Mobile Money, Mobile Problems
- Seminararbeit -

Struktur

- Wer?
- Was? / Was nicht?
- Wie?
- Ergebnisse?
- Haftung?
- Reaktionen?
- Fragen?

Wer?

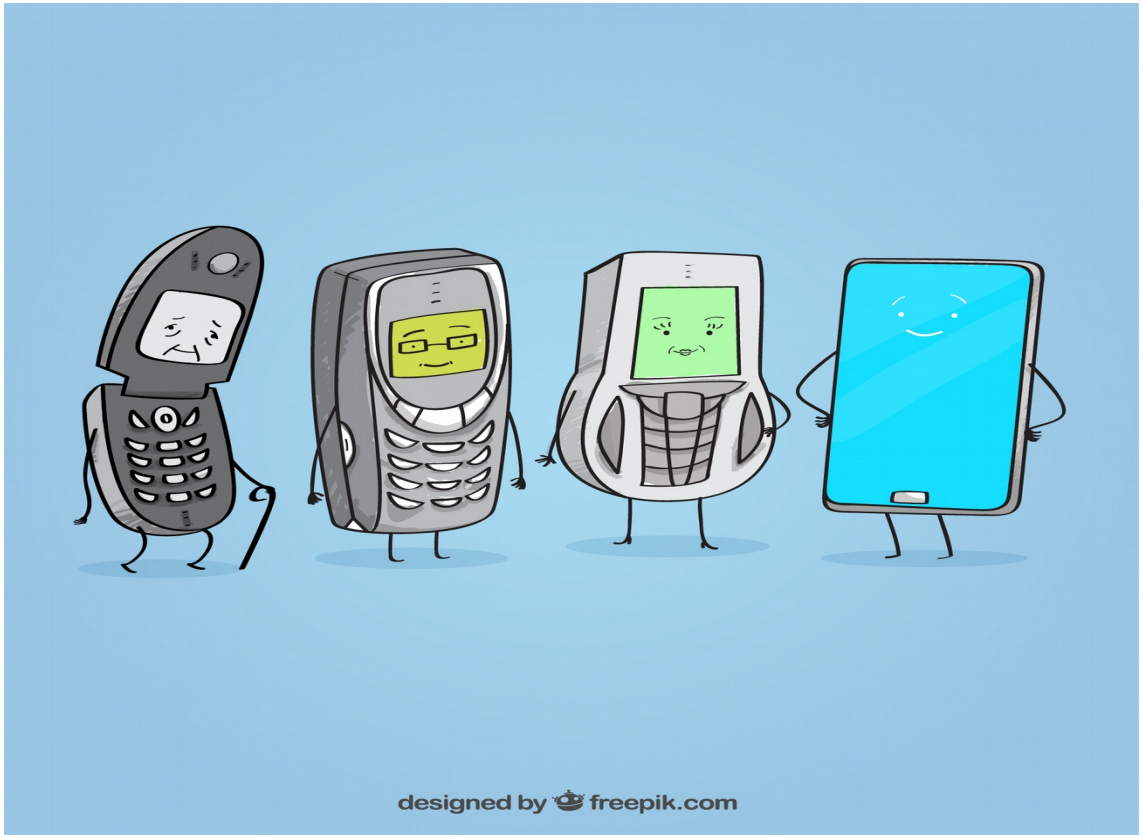
- Bradley Reaves, Nolen Scaife, Adam Bates, Patrick Traynor, and Kevin R.B. Butler
- University of Florida
- 24. USENIX Security Symposium
- August 2015

Was?

- Branchless Banking / Mobile Money

Was?

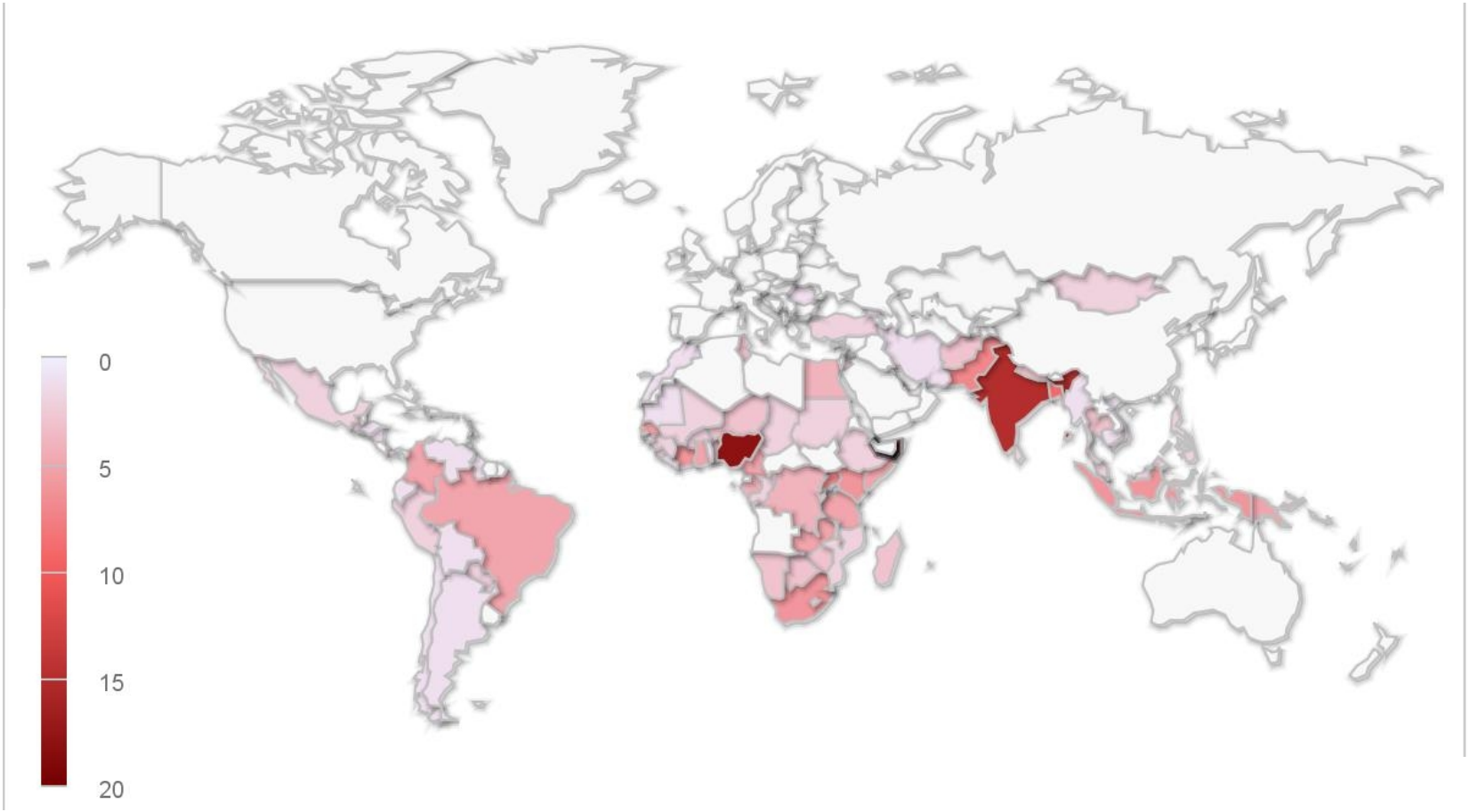
- Branchless Banking / Mobile Money



Ursprung: M-PESA

- 2007: Vodafone & Safaricom in Kenia
- Guthaben aufladen / versenden / auszahlen

Verbreitung



http://www.gsma.com/mobilefordevelopment/programmes/mobile-money/insights/tracker

Vorteile

Was nicht? - Mobile Payment

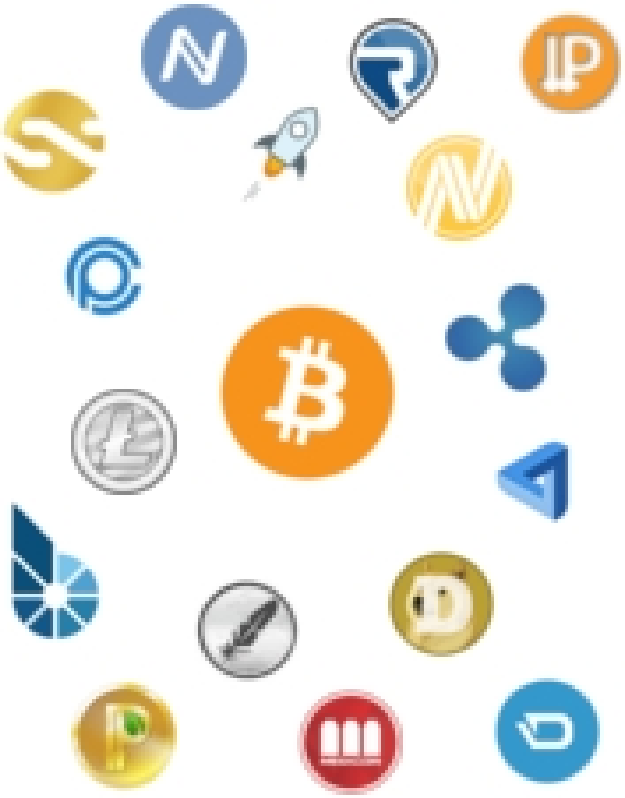
Was nicht? - Mobile Wallets

PayPal™

Google wallet

Pay

Was nicht? - Kryptowährungen



Wie? - Vorgehen der Forscher

Wie? - Vorgehen der Forscher

- Automatisierte Analyse der 46 verfügbaren Apps
- Mallodroid:
  - Über 50 % der Apps kritische TLS-Fehler
  - Durchschnittlich 9,3 % TLS-Fehler laut Mallodroid-Paper

Wie? - Ausgewählte Apps

	GCash	Phillipines
	Zuum	Brazil
mCoin	MCoin	Indonesia
MONEY ON MOBILE	Money on Mobile	India
mpay	Mpay	Thailand
airtel	Airtel Money	India
	Oxigen Wallet	India

Wie? - Ausgewählte Apps

GCash	7
Money on Mobile	6
Oxigen Wallet	6
Mpay	4
MCoin	3
Airtel Money	2
Zuum	0

Wie? - TLS Scans

- Qualys SSLLabs
- testssl.sh

SSL Report: api.myairtelapp.bsbportal.in (125.21.246.65)

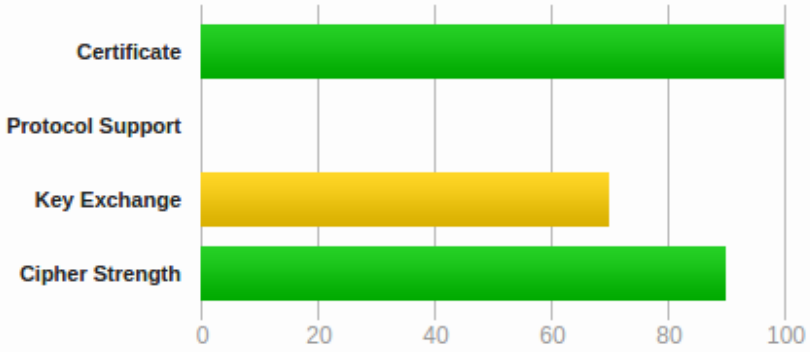
Assessed on: Sat, 09 Jan 2016 18:28:09 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the OpenSSL CCS vulnerability (CVE-2014-0224) and exploitable. Grade set to F.

This server is vulnerable to the Heartbleed attack. Grade set to F.

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > partnerapp.mpay.co.th

SSL Report: partnerapp.mpay.co.th (202.149.26.106)

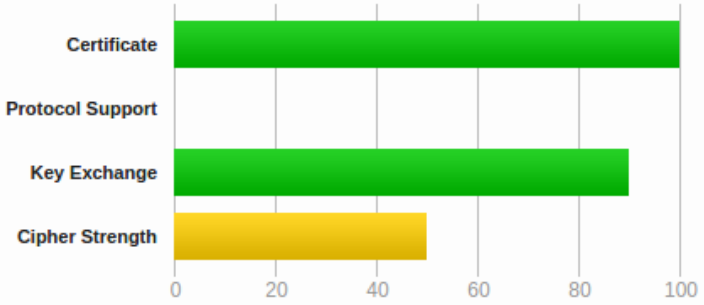
Assessed on: Sun, 10 Jan 2016 09:53:42 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the POODLE TLS attack. Patching required. Grade set to F. MORE INFO »

This server is vulnerable to MITM attacks because it supports insecure renegotiation. Grade set to F.

This server uses SSL 3, which is obsolete and insecure. Grade capped to B. MORE INFO »

Certificate has a weak signature and expires after 2015. Upgrade to SHA2 to avoid browser warnings. MORE INFO »

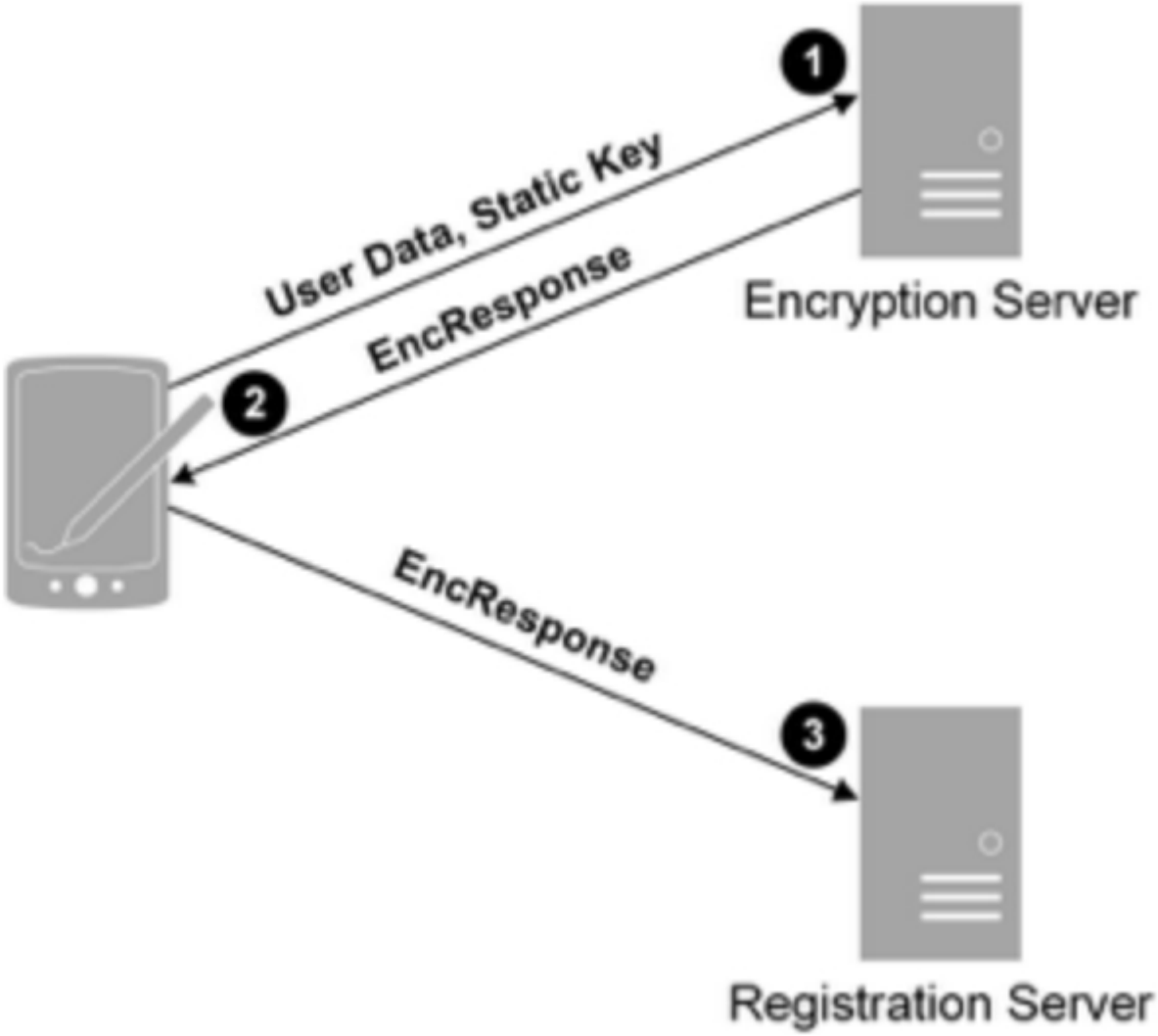
This server uses RC4 with modern protocols. Grade capped to C.

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Ergebnisse? - SSL / TLS

- Android übernimmt Zertifikatsvalidierung standardmäßig
- Entwickler überschreiben sichere Routinen
  - MCoin nutzte ein seit Jahren abgelaufenes, selbstsigniertes Zertifikat für localhost !
  - Money on Mobile nutzt gar kein TLS

Ergebnisse? - Seltsame Krypto



Ergebnisse? - Kreative Keys I

$$Key_{enc} = \texttt{j7zgy1yv} \,||\, phone\# \,||\, account\#$$

Ergebnisse? - Kreative Keys II

Oxigen Wallet

$$Key_{enc} = \texttt{Random.Random}[17] \,||\, phone\# \,||\, date \,||\, 0^{128-n}$$

Haftung? - AGBs!

- Hersteller: unsere Apps sind sicher!
- Betrug nur möglich, wenn Nutzer schlecht mit seinen Zugangsdaten umgeht

Haftung? - AGBs!

- Hersteller: unsere Apps sind sicher!
- Betrug nur möglich, wenn Nutzer schlecht mit seinen Zugangsdaten umgeht

Nutzer haftet zu 100% !

Reaktionen? - ...

- 6 Hersteller der problematischen Apps angeschrieben (6 / 7)

Reaktionen? - ...

- 6 Hersteller der problematischen Apps angeschrieben (6 / 7)

Oxigen: “We knew there are problems and are working on it”

Money On Mobile: “We’ll get back to you”

Schluss! - Vorbei.

- Möglichkeiten moderner Technik sinnvoll für Entwicklungsländer
- Hohe Risiken im Bereich Mobile Money aufgrund schlechter Implementierungen
- MangelndesSicherheitsbewusstsein / Wissen über IT-Sicherheit

Fragen? - Hä?