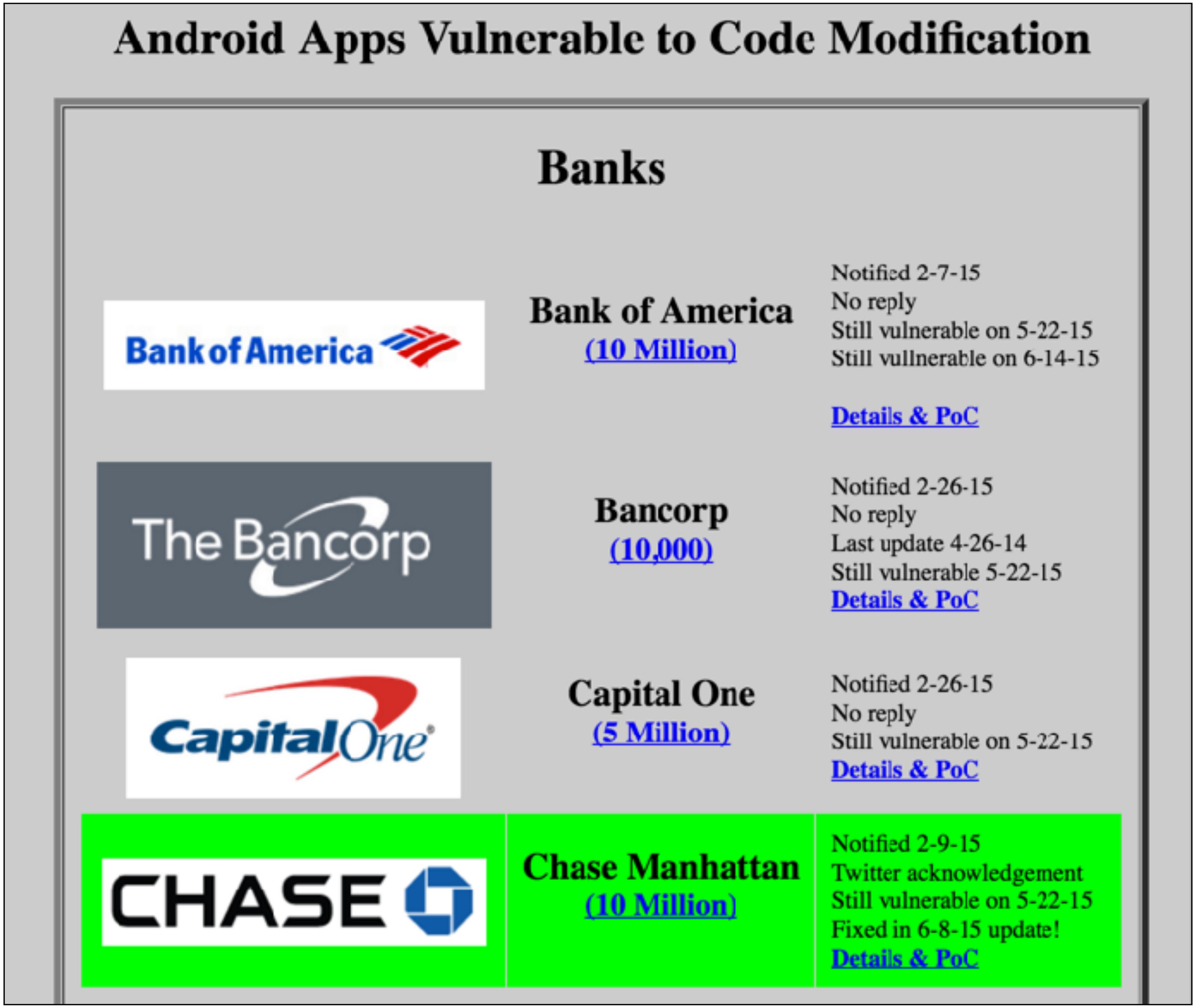
21 apps, > 40 Million installs
3 fixed as of 5-22-15

M3: SSL Validation Failures Previously Reported by CERT

36 general apps, >350 Million Installs
16 medical apps
Ars Technica Articie 4-27-15
Blue Cross Blue Shield NC

Retailers

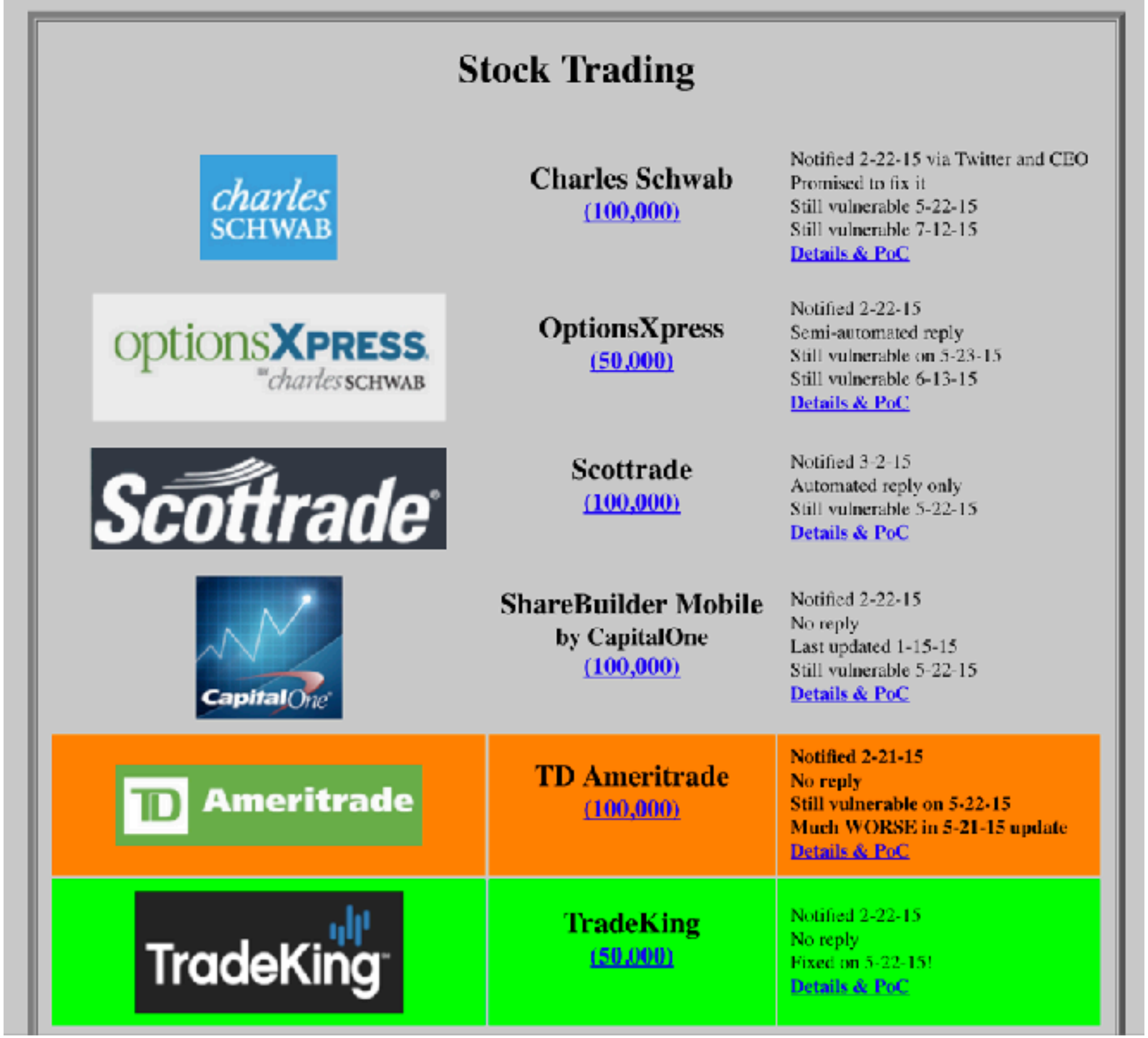
- **Link Ch 1b**



Android Apps Vulnerable to Code Modification

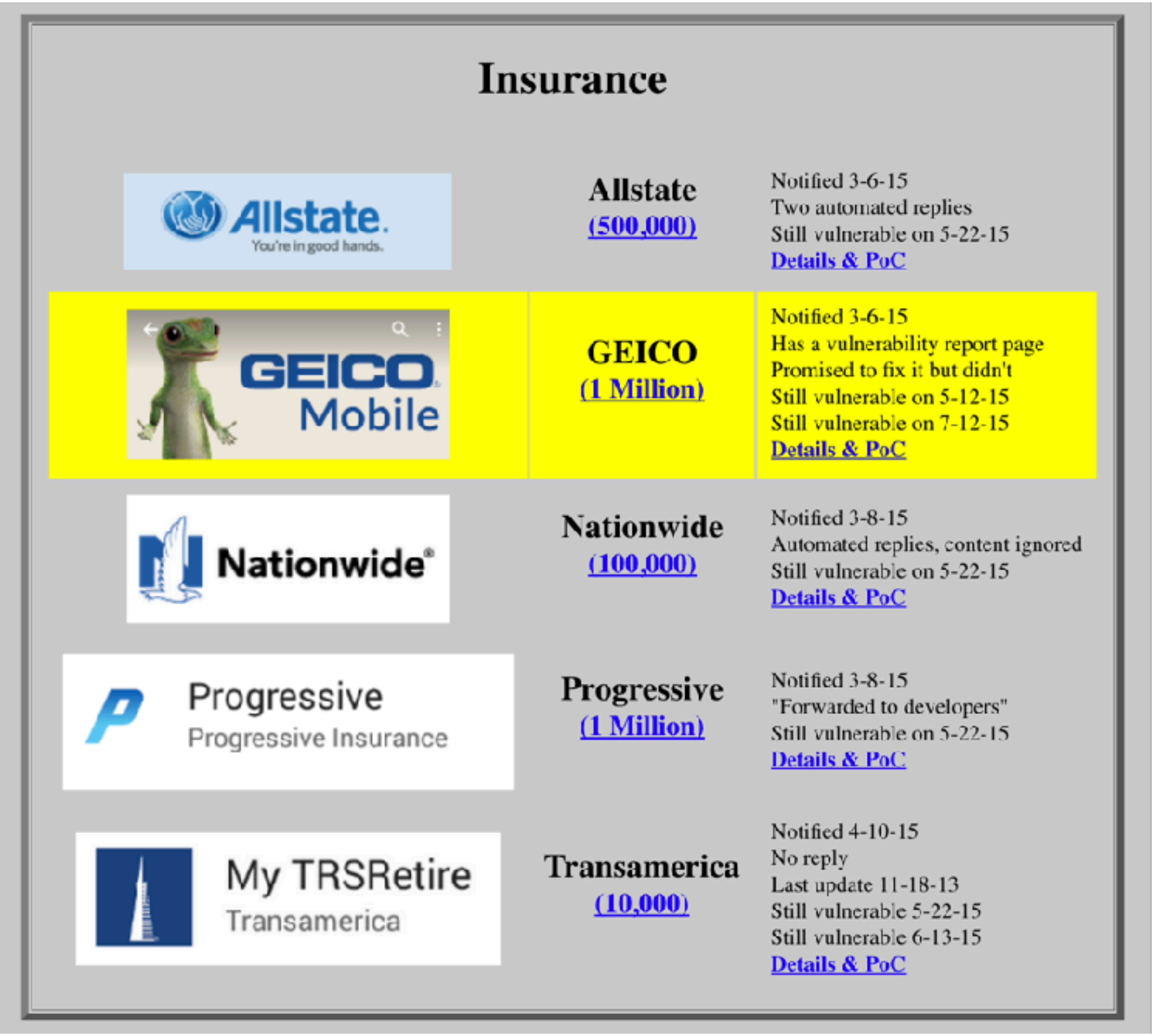
Banks

Bank of America	**Bank of America** **(10 Million)**	Notified 2-7-15 No reply Still vulnerable on 5-22-15 Still vullnerable on 6-14-15 **Details & PoC**
The Bancorp	**Bancorp** **(10,000)**	Notified 2-26-15 No reply Last update 4-26-14 Still vulnerable 5-22-15 **Details & PoC**
Capital One	**Capital One** **(5 Million)**	Notified 2-26-15 No reply Still vulnerable on 5-22-15 **Details & PoC**
CHASE	**Chase Manhattan** **(10 Million)**	Notified 2-9-15 Twitter acknowledgement Still vulnerable on 5-22-15 Fixed in 6-8-15 update! **Details & PoC**



Stock Trading

	Charles Schwab (100,000)	Notified 2-22-15 via Twitter and CEO Promised to fix it Still vulnerable 5-22-15 Still vulnerable 7-12-15 Details & PoC
	OptionsXpress (50,000)	Notified 2-22-15 Semi-automated reply Still vulnerable on 5-23-15 Still vulnerable 6-13-15 Details & PoC
	Scottrade (100,000)	Notified 3-2-15 Automated reply only Still vulnerable 5-22-15 Details & PoC
	ShareBuilder Mobile by CapitalOne (100,000)	Notified 2-22-15 No reply Last updated 1-15-15 Still vulnerable 5-22-15 Details & PoC
	TD Ameritrade (100,000)	**Notified 2-21-15** **No reply** **Still vulnerable on 5-22-15** **Much WORSE in 5-21-15 update** Details & PoC
	TradeKing (50,000)	Notified 2-22-15 No reply Fixed on 5-22-15! Details & PoC



Insurance

Allstate. You're in good hands.	**Allstate** (500,000)	Notified 3-6-15 Two automated replies Still vulnerable on 5-22-15 Details & PoC
GEICO. Mobile	**GEICO** (1 Million)	Notified 3-6-15 Has a vulnerability report page Promised to fix it but didn't Still vulnerable on 5-12-15 Still vulnerable on 7-12-15 Details & PoC
Nationwide®	**Nationwide** (100,000)	Notified 3-8-15 Automated replies, content ignored Still vulnerable on 5-22-15 Details & PoC
Progressive Progressive Insurance	**Progressive** (1 Million)	Notified 3-8-15 "Forwarded to developers" Still vulnerable on 5-22-15 Details & PoC
My TRSRetire Transamerica	**Transamerica** (10,000)	Notified 4-10-15 No reply Last update 11-18-13 Still vulnerable 5-22-15 Still vulnerable 6-13-15 Details & PoC

Android App Vulnerabilities Disclosed at DEF CON 25

Password Stored with Reversible Encryption

Home Depot	Notified 4-19-17; automated reply, no fix as of 7-28-17
Kroger	Notified 4-24-17; no reply; still vulnerable as of 7-28-17
Safeway	Notified 4-21-17; no reply; changed but probably still vulnerable as of 7-28-17
Walgreens	Notified 5-3-17; no reply; still vulnerable as of 7-28-17

Kahoot!