I nuovi servizi bancari e di pagamento in mobilità e i relativi scenari di rischio

Guido Ronchetti
Product Manager: soluzione MORE®
guido.ronchetti@iks.it

www.iks.it
informazioni@iks.it
049.870.10.10

IKS: Centro di Competenza XTN-labs

Il Centro di Competenza XTN-labs (Gruppo IKS) è focalizzato nello sviluppo di sistemi di **Antifrode in ambito finanziario** e **sicurezza in ambito Mobile**, fornendo anche tutti i servizi a supporto.

In particolare:

- Sviluppo e supporto delle soluzioni MORE® e SMASH®;
- Attività di Intelligence in ambito Cyber Security;
- Attività di assessment di sicurezza su applicazioni mobile e legacy;
- Expertise su sistemi di predictive analysis ed analisi comportamentale.

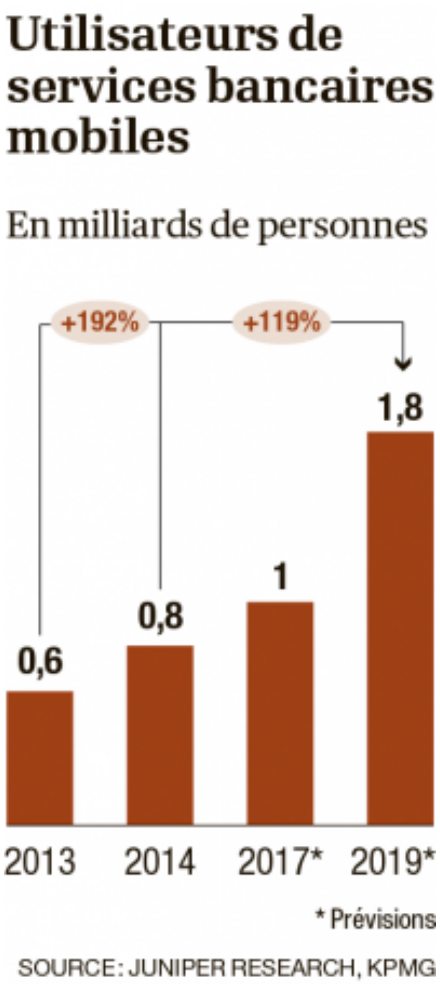
Abstract

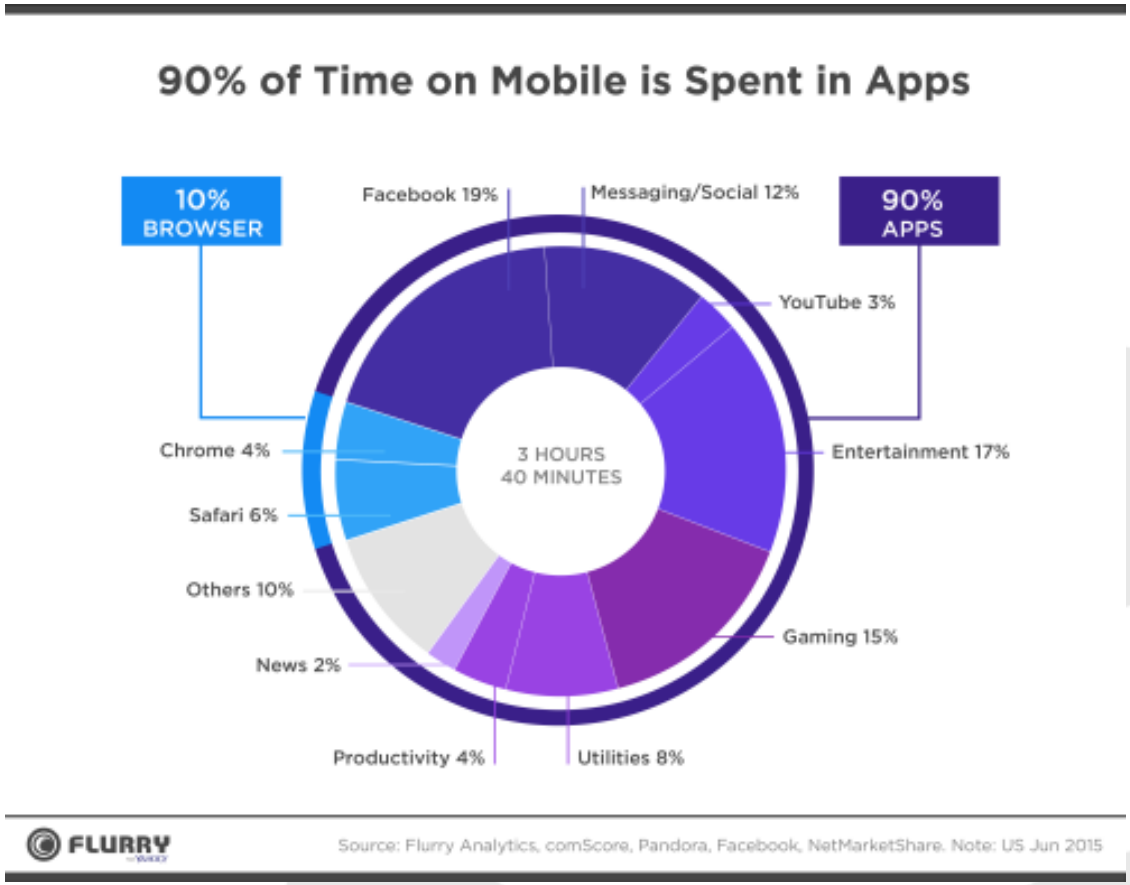
L'intervento descriverà come il mondo del mobile payment e banking stia evolvendo e quali potenziali problematiche di sicurezza sta mettendo in luce.

Agenda

- **Numeri del mobile oggi**
- Nuovi servizi bancari, payment e finanziari
- Sicurezza mobile oggi
- Sfide per la sicurezza
- Conclusioni
- Domande

Trend tecnologico globale





Fonte: Flurry (Yahoo Inc.)

Trend tecnologico italiano (ambito bancario)

Previsione di utilizzo dei diversi canali bancari

Sportello: 1-2 volte l'anno

Call center: 5-10 volte al mese

Bancomat: 3-5 volte al mese

Tablet: 7-10 volte al mese

Smartphone: 20-30 volte al mese

Fonte: prof. Fabrizio Cresti, Università Cattolica

Agenda

- Numeri del mobile oggi
- **Nuovi servizi bancari, payment e finanziari**
- Sicurezza mobile oggi
- Sfide per la sicurezza
- Conclusioni
- Domande

Nuovi servizi e modelli

Si sono affermati nuovi servizi e modelli in ambiti tradizionali:

- Nuove banche;
- Sistemi di pagamento;
- Trasferimento di denaro P2P;
- Trading.

Tutte queste hanno in comune l'utilizzo di mobile app…

Nuove banche esempio: Number26

Genesi:

- Fondata nel 2013
- Oggi 100 dipendenti c.a
- Presente in 8 paesi con c.a. 100.000 utenti

Servizi:

- Conto corrente (solo per singoli)
- Carta di Credito pre-pagata
- P2P (via email o SMS)

Addon:

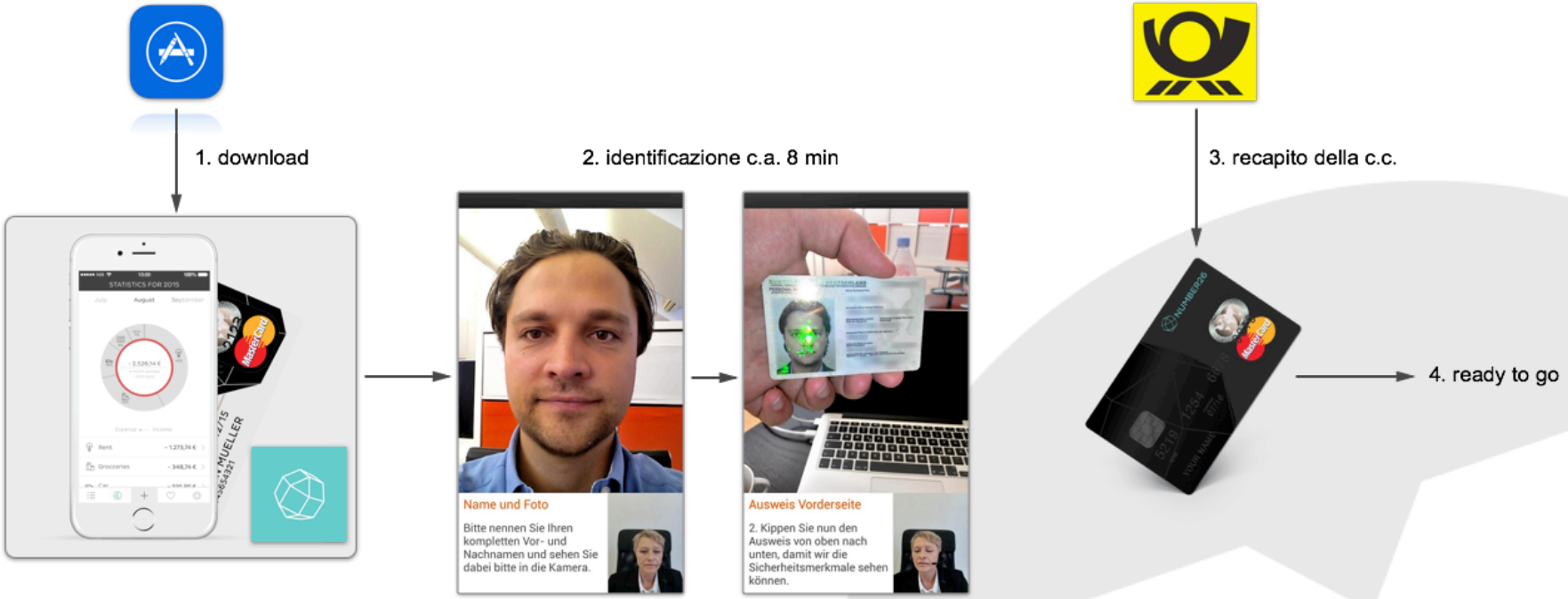
- Accesso via app mobile o web app (la prima ha funzionalità aggiuntive)
- Tracking e categorizzazione delle operazione di pagamento in tempo reale (via notifiche di push)
- Incentivo ad invitare nuovi utenti di 10€

Need di sicurezza:

- Identificazione iniziale degli utenti
- Protezione delle transazioni
- Non degradare la user experience degli utenti mantenendo un adeguato livello di protezione
- Notifiche di push per mantenere l'utente informato dell'operatività

Nuove banche esempio: Number26

Signup di un nuovo utente:



Identificazione dell'utente gestita tramite verifica del passaporto

Sistemi di pagamento esempio: Sum Up

Genesi:

- Fondata nel 2012
- 100 dipendenti c.a

Servizi:

- Pagamenti mPOS (certificazione Europay, MasterCard, Visa (EMV) e PCI-DSS)

Business model:

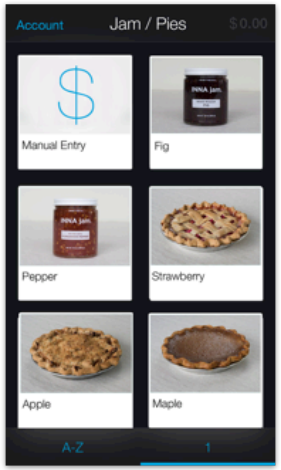
- Percentuale a transazione del 2.75%
- Nessun canone per il dispositivo POS (acquisto a 79 €)
- Payout in 1-2gg

Need di sicurezza:

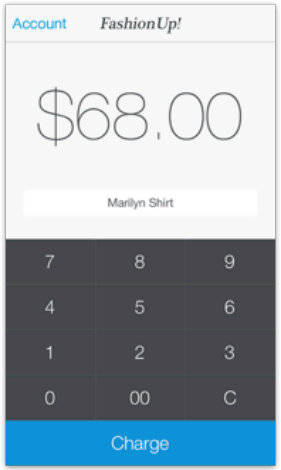
- Garantire la sicurezza delle transazioni e informazioni sulle cc
- Non degradare la user experience degli utenti mantenendo un adeguato livello di protezione
- Gestire la privacy degli acquirenti
- Garantire la sicurezza dei merchants

Sistemi di pagamento esempio: Sum Up

1a. seleziona prodotto



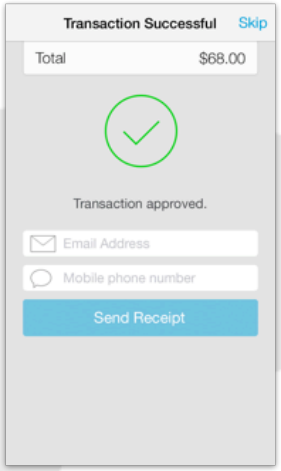
1b. inserisci prezzo



2. lettura cc

3. inserimento PIN

4. invio ricevuta



Trasferimento di denaro esempio: TransferWire

Overview:

- Fondata nel 2011
- 500 dipendenti c.a
- Supporta c.a. 300 valute movimentando c.a. 650 milioni di euro al mese

Servizi:

- Trasferimento di denaro tra paesi con valute differenti

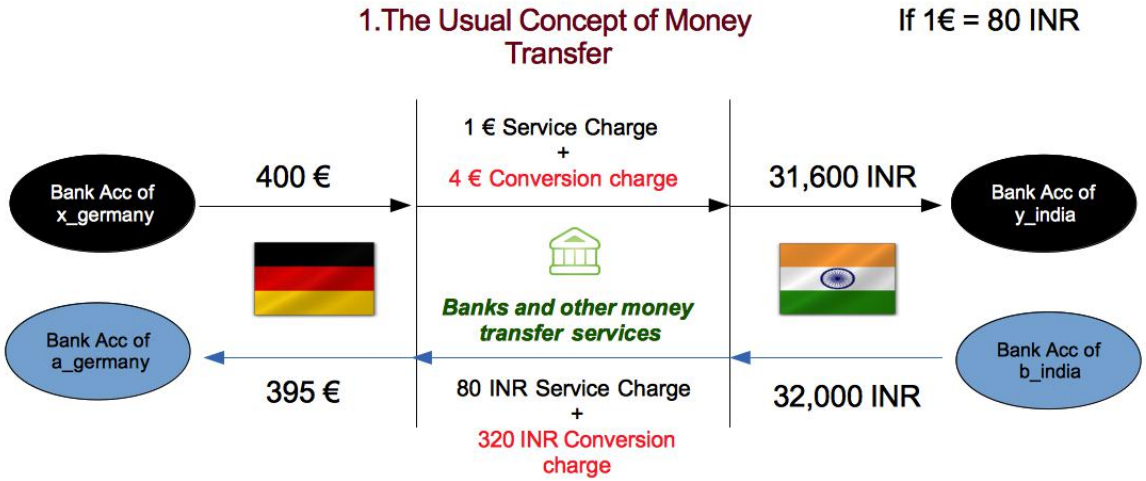
Business model:

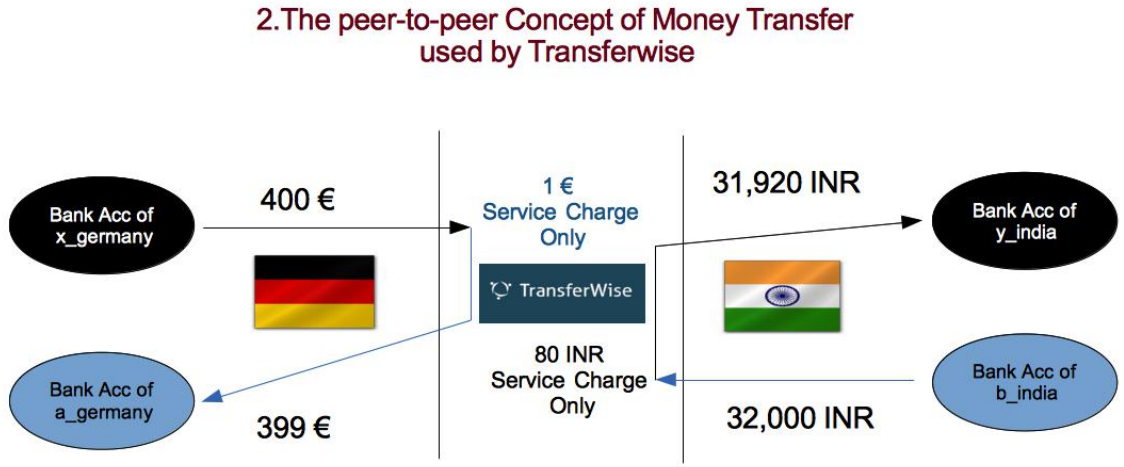
- P2P senza effettivo cambio di valuta
- Commissione

Need di sicurezza:

- Assicurare la sicurezza delle transazioni P2P
- Non degradare la user experience degli utenti mantenendo un adeguato livello di protezione
- Proteggere le informazioni legate al conto d'appoggio o cc dell'utente

Trasferimento di denaro esempio: TransferWire





Trading esempio: eToro

Overview:

- Fondata nel 2006;
- 150 dipendenti c.a;
- Oltre 4.5M di utenti.

Servizi:

- Social trading (valuta, azionario, commodities, indici e bitcoin).

Peculiarità:

- La possibilità di vedere le operazioni degli altri utenti e decidere di "*copiare*" un altro investitore nel network.

Need di sicurezza

- Proteggere gli ordini degli utenti (e la loro puntualità)
- Non degradare la user experience degli utenti mantenendo un adeguato livello di protezione
- Gestire le informazioni sui conti di appoggio e cc degli utenti

Elementi comuni

- Nuovi modelli di business e diffusione virale (social e P2P)
- Non degradare la user experience degli utenti mantenendo un adeguato livello di protezione
- Mostrarsi sicuri (il danno d'immagine dovuto ad un incidente di sicurezza può essere fatale)
- Interazione con gli utenti da remoto (nessun contatto diretto)

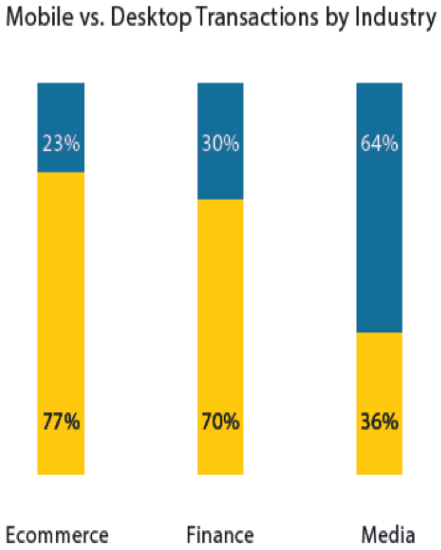
Agenda

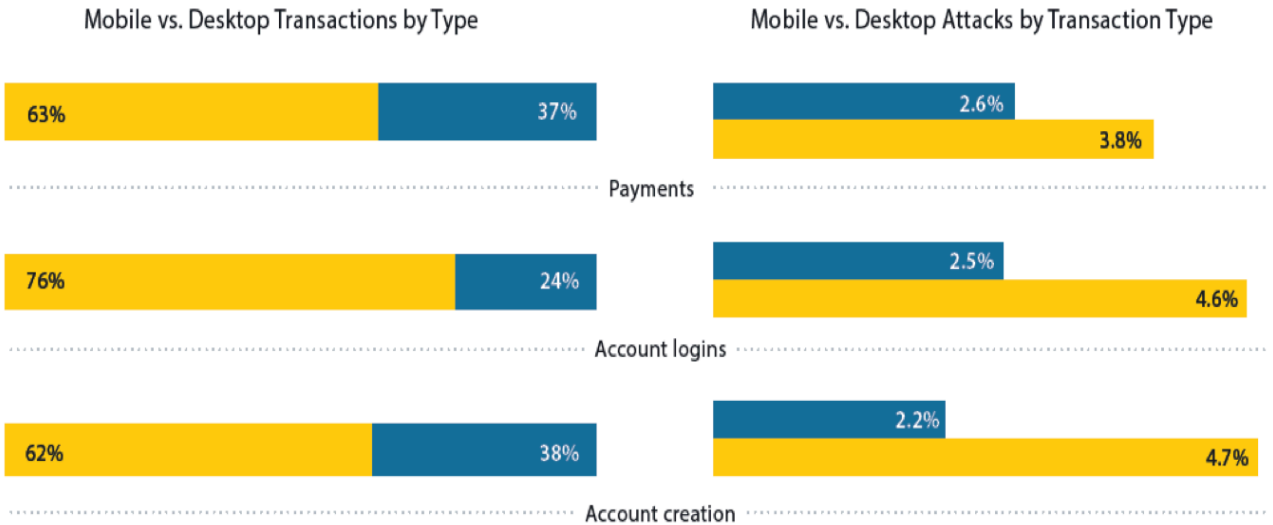
- Numeri del mobile oggi
- Nuovi servizi bancari, payment e finanziari
- **Sicurezza mobile oggi**
- Sfide per la sicurezza
- Conclusioni
- Domande

Mobile security oggi: quali minacce

- Furto di informazioni sensibili (CC, credenziali bancarie, privacy);
- Danno di immagine per il servizio;
- Ransomware (solo Android);
- Trojanized Ad-ware;
- DDoS: distribuiti verso client di servizi specifici;
- …

Trend delle minacce

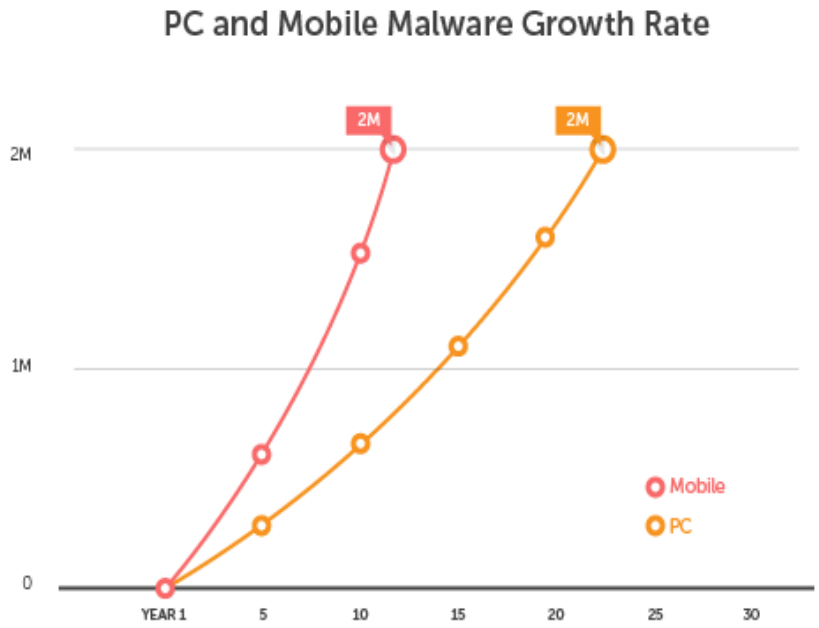


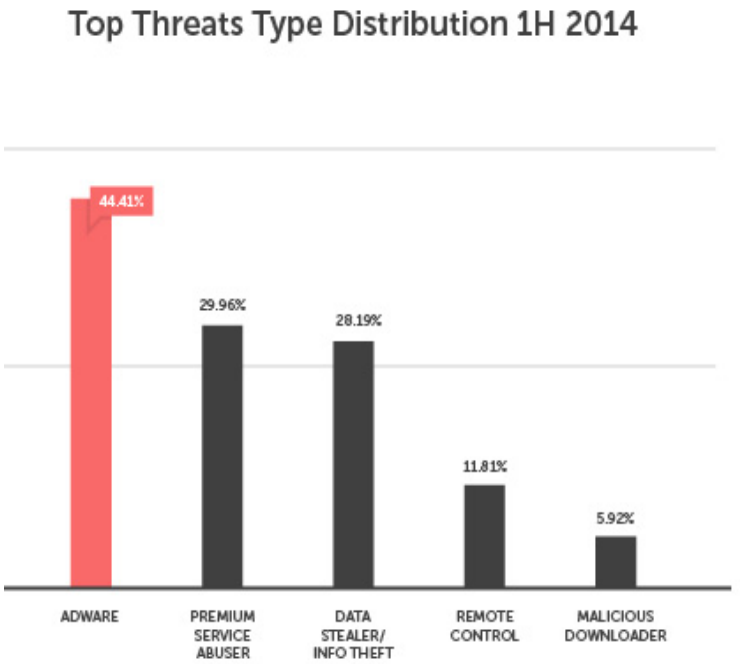


Source: ThreatMetrix Cybercrime Report 3Q2015

Trend delle minacce

Si tratta di un *trend* in rapida espansione il cui target principale sono le applicazioni ***consumer facing***





http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/the-mobile-landscape-roundup-1h-2014

Trend delle minacce

"Using mobile malware is cheaper and safer than using banking trojans for those who target personal bank accounts." *(post legato al leak del codice di* GM Bot https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/)

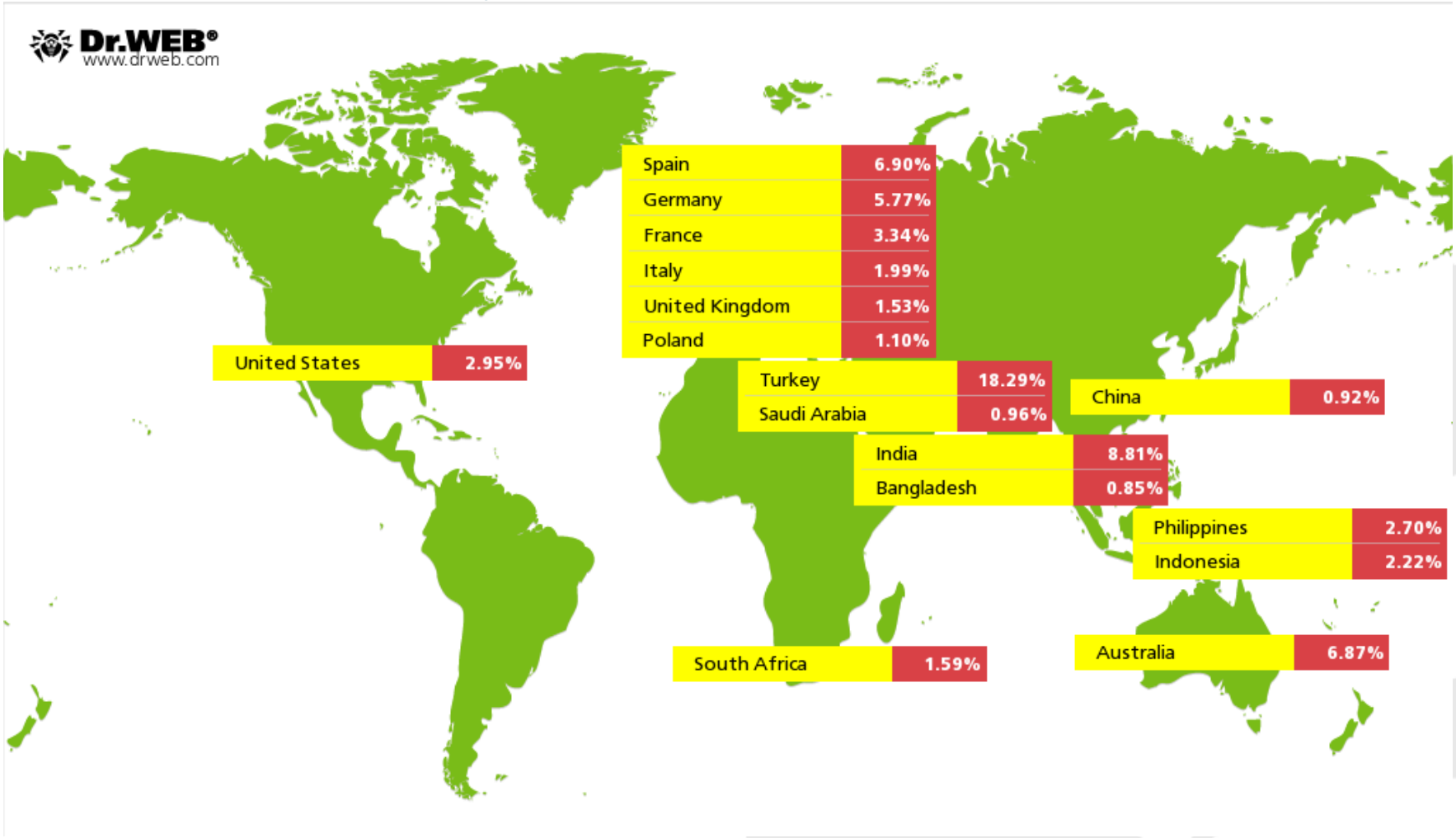
Un esempio reale

Android.SmsSpy.88.origin:

- Banking trojan scoperto all'inizio del 2014;
- Inizialmente pensato per intercettare SMS ed effettuare chiamate si è evoluto molto negli anni;
- Venduto sul black market come un prodotto compresa la sua console di gestione (al costo di pochi migliaia di euro);
- Oggi è stato specializzato su più di 100 istituti bancari;
- Presenta anche funzionalità ransomware.

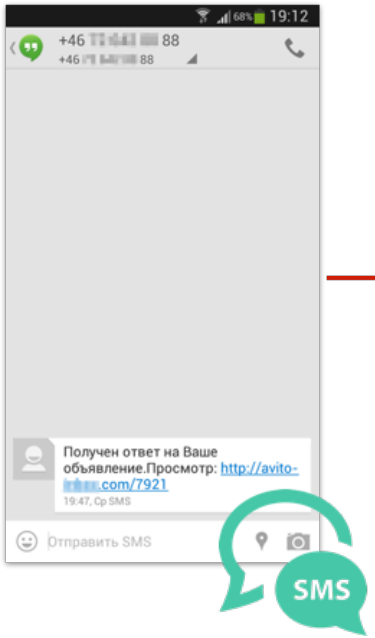
Un esempio reale: diffusione

Dati 2016: 2% in Italia (su più di 50 botnet di mobile device individuate)



Un esempio reale: installazione

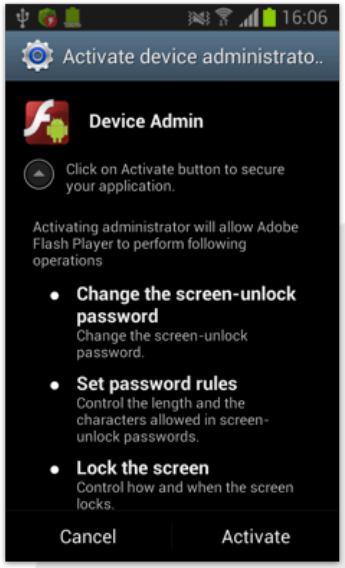
1. Link via SMS



2. Download da un server controllato dall'attaccante

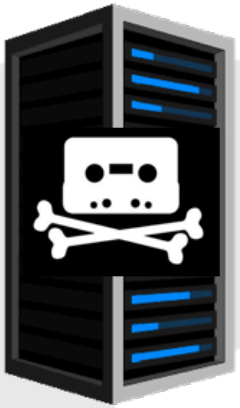
APK hosting server

3. Installazione spacciandosi per applicazione lecita



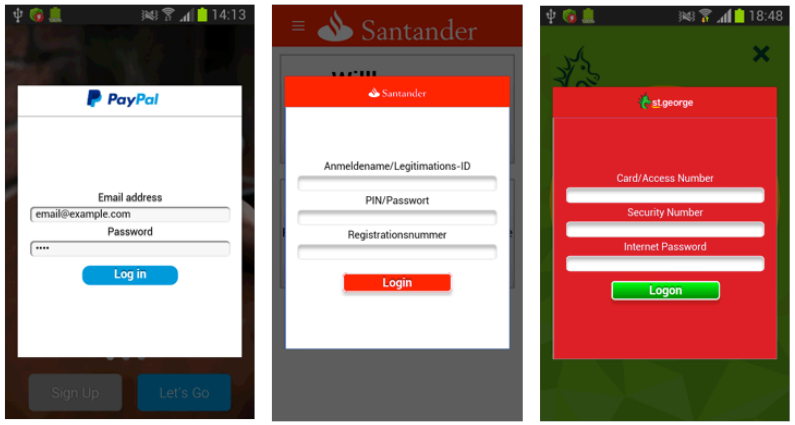
4. Identifica il device e stabilisce il contatto con server C&C

C&C server



Un esempio reale: installazione

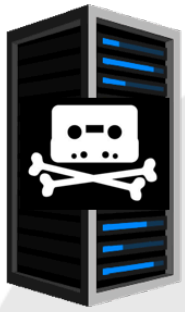
1a. non appena un applicazione target è utilizzata dall'utente il trojan si attiva, aggancia l'app e mostra un finto dialogo di login per rubare le credenziali utente



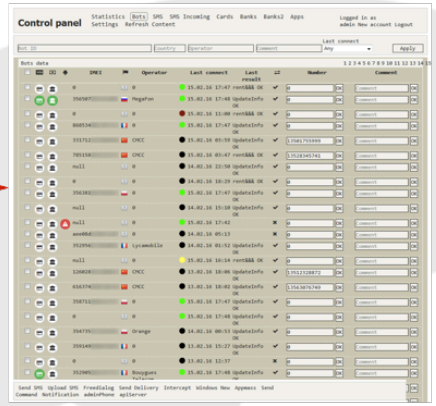
1b. lo stesso può avvenire richiedendo i dati della CC qualora il servizio target normalmente li utilizzi

2. Le credenziali sono subito invite al server

trojan backend



3. L'organizzazione controlla il dispositivo dell'utente dal control panel (botnet, ransomware)



Mobile security oggi: il nostro punto di vista

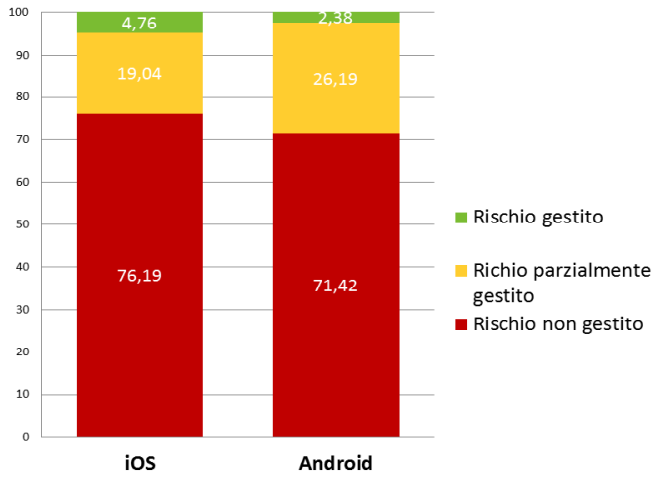
Report mobile security Q3 2015 (iOS e Android):

- Campione di applicazioni italiane ed internazionali:
  - Mobile Banking
  - Automotive
  - Home automation
  - Mobile Payment
  - Social networking
  - Entertainment
  - Enterprise management (MDM, MAM)

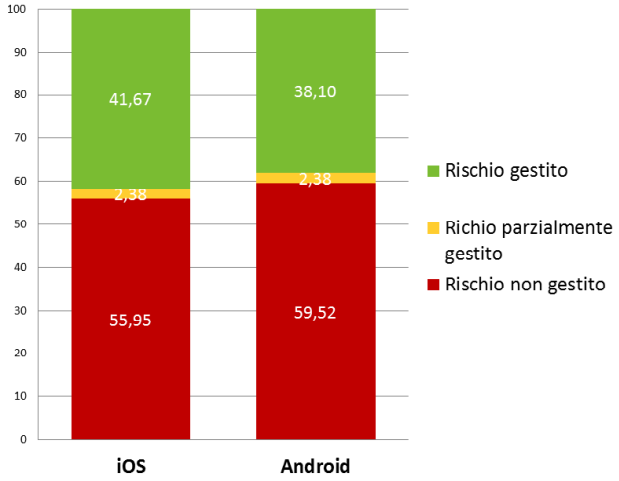
- Criteri di analisi:
  - Sicurezza run-time
  - Network communication security
  - Persistenza cache indesiderate su file-system
  - Intellegibilità delle logiche implementative
  - Informazioni sensibili nel pacchetto dell'eseguibile

Mobile security oggi: il nostro punto di vista

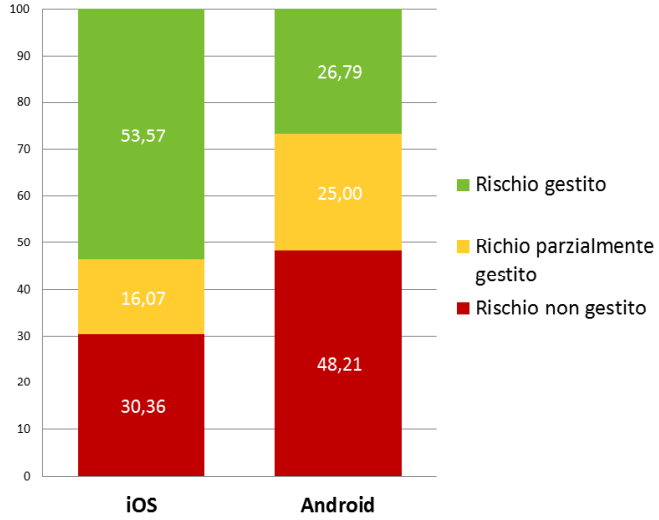
Sicurezza run-time:



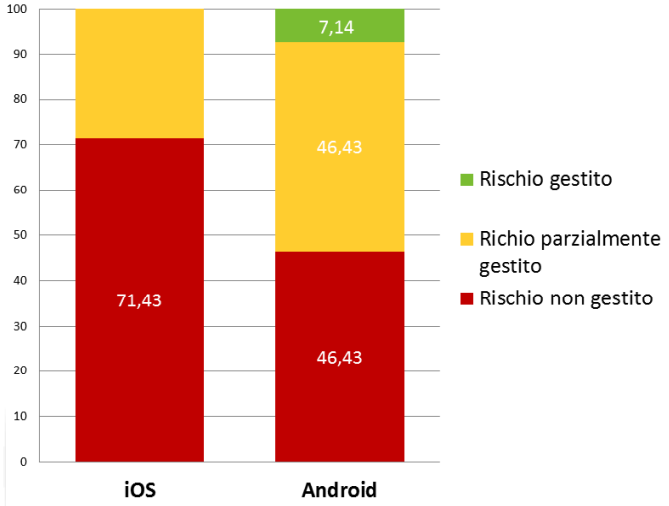
Network communication security:



Persistenza cache indesiderate su file-system:



Intellegibilità della logica implementativa:



Agenda

- Numeri del mobile oggi
- Nuovi servizi bancari, payment e finanziari
- Sicurezza mobile oggi
- **Sfide per la sicurezza**
- Conclusioni
- Domande

Mobile economy vs Security

Business needs dei nuovi servizi e modelli mobile oriented:

- User experience;
- Reputazione (dare **garanzie di sicurezza all'utente** finale evitando incidenti);
- Time to market rapido nelle evoluzioni;
- Automazione dei processi;
- Attitudine *social*.

Vs

Approccio di sicurezza tradizionale:

- Richiesta di password, 2f auth, …
- Assessment di sicurezza annuali
- Identificazione in filiale, e invio delle quantità di sicurezza via posta
- Procedure *speculari* su canali diversi

Dal punto di vista della sicurezza vi sono molteplici sfide da affrontare per permettere l'evoluzione del business senza abbassare il livello di sicurezza: sono ***necessari nuovi paradigmi***

Mobile security oggi: problematiche

- Si tenta spesso di adeguare **tecniche legate al web** alle piattaforme mobili;
- C'è un approccio spesso **DIY** (Do-It-Yourself) per gestire problematiche complesse;
- Cicli di **rilascio rapidi** portano a non permettere assessment completi delle applicazioni ad ogni aggiornamento;
- La spinta alla **semplificazione della UX** porta a dover trovare **compromessi** sulla sicurezza;
- **Cattive pratiche di sviluppo sicuro**: realtà poco formate sulle tematiche specifiche della mobile security;
- Assenza di strumenti completi a supporto delle verifiche post-sviluppo

Mobile security oggi: la risposta dei vendor

Contesti d'impiego delle soluzioni disponibili:

- **Enterprise:** dispositivi aziendali utilizzati per accesso a risorse e servizi interni
- **BYOD:** dispositivi personali che hanno anche accesso a dati aziendali (più o meno isolati)
- **Consumer:** proteggere i servizi offerti dall'azienda verso gli utenti finali (consumer)

Si tratta di mondi separati?

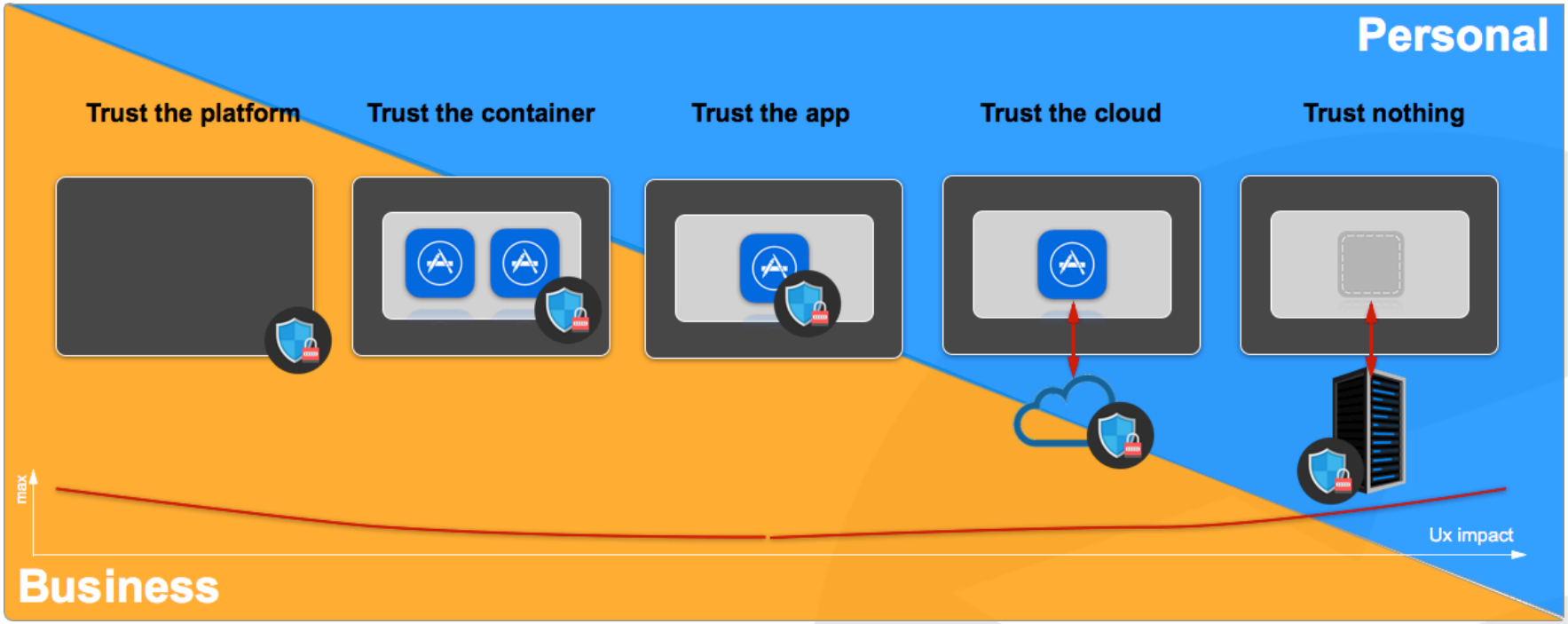
Mobile security oggi: la risposta dei vendor

Le problematiche sono comuni ma non le soluzioni:

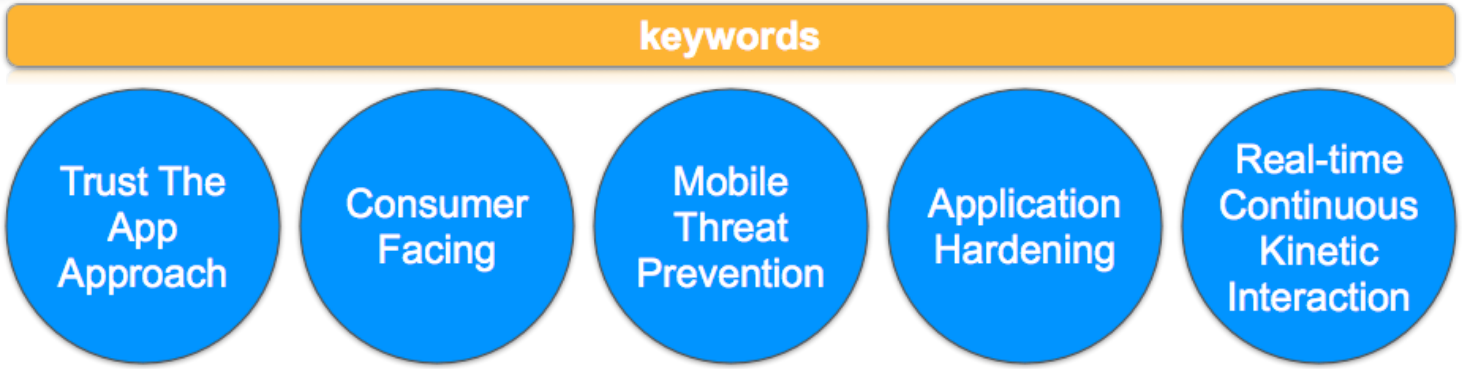
- Sono disponibili molte soluzioni diverse, spesso orientate al solo ambito interno Enterprise
- **E' necessario definire una stategia calata sulle proprie esigenze valutando l'uso di strumenti diversi.**

Mobile security oggi: la risposta dei vendor

Gli approcci alla mobile security:



MORE® il nostro approccio



Identificazione tramite Passive Biometrics

- MORE® genera una firma biometrica dell'utente basata sui fattori cinetici d'interazione con il dispositivo

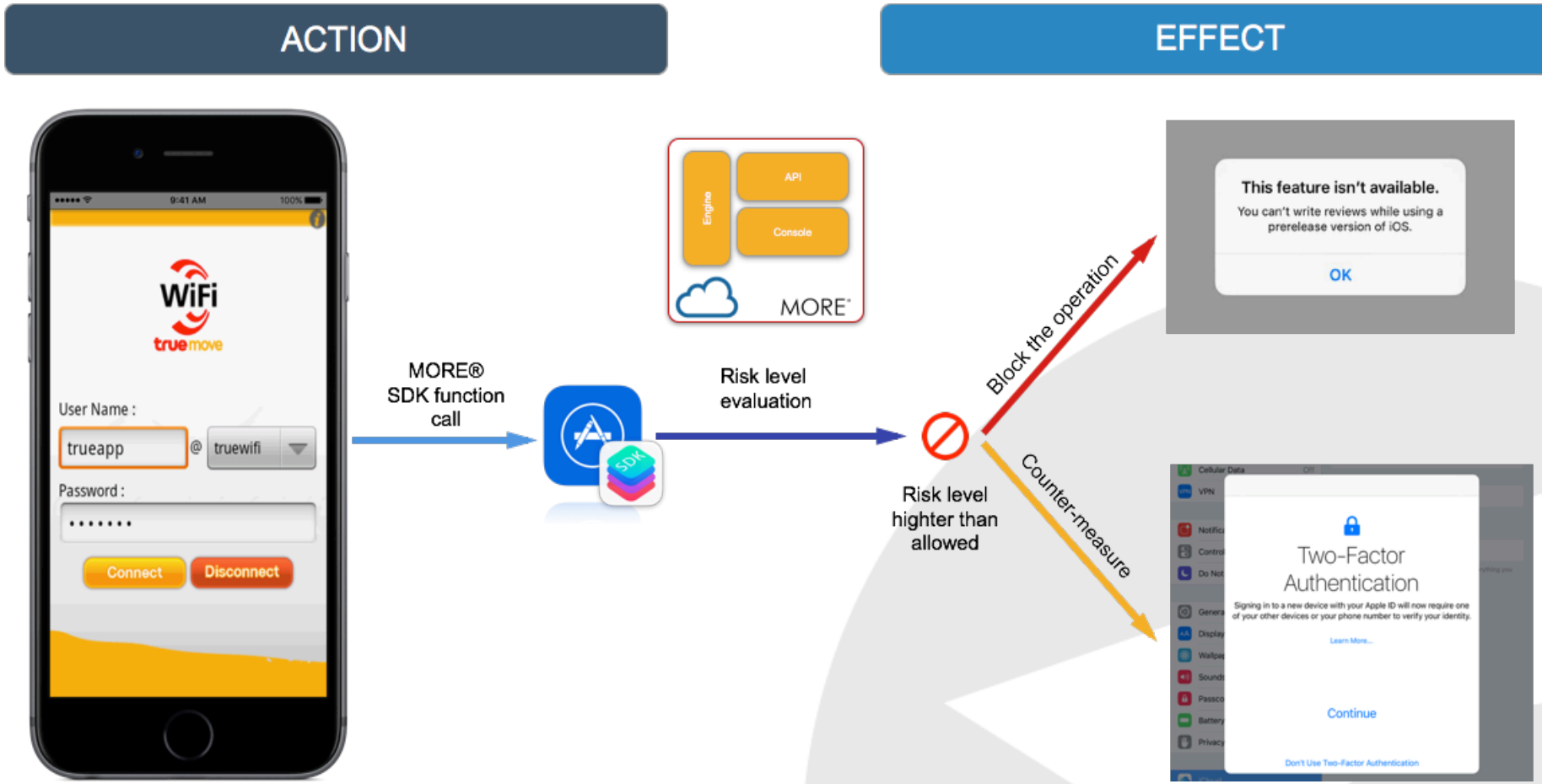
Runtime environment check

- MORE® opera in real-time valutando lo stato di sicurezza del dispositivo durante l'utilizzo dell'app

Device fingerprinting

- MORE® associa l'utente con i suoi dispositivi, valutandone le abitudini d'uso, e creando un fingerprint dei dispositivi

Use Case – Login



Agenda

- Numeri del mobile oggi
- Nuovi servizi bancari, payment e finanziari
- Sicurezza mobile oggi
- Sfide per la sicurezza
- **Conclusioni**
- Domande

Riassumendo

L'ambito bancario e payment sta subendo una trasformazione:

- Orientamento alla mobilità;
- UX semplice e intuitiva;
- Automazione dei processi d'interazione con l'utente;
- Continua e rapida risposta alle esigenze dei clienti (tramite rilasci rapidi e qualitativamente validi delle app);
- Sfida globale nel offrire servizi a basso costo ed efficienti;

Questo implica nuove sfide per la gestione della sicurezza:

- Specificità per l'ambito mobile;
- Necessità di non essere invasivi rispetto all'uso dell'applicazione
- Continua valutazione delle minaccie;
- Gestione strutturata del tema sfruttando strumenti mantenuti e affidabili .

Strategia

Cosa fare:

- Concentrarsi su **app-level security**, minimizzando il lockdown del dispositivo;
- **Esternalizzare i controlli** di sicurezza separandoli dalla business logic dell'applicazione;
- Mantenere le strategie di protezione **B2B e B2C separate (**non è sempre possibile risolvere problemi caratteristici di ciascun contesto in modo uguale)
- Proteggere le applicazioni mobile con l'obiettivo di **favorire la usabilità** senza rinunciare ad **un livello di sicurezza adeguato** (ne dipende il successo dell'app).

Cosa non fare:

- Bloccarsi in strategie a lungo termine: la continua evoluzione richiede agilità;
- Ingaggiare approcci di sicurezza che cerchino di imitare la sicurezza su web o PC;

Agenda

- Numeri del mobile oggi
- Nuovi servizi bancari, payment e finanziari
- Sicurezza mobile oggi
- Sfide per la sicurezza
- Conclusioni
- **Domande**

Domande

www.iks.it
informazioni@iks.it
049.870.10.10

appassionati all'eccellenza