



Mobile Threat Landscape and Device Biometrics

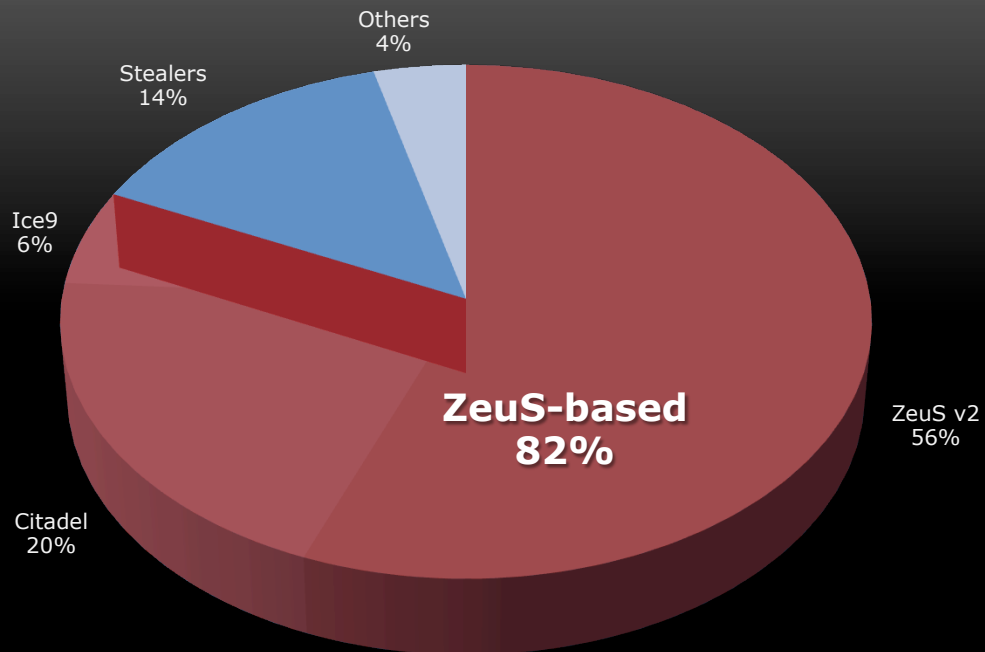
Sean Taylor

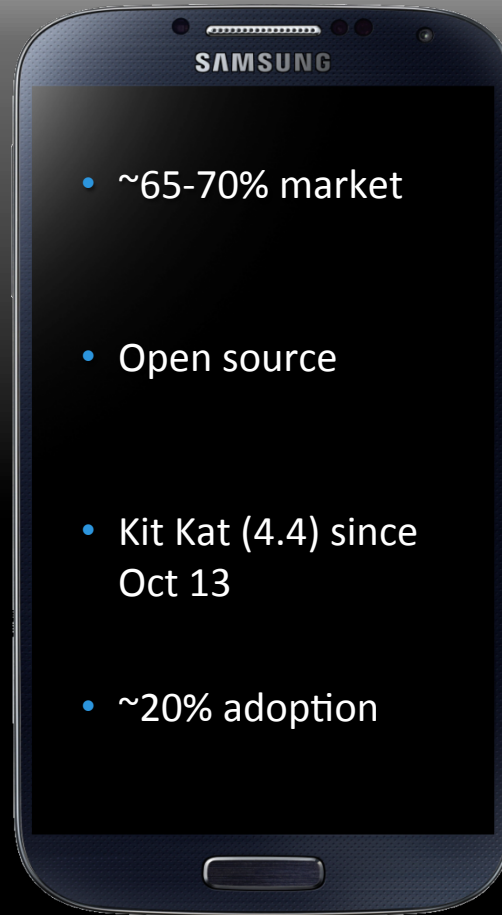
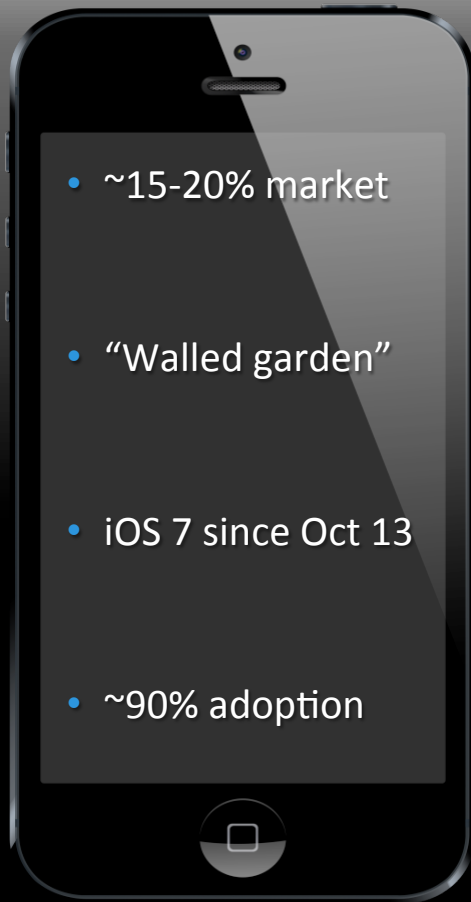
Senior Systems Engineer – Fraud and Risk Intelligence





Malware Landscape (RSA AFCC, 2014 H1)







Do you want to install this application? It will get access to:

PRIVACY



directly call phone numbers
📞 this may cost you money
read phone status and identity



edit your text messages (SMS or MMS)
read your text messages (SMS or MMS)
receive text messages (SMS)
send SMS messages
📞 this may cost you money



record audio



read call log
read your contacts



modify or delete the contents of your USB storage



iBANKING Admin Area

Project ID: 555 (11 phones, user) Color scheme: Yellow

Manage users and projects

Oct 06, 2014 09:26:59

User: admin

iBANKING Admin Area

Project ID: 555 (11 phones, user) Color scheme: Yellow

Manage users and projects

Oct 06, 2014 09:30:21

User: admin

Selected phone: 107 Last command: call list (send) Send time: 02-10-2014 09:18:31 Status: SMS ON Call OFF Rec OFF Admin ON Rec call OFF

General Info | Intercepted SMS List | All SMS List | All Call List | Contact List | URL Analyse | Sounds List | Application List | Pictures List | Code History |

Commands

Refresh Status Bar

Commands

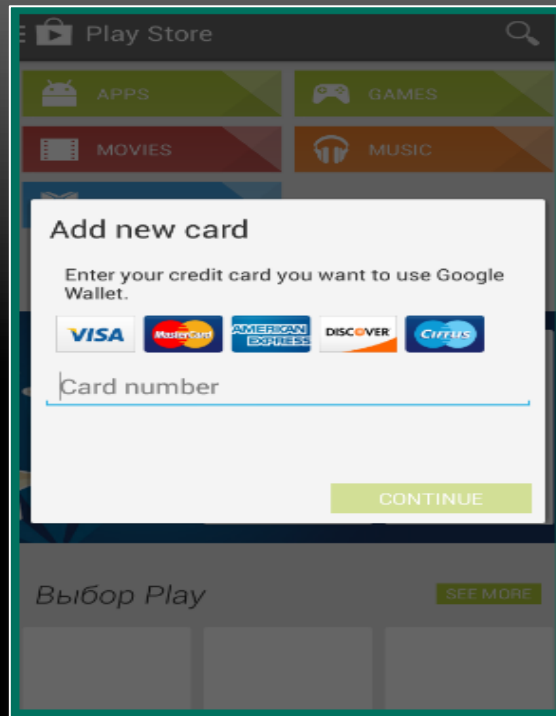
Start SMS	Stop SMS	Start call	Stop call	Start record	Stop record	Start call to #
Get SMS	Get Call	Contact list	Send SMS	Check URL	Get images	Get place
Get apps	Grid	Start record call	Stop record call	Change control number	Change control number for all project	Wipe data

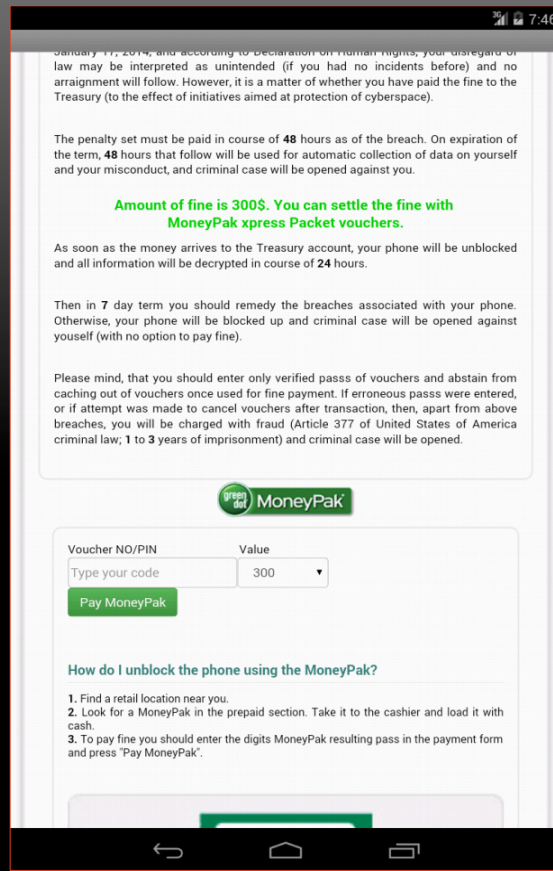
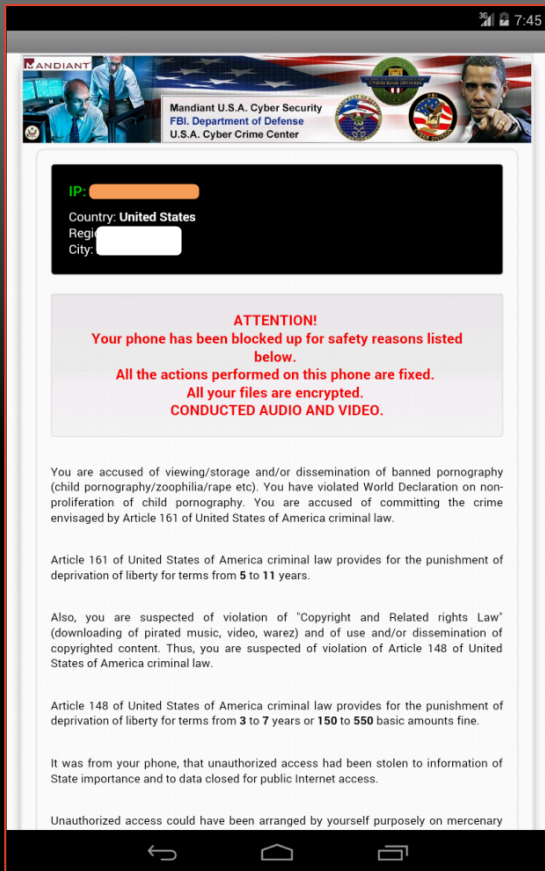
Number IMEI ICCID Code Info

Show all phone | Show favorites only

761	☆
107	☆
191	☆
613	☆
210	☆
549	☆
120	☆
704	☆
	☆
	☆
635	☆

SVPENG: Mobile Phishing





Agence Nationale de la Sécurité des Systèmes d'Information
Haute Autorité pour la Diffusion des Œuvres et la Protection des Droits sur Internet

IP: [redacted]
Pay: [redacted]
Reg: [redacted]
City: [redacted]

ATTENTION!
Votre téléphone est bloqué pour des raisons de sécurité suivantes.
Toutes les opérations effectuées à partir de ce téléphone, sont enregistrées.
Tous vos fichiers sont cryptés.

POLITIE
Kerpi Landelijke Politiediensten
Oronksker Ministerie
CYBERSCHEM POLITIE NEDERLAND

IP: [redacted]
Land: Netherlands
Regio: [redacted]
City: [redacted]

ATTENTIE! Uw telefoon wordt geblokkeerd om veiligheidsoverwegingen wegens de hieronder opgegeven redenen.
Alle op deze telefoon uitgevoerde activiteiten zijn opgetekend.
Al uw bestanden zijn gecodeerd.

FEDPOL Bundeskriminalpolizei
Ordnungsministerium für Ankauf und Verkauf
der Internet-Kriminalität (OKZK)

IP: [redacted]
Land: Switzerland
Bereich: [redacted]
Stadt: [redacted]

WARNING! Zugang von Ihrem Telefon wurde vorläufig aus den unten aufgeführten Gründen gesperrt.
Alle Tätigkeiten, die auf diesem Telefon durchgeführt werden, werden fixiert.
Alle Ihre Dateien sind verschlüsselt.

Polizja. Biuro Służby Kryminalnej
Wydział Wpływu Związana Ciężkimi Przestępstwami

IP: [redacted]
Kraj: Poland
Region: [redacted]
Miasto: [redacted]

UWAGA! Pańska telefon został zablokowany ze względu na bezpieczeństwo z wskazanych niżej przyczyn.
Wszystkie działania tego telefonu są monitorowane.
Wszystkie Pańskie pliki zostały zaszyfrowane.

Vous êtes accusé de violation/stockage et/ou de la distribution de matériel de caractère pornographique (téléchargement de la musique et distribution du contenu de la musique) et/ou de la violation de la Loi sur la protection de la vie privée et de la Loi sur la protection de la vie privée de la République Française.

L'article 161 du Code pénal d'incarcération allant de 5 à 11 ans.

En outre Vous êtes soupçonné (chargement de la musique et distribution du contenu de la musique) et/ou de la violation de la Loi sur la protection de la vie privée de la République Française.

L'article 148 du Code pénal d'amende de 150 à 550 unités de monnaie nationale.

Un accès non autorisé à l'Internet a été constaté dans le réseau Internet.

U wordt beschuldigd van het gebruik/opslaan en/of verspreiden van de pornografische producten (wat inhoudt: het downloaden van muziek en het verspreiden van muziek) en/of van de verspreiding van de inhoud van de internationale Declaratie over de bestrijding van de kinderpornografie (downloaden van muziek en verspreiden van muziek) en/of van de verspreiding van de inhoud van de Wetboek van Strafrecht van het Koninkrijk der Nederlanden.

De misdrijven van deze aard worden strafbaar gesteld in het Koninkrijk der Nederlanden de duur van 5 tot 11 jaar.

Daarnaast wordt u ook verdacht van het schenken van naburige rechten (wat inhoudt: downloaden van muziek en verspreiden van muziek) en van het gebruik van auteursrechtelijk beschermd materiaal (downloaden van muziek en verspreiden van muziek) en van het gebruik van auteursrechtelijk beschermd materiaal (downloaden van muziek en verspreiden van muziek) en van het gebruik van auteursrechtelijk beschermd materiaal (downloaden van muziek en verspreiden van muziek).

Volgens artikel 148 van het Wetboek van Strafrecht van het Koninkrijk der Nederlanden kan u worden veroordeeld tot een boete van 150 tot 550 van de basiseenheid van de munt van het Koninkrijk der Nederlanden.

Es wird die Ansicht/Lagerung und/oder den Vertrieb von pornographischem Material und/oder die Verbreitung von pornographischem Material (Herunterladen von Musik und Verbreitung von Musik) und/oder die Verbreitung von der internationalen Erklärung zur Bekämpfung der Kinderpornografie (Herunterladen von Musik und Verbreitung von Musik) und/oder die Verbreitung von der internationalen Erklärung zur Bekämpfung der Kinderpornografie (Herunterladen von Musik und Verbreitung von Musik) und/oder die Verbreitung von der internationalen Erklärung zur Bekämpfung der Kinderpornografie (Herunterladen von Musik und Verbreitung von Musik).

Es wird die Verletzung des "Gesetz über Urheberrechte" (Herunterladen von Musik und Verbreitung von Musik) und die Verwendung und/oder Weitergabe von urheberrechtlich geschütztem Material (Herunterladen von Musik und Verbreitung von Musik) und die Verwendung und/oder Weitergabe von urheberrechtlich geschütztem Material (Herunterladen von Musik und Verbreitung von Musik) und die Verwendung und/oder Weitergabe von urheberrechtlich geschütztem Material (Herunterladen von Musik und Verbreitung von Musik).

Es wird die Verletzung des "Gesetz über Urheberrechte" (Herunterladen von Musik und Verbreitung von Musik) und die Verwendung und/oder Weitergabe von urheberrechtlich geschütztem Material (Herunterladen von Musik und Verbreitung von Musik) und die Verwendung und/oder Weitergabe von urheberrechtlich geschütztem Material (Herunterladen von Musik und Verbreitung von Musik).

Pan/Pani jest oskarżony/a w zarządzie/przechowywaniu i/abno rozpowszechnianiu materiałów pornograficznych (pobieranie i rozpowszechnianie muzyki i rozpowszechnianie treści) i/lub naruszenie międzynarodowej Deklaracji o zwalczaniu pedofilii (pobieranie i rozpowszechnianie muzyki i rozpowszechnianie treści) i/lub naruszenie międzynarodowej Deklaracji o zwalczaniu pedofilii (pobieranie i rozpowszechnianie muzyki i rozpowszechnianie treści) i/lub naruszenie międzynarodowej Deklaracji o zwalczaniu pedofilii (pobieranie i rozpowszechnianie muzyki i rozpowszechnianie treści).

Art. 161 Kodeksu Karyminalnego

Ważny! Twój telefon został zablokowany z powodów bezpieczeństwa z wymienionych poniżej przyczyn. Wszystkie działania tego telefonu są monitorowane. Wszystkie Twoje pliki zostały zaszyfrowane.

Cheshire PCOU
Serious Organised Crime Agency
METROPOLITAN BRITISH POLICE

IP: [redacted]
Country: United Kingdom
Region: [redacted]
City: [redacted]

ATTENTION!
Your phone has been blocked up for safety reasons listed below.
All the actions performed on this phone are fixed.
All your files are encrypted.
CONDUCTED AUDIO AND VIDEO.

POLISI
POLISHSHALLITUKSEN
Keskusrikospoliisi
Polishsi Teknilliskeskus

IP: [redacted]
Maa: Finland
Alue: [redacted]
Kaupunki: [redacted]

HUOMIO!
Puhelin on lukittu turvallisuuden vuoksi allamainittujen syiden takia.
Kaikki tässä puhelin tyhdyt toiminnat on merkity.
Kaikki Teidän tiedostonne on kirjoitettu salaksiksi.

YANDARMA GENEL KOMUTANGLI
Türkiye Cumhuriyeti İçişleri Bakanlığı
Türkiye Cumhuriyeti İçişleri Bakanlığı

IP: [redacted]
Ülke: Turkey
Bölge: [redacted]
Şehir: [redacted]

DİKKAT!
Telefon güvenliğin hususunda aşağıdaki nedenlerle bloke edilmiştir.
Bu telefon yapılan tüm eylemleriniz kaydedilecektir.
Tüm dosyalarınız şifrelenmiştir.

You are accused of viewing/storage and/or dissemination of banned pornography (child pornography/zoophilia/etc etc). You have violated World Declaration on non-proliferation of child pornography. You are accused of committing the crime envisaged by Article 161 of the Kingdom of Great Britain criminal law.

Article 161 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 5 to 11 years.

Also, you are suspected of violation of "Copyright and Related rights Law" (downloading of pirated music, video, and/or of use and/or dissemination of copyrighted content). Thus, you are suspected of violation of Article 148 of the Kingdom of Great Britain criminal law.

Article 148 of the Kingdom of Great Britain criminal law provides for the punishment of deprivation of liberty for terms from 3 to 7 years or 150 to 550 basic-amounts fine.

It was from your phone, that unauthorized access had been stolen to information of State importance and to data classed for public internet access.

Unauthorized access could have been arranged by yourself purposely or maliciously.

Sinut syytetään katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.)

Suomen tasavallan rikoslain luvun 161 edellyttää rangaistuksena vapausrajoitusta 2-8 vuotta.

Sinä olet epäilty rikosten "Tekijänoikeus ja liittyvät oikeudet" (kopiointi ja levitys kiellettyä musiikkia, videoita, ja/tai niiden käyttöä ja levitystä) rikosten takia. Näin olet epäilty rikosten takia luvun 148 rikosten takia.

Suomen tasavallan luvun 148 edellyttää 150-550 perusyksikköä sakkoa tai vapausrajoitusta 3-7 vuotta.

puhelin avulla suoritettiin luvaton pääsy suljetuille tiedoille ja vahingonaiheisesti merkittävien tietojen tietokoneelliseen tutkimiseen.

Luvaton pääsy sinä olet suorittanut tahallan rikoksillään syytä tai laiton pääsy yrityksen suorittama puhelinneuvon sinun henkilösiä tai ilman suostumustasi, koska

Sinun syytetään katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.) katsella/ tallentaa ja/tai levittää kiellettyä pornografista materiaalia (lapsipornografia/soofiilia/ jne.)

Suomen tasavallan rikoslain luvun 161 edellyttää rangaistuksena vapausrajoitusta 2-8 vuotta.

Sinä olet epäilty rikosten "Tekijänoikeus ja liittyvät oikeudet" (kopiointi ja levitys kiellettyä musiikkia, videoita, ja/tai niiden käyttöä ja levitystä) rikosten takia. Näin olet epäilty rikosten takia luvun 148 rikosten takia.

Suomen tasavallan luvun 148 edellyttää 150-550 perusyksikköä sakkoa tai vapausrajoitusta 3-7 vuotta.

puhelin avulla suoritettiin luvaton pääsy suljetuille tiedoille ja vahingonaiheisesti merkittävien tietojen tietokoneelliseen tutkimiseen.

Luvaton pääsy sinä olet suorittanut tahallan rikoksillään syytä tai laiton pääsy yrityksen suorittama puhelinneuvon sinun henkilösiä tai ilman suostumustasi, koska

Siz yasaq pornografi matnalarını oxuməsi, saxlaməsi və ya qeyri dağdımında sudlanırsınız (çocuk pornografisi, zoofili, teceviz vb.) Siz çocuk pornografisi dağdımına keçir maddələrin Genel Qanun 161-ci maddəsi ilə əsas işləməli sudlanırsınız.

Türkiye Cumhuriyeti Ceza Kanununu 161-ci maddəsi ilə 5 yıldan 11 yıla kadar hapis cezası olaraak sağlar.

Ayrıca zəhmətə "Telif Haqqı və Əqli Haklar Yasası" nı pozmaqla sığışdır kəməndə bulunsunuzdur (burada musiqi, video, yasaq program yayımlama idarəmə) və Telif haqqının korunan işçisi kullandı və ya dağıtdı. Bəyəcə Siz Türkiye Cumhuriyeti Ceza Kanununu 148-ci maddəsinə bəzəmlə sığışdır kəməndə bulunsunuzdur.

Türkiye Cumhuriyeti Ceza Kanununu 148-ci maddəsi ilə 150-dən 550 həməd dəğər bəyudənə cəza cəzası və ya 3 yildən 7 yıla kadar hapis cezası olaraq sağlar.

Sizin telefon internetə kamru giriş kapalı bilgilye və uşaq idarəmə bilgilye yekitmiş giriş yelpizmiş.

Siz yekitmiş giriş bəzəmlə emalardə nəmərləy yekitmiş oblağıntınız və ya yekitmiş giriş Sizin habərət və Sizin izni olmaksızın yayımladı. Sizin telefon zararı programlara bulursunuz olarsa. Bəyəcə Siz əşyalarını saxlamalı Türkiye Cumhuriyeti

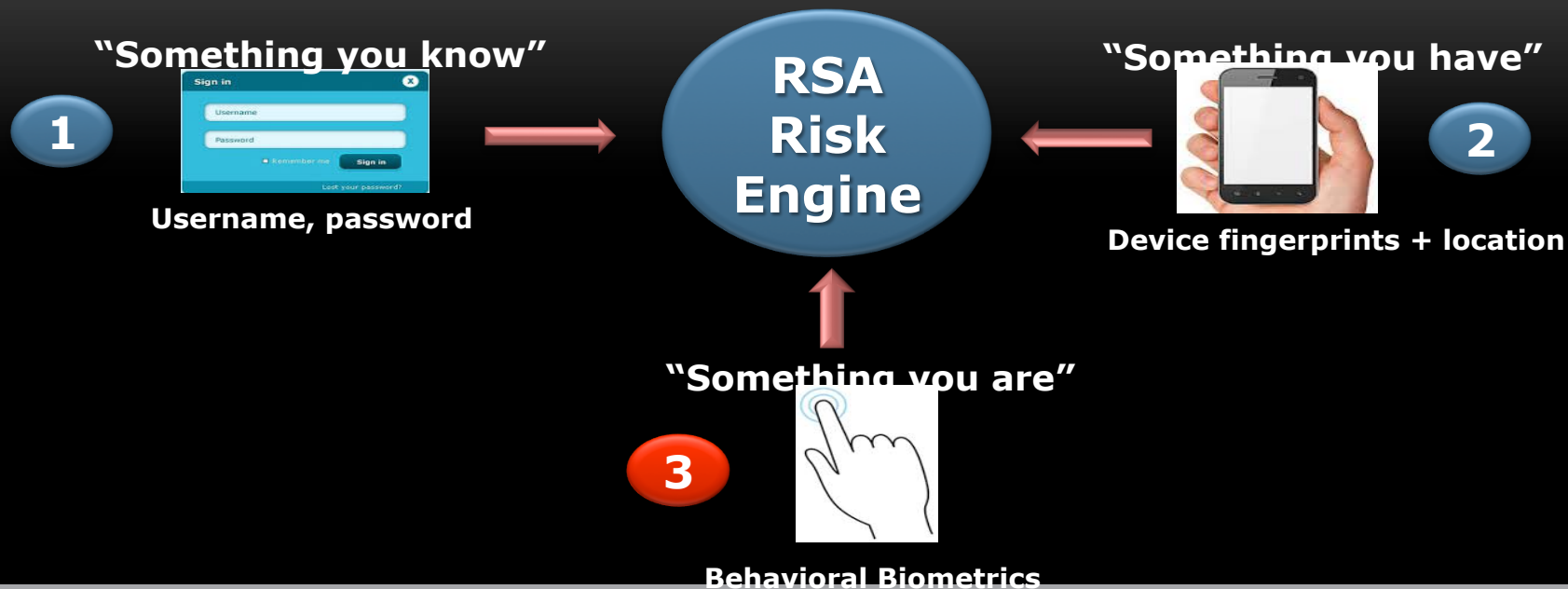


Primary Use Cases

- Step up authentication in online application
- Step up authentication for mobile application
 - Enhanced Biometric Authentication
 - Behaviometrics
- 3DS/Securecode
 - Joining MasterCard effort to redefine 3DS protocol for mobile
 - Support RSA 3DS platform
 - Allow mobile app transaction to go through 3DS protocol
 - Sell through development platforms: Shopify and more mobile app builders

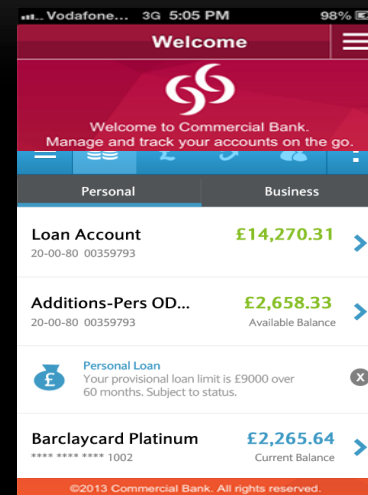
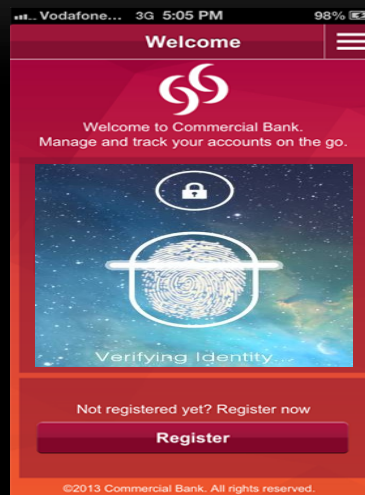
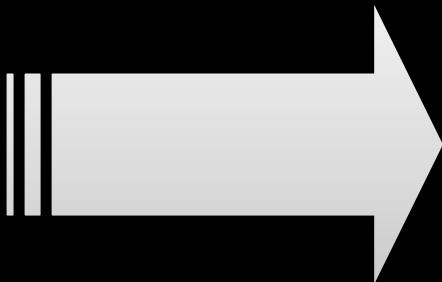
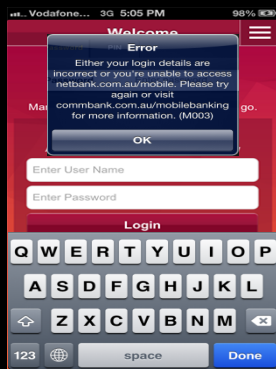
Behaviometrics

- Enhance mobile security by adding a third factor
 - “Something you are”



Consumer Mobile Primary Authentication

- Biometric and Behaviometric knowledge to authenticate a user to a mobile app without needing a username and password.
 - Improving usability
 - Increasing security

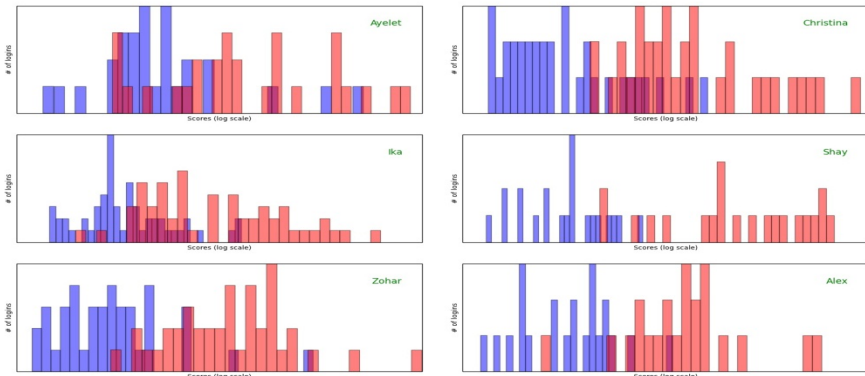


PoC Description

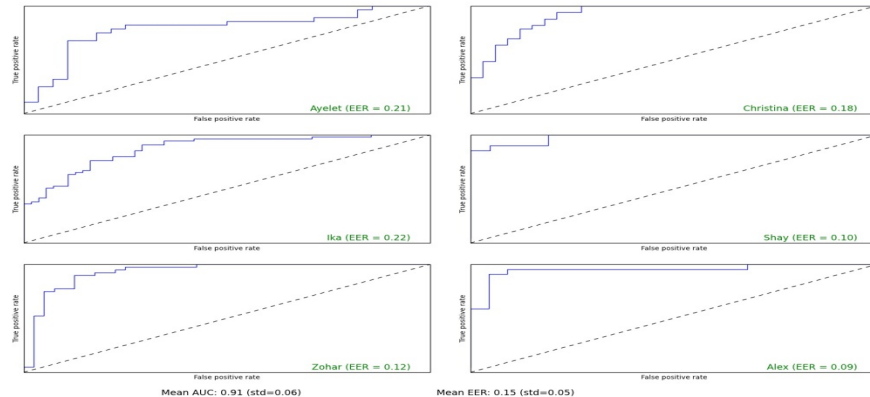
- MIT demo app for Android was configured to collect typing time latencies during login
 - Digraphs: time between each letter
 - Trigraphs: time between every other letter
- Data collection
 - Employees were selected to type a random generated credentials
 - Username: 34cJ817X; PW: x5651DA9
 - ~50 times each over a day or two

Results Analysis

Log-Score histograms (Training size = 15)



ROC curves (Training size = 15)



- Genuine users can be distinguished from impostors
 - Average equal error rate: ~20%

THANK YOU



sean.taylor2@rsa.com



uk.linkedin.com/in/staylor1



@snejsecurity



RSA®

EMC²®