IPA Better Life with IT

ハードウェア脆弱性評価の最新技術動向に関するセミナー
— black hat/CARTES参加報告 —

2016年2月4日

独立行政法人　情報処理推進機構
技術本部 セキュリティセンター

概要紹介

概要紹介

- black hat EUROPE 2015
  - コンピュータセキュリティの国際カンファレンスであり、市場に出回っているもの（製品）への攻撃事例が報告される。EUROPE以外にASIA、USAがある。
  - AMSTERDAM RAI, NETHERLANDS
  - 2015/11/12～11/13、参加者1500人
  - （11/10～11/11は実践的な攻撃のトレーニングが行われた。これには不参加。）

概要紹介

- black hat EUROPE 2015
  - TRAININGS：Hands-on Hardware Hacking and Reverse Engineeringなど実践的な攻撃のトレーニングが9（予定では10、参加者居ないため一つがキャンセル）
  - ARSENAL：Android Device Testing Frameworkなどのツールのデモが24
  - SPONSORED SESSIONS：展示会場でのセッションが12
  - BRIEFING：攻撃事例の紹介として40のセッション
    - 14分類：Crypto、Incident Response、Mobile、Defense、Hardware/Embedded、Network、Reverse Engineering、Enterprise、IOT、OS、Virtualization、Exploit Development、Malware、Web
    - 参加した10セッション：Crypto（3）、Virtualization（1）、Mobile（1）、Web（1）、Enterprise（1）、Hardware Embedded（2）、Incident Response（1）

概要紹介

- black hat EUROPE 2015 | BRIEFING
  - 最初のKeynote：
    - 「ネットワークのブレーク、サイバーセキュリティが課題」
  - 個別の報告事案：
    - システムへの攻撃事例が多い。Windows、Linux、AndroidなどOSのパスワード認証のバグを突いて攻撃する方法、Office、Yahoo Mail、Twitterなどアプリケーションのセキュリティ設定ミスによる脆弱性に関するもの。ただし攻撃が成功したことは当該ベンダーに報告済みであり、ベンダーも対策品をリリースしているので実害はないと報告されていた。
    - 数件であるがICチップのハードウェア、車の自動運転システムに関する報告あり。ただしJHASやJTEMSの議論から比較すると表面的。
    - Blackhat sound bytesと称して対策案、回避案を提示。
  - 最後のLocknote：
    - 「セキュリティエンジニアがもっと必要」
    - 「セキュリティポリシーが製品に反映されてない」
    - 「セキュリティコミュニティで経験と技術を広く共有することが必要」

概要紹介

- CARTES | The Global Event for Payment/Identification/Mobility
  - IDカード、Paymentなどに関する国際カンファレンスであり、市場動向に関する展示や事例報告がなされる。2015年で30周年。
  - Paris Nord Villepinte, France
  - 2015/11/17～11/19、参加者15,090人、参加企業394社（82%がフランス外）
  - CONFERENCE：4つのシリーズ、計84セッション
    - Biometrics & eID Key Trends
      - このセッションに参加
    - Navigating the Mobile Contactless Payment Landscape
      - NFC、HCE、SE、Tokenization
    - Fighting Fraud & Ensuring Privacy
      - EMV、Wearable
    - Money on the Move
      - E-money、M-money、MPOS

概要紹介

- CARTES | The Global Event for Payment/Identification/Mobility
  - もはやICカード、IDカード単体の話は無く、それらを使ったシステムの話、使い方（適用事例）の話、標準化の話に移行。会場にはV2Cloudの実車まで展示。
  - 生体認証の先進国であるアメリカでは指紋認証が主流。今回のCARTESでの報告は、顔認証、音声認証、指紋認証、サインが従来のパスワードとあわせて使われる事例。精度向上のために複数の生体認証を組み合わせているのが理由だが利便性、標準化に課題。
  - 現在の生体認証普及率（20%）での課題として、
    (1)対処すべきアプリケーションが多すぎる、
    (2)キラーアプリがないのでユーザがシフトしない
    などといった点が指摘。
  - 展示のないブース、当日キャンセルのカンファレンスが目立つ。

トピックス

black hat トピックス
2014年～今回までの話題の傾向

US2014	EU2014	US2015	EU2015
開発者がセキュリティの背景を知らない	ネットワーク解析の自動化	機械学習	通常のツールに潜む脅威
マルウェア追跡ボット →	脆弱性検索&バックドアツール →	カーネルバグをファジング →	自動化ツール操作ミスの脅威
車リモート攻撃 →		車載ラジオのハック →	自動運転車への攻撃
Bad USB →	スマートメータ、ATMへの攻撃 →	スマートカードのリバースエンジニアリング	
IntelCPUのメモリ競合回避命令 →	OSXの解析 →	iOSファジング X86のバグ TrustZone（ARM）の脆弱性ツール →	グリッチ攻撃
難読化の提案 →	難読化コードの解析 →	難読化コードの解析と改ざん →	WBC攻撃
ASLRバイパス →	回避して不正コードをロード →	クラウドサーバのデータ解析 →	クラウドサーバでのASLRバイパス

black hat トピックス
Unboxing the White-Box（Riscure）

- White-Box Cryptoとは
  - 安全でない環境で鍵を守るための実装
  - http://crypto.stanford.edu/DRM2002/whitebox.pdf
  - コントロールフローの難読化
  - データフローの難読化
  - デバッガモードの検出
  - デバッガフックの検出
  - デバイス固有の鍵込みで実装

同じアルゴリズムでもデバイスによって実装が異なる。ルックアップテーブルを切り替えることで実装。

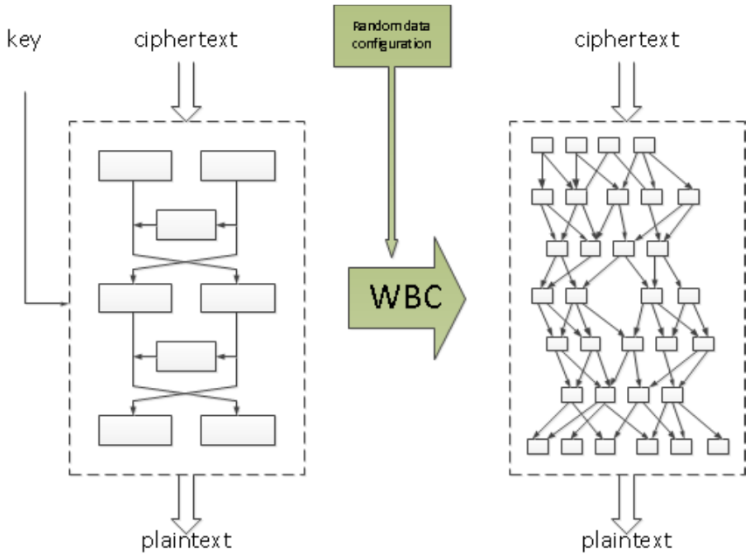
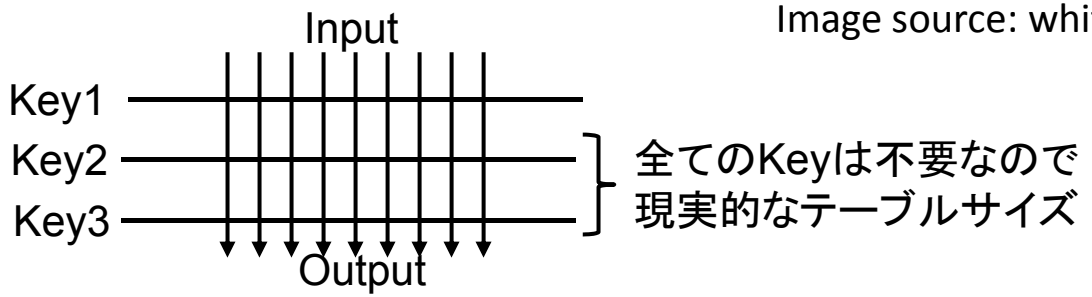


Image source: whiteboxcrypto.com



black hat トピックス
ホワイトボックス暗号 （Riscure）

- White-Box Cryptoに対するDFA、DPA
  - 難読化したWBCは、リバースエンジニアリングには強いが、DFAやDPAに無力（2014年のRiscure社Workshopでは耐性が懸念されていた）

中間値の改変に依存した出力の変化があればDFA可能。
コードの途中に故障注入で出力が変化するなら、入力を変えて、正しい答えと誤った答えが得られる。

秘密情報の処理に依存した情報のリークがあればDPA可能。
乱数の入力で入出力値のペアを集める。正しい仮定と誤った仮定に分類して差分を取る。

RAMBUS BLOG
にも書かれている。

http://www.rambusblog.com/2015/12/16/security-breaking-software-based-white-box-cryptography-wbc/

- 対策
  - 乱数によるマスキング
  - コーディングでダブルチェックを実装
  - CRC付きでオペレーション
  - 故障の伝搬を途中で止める（出力に影響させない）
  - スタック変数のアクセスによるアドレスリークにはダミーアクセス

black hat トピックス

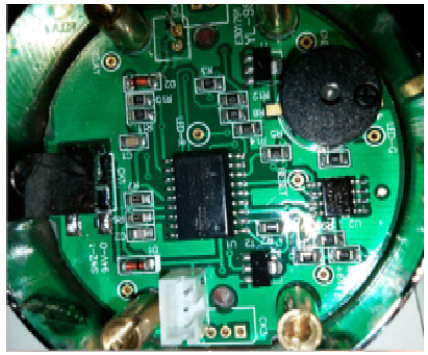
Implementing Practical Electrical Glitching Attacks (NCC group)

- アタックの対象
  - 認証チェックのプログラム
  - 境界チェックのプログラム
  - メモリのリード/ライト
- グリッチアタックの結果
  - 命令のスキップ
  - データリード/ライトの失敗
  - 命令デコードの不正
- グリッチの種類とその影響
  - クロックグリッチ　→スパイクの挿入、周波数の変更
  - 電源グリッチ凹型　→命令実行の不正、遅延の増大
  - 電源グリッチ凸型　→ダメージ、フローティング信号の変化

2015年BrightSightセミナーでは、クロックやリセット信号にグリッチを入れてセキュリティ機能をoffにできることが紹介されている

black hat トピックス
グリッチアタック （NCC group）

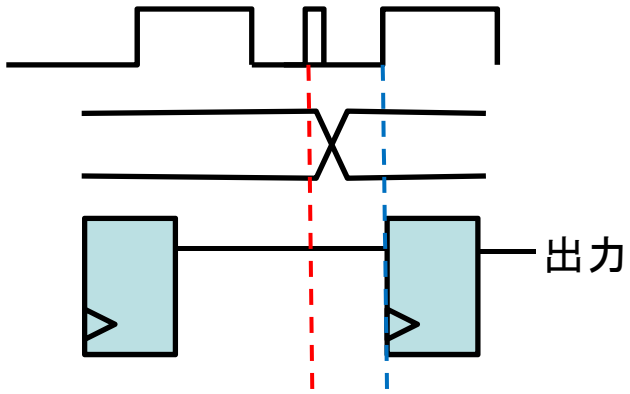
- 報告のあった攻撃の対象
  - Xbox 360
    ブート時にハイパーバイザーがロードされる。ここでCPU_PLL_BYPASS信号にグリッチ印加して命令スキップ。その後POST-BUS（ダイアグバス）に0x36コードをダミー注入
  - ATMega328p
    ロングループのコードにクロックグリッチでループを抜けた。
    Vccに凹型グリッチを印加。しきい値に個体差があった。
  - LPC1343（ARMボード）
    クリスタルとキャパシタを外してクロックグリッチを印加
  - Door Lock
    電源ICが見える
  - Intel Galileo
    電源IC、クリスタルが見える
  - Set top box
    クリスタル、Vccレギュレータ、キャパシタが見える



https://www.blackhat.com/html/archives.html

black hat トピックス
グリッチアタック （NCC group）

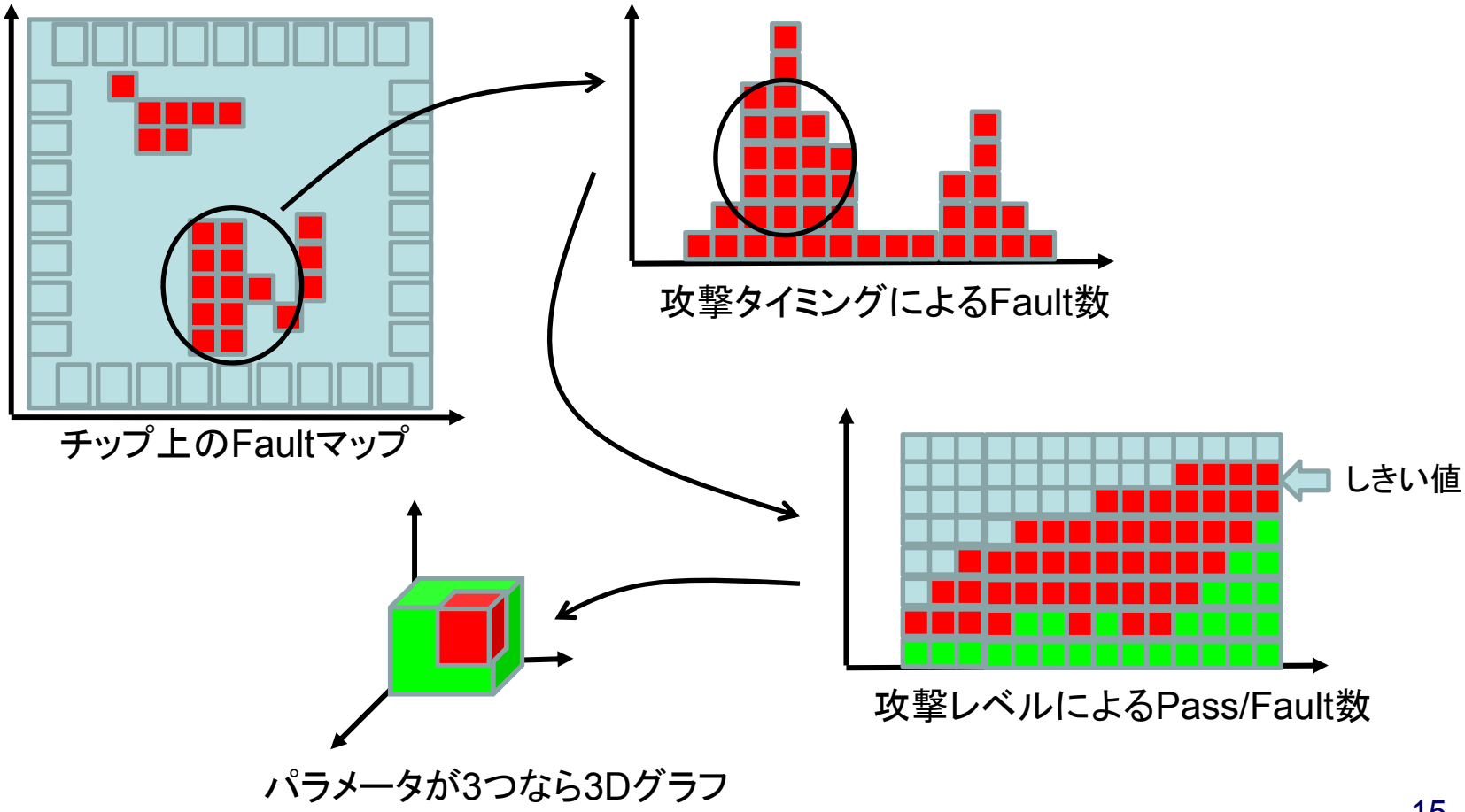
- グリッチアタックの手順（攻撃者の行動パターン）
  - 公開仕様書からアタックターゲットを決める
  - 動作範囲、セキュリティ機能などのしきい値を探す
    - 1クロックより長い命令、かつ、ライトバックのある命令がクリティカル
    - グリッチの幅、挿入タイミングなどの条件出しを行う
  - マニュアルでグリッチを入れて結果の確認
  - 繰り返し攻撃のためにFPGAで自動化環境作成
  - FPGAを使って条件出し（結果をサンプリングできること）



異常クロックを原因とするFaultの分解
遅延によるセットアップ不足
フリップフロップ出力の反転
想定外入力による想定外動作

black hat トピックス
グリッチアタック （NCC group）

- しきい値を求めるためのFIAのツールの例
  - パラメータをスキャンしグラフ化する



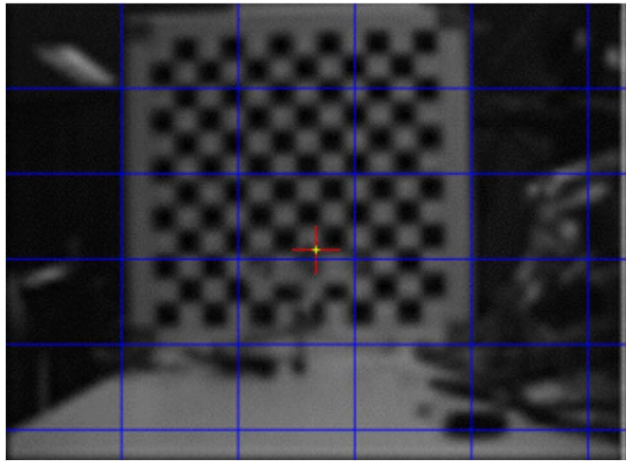
black hat トピックス
グリッチアタック （NCC group）

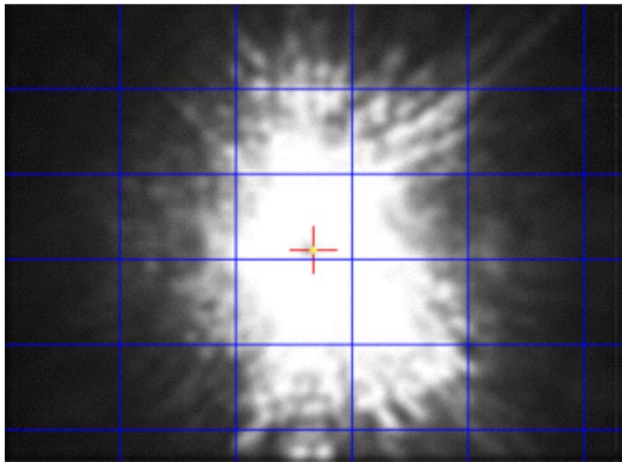
- 対策
  - グリッチ検出
  - 二重化（冗長化）
  - クロックやリセットのドメイン分離
  - ロックステップ
  - 不当命令検出
  - カナリア
  - 不要なダイアグ信号の無効化
  - 非同期
  - 内部クロック
  - DIFT (Dynamic Information Flow Tracking)
  - CFI (Control Flow Integrity)

black hat トピックス

Self-Driving and Connected Cars (Security Innovation)

- カメラへのアタック
  - MobilEye C2-270
  - レーン認識
  - 後方接近警告
  - 歩行者接近警告
  - フラッシュだと
    6秒くらい目くらまし状態





- 対策
  - カメラの追加（部分、全体）
  - レーザーのセンサー
  - 脅威対策が実装されるまでは
    自動運転を信用しないこと

https://www.blackhat.com/html/archives.html

black hat トピックス
自動運転車へのアタック (Security Innovation)

IPA

- ニュータイプのアタッカーはV2Xを狙う
  - BEACONのコンテンツに情報
  - センサーの情報処理部にマルウェア
  - V2Xサーバをブレークすると・・・
  - 居場所がゾーン/道レベルで判明

2015年Riscure社のWorkshopでは、Mobileの位置検出として PowerSpy

- 対策
  - アノニマス化
  - 暗号化
  - Opt-out、Pseudonym
    例えば5分ごとにIDを変更すると
    90%はトラッキングに失敗

0 8

Station ID	Sequence Number	
Timestamp		
Latitude		
Longitude		
Speed	Bearing	GPS Mode
Latitude error	Longitude error	
Velocity Error	Bearing Error	

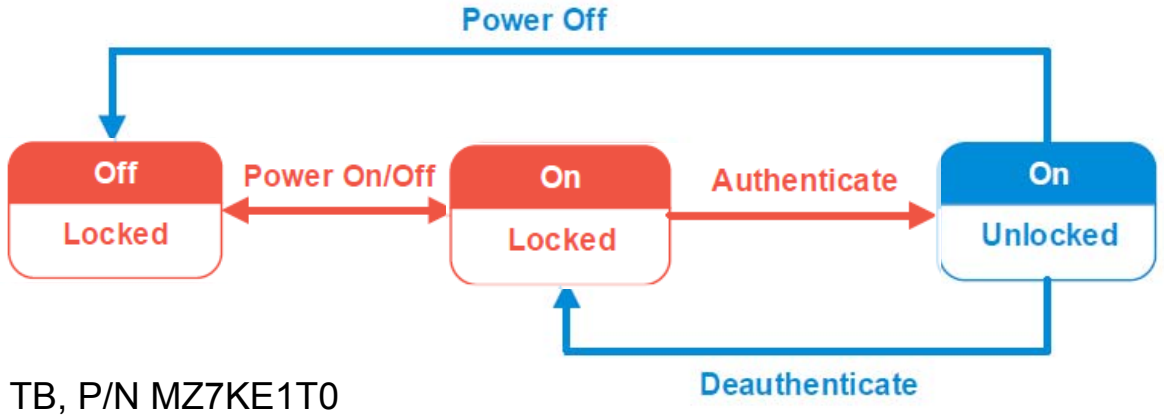
https://www.blackhat.com/html/archives.html

https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-michalevsky.pdf

black hat トピックス

Bypassing SED in Enterprise Environments (KPMG Canada)

- Self-Encrypting DriveはHDC制御のハードウェア実装。この互換性にリスクはないかと調査。
- PCがS0（on）かS3（Sleep）のときセキュアな状態でない。ここで認証をバイパスしてHDの交換が可能。



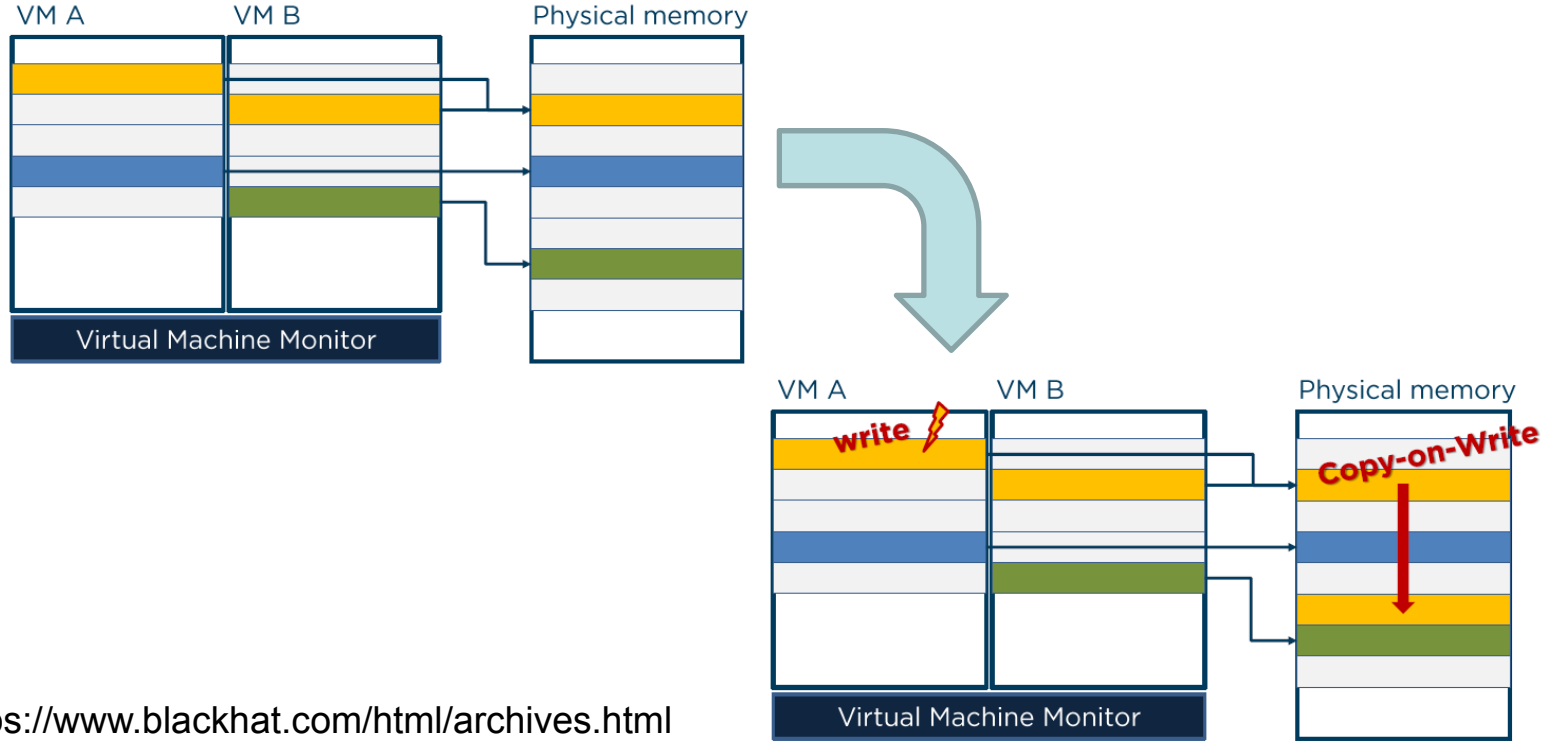
Tested Configurations
Combination of
Drives
  Samsung 850 Pro, SSD, 1 TB, P/N MZ7KE1T0
  Samsung PM851, SSD, 256GB, P/N MZ7TE256HMHP –000L7
  Seagate ST500LT015, HDD, 500 GB, P/N 1DJ142-500
  Seagate ST500LT025, HDD, 500 GB, P/N 1DH142-500
Laptops
  Lenovo ThinkPad T440s, BIOS version 2.32
  Lenovo ThinkPad W541, BIOS version 2.21
  Dell Latitude E6410, BIOS version A16
  Dell Latitude E6430, BIOS version A16

https://www.blackhat.com/html/archives.html

black hat トピックス

Silently Breaking ASLR in the Cloud (VRIJE Univ. AMS.)

- VM間で物理メモリをシェアしているとき、片方が書き込むとシェアできなくなりコピーが発生＝TA可能。
- ASLRで実装しているがTAリスクとのトレードオフ。Linuxではアタックできた。
- Hyper-Vはできなかった。



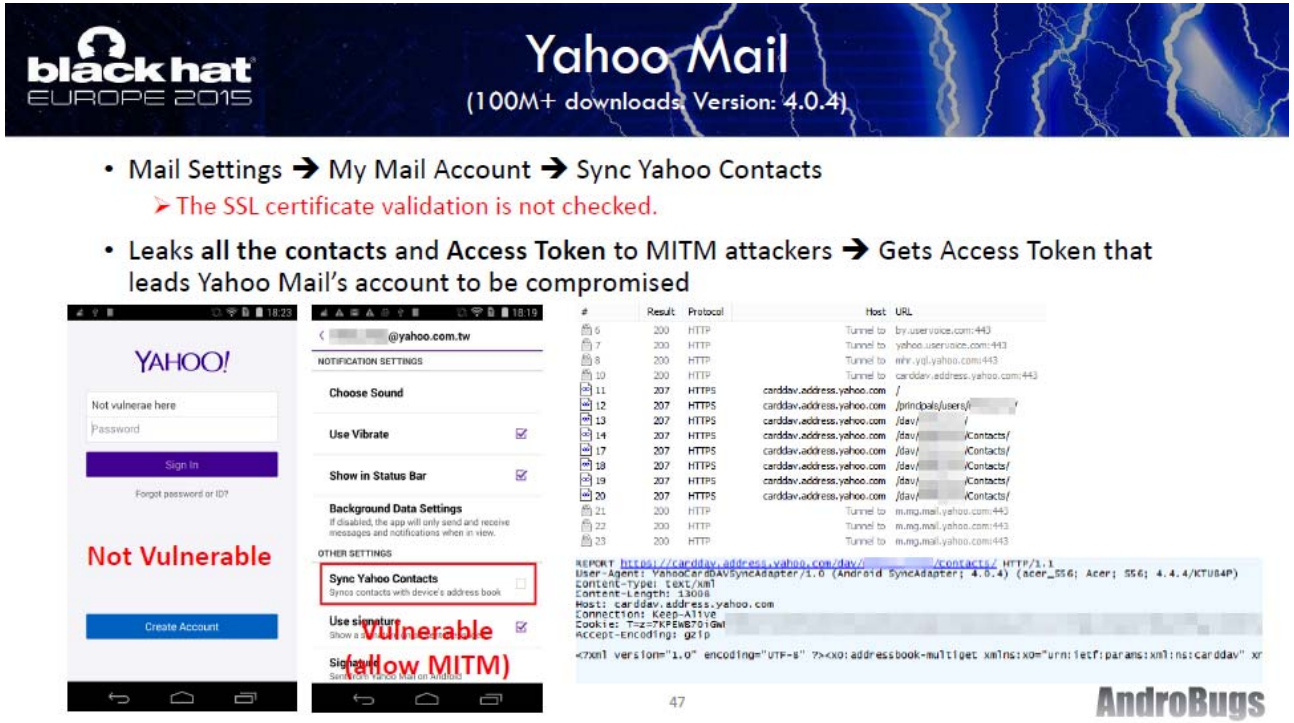
https://www.blackhat.com/html/archives.html

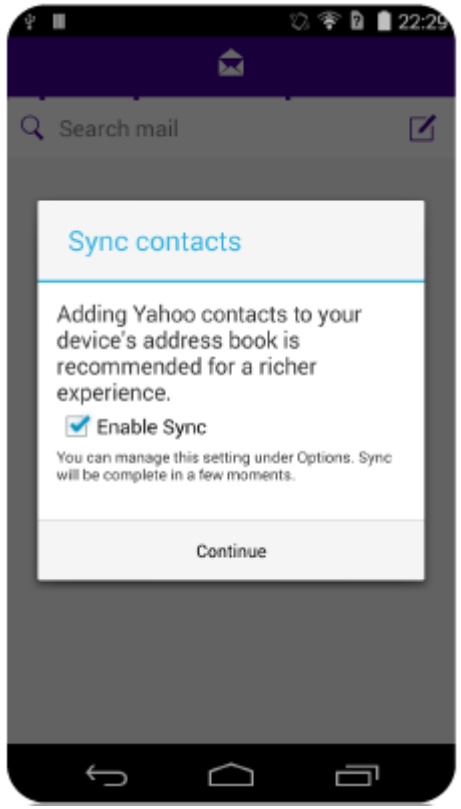
black hat トピックス

Android Application Security Vulnerability Scanner

(National Tsing Hua Univ. Taiwan)

- AndroBugsというツールを使ってInvoke-virtualなどを探す。
- MS office mobile, MS Bing, Yahoo mail, Twitterに設定ミスや登録忘れによる脆弱性を発見。
- 設計者は同じ失敗を繰り返す。





https://www.blackhat.com/html/archives.html

black hat トピックス

Detecting & Exploiting Command Injection Flaws

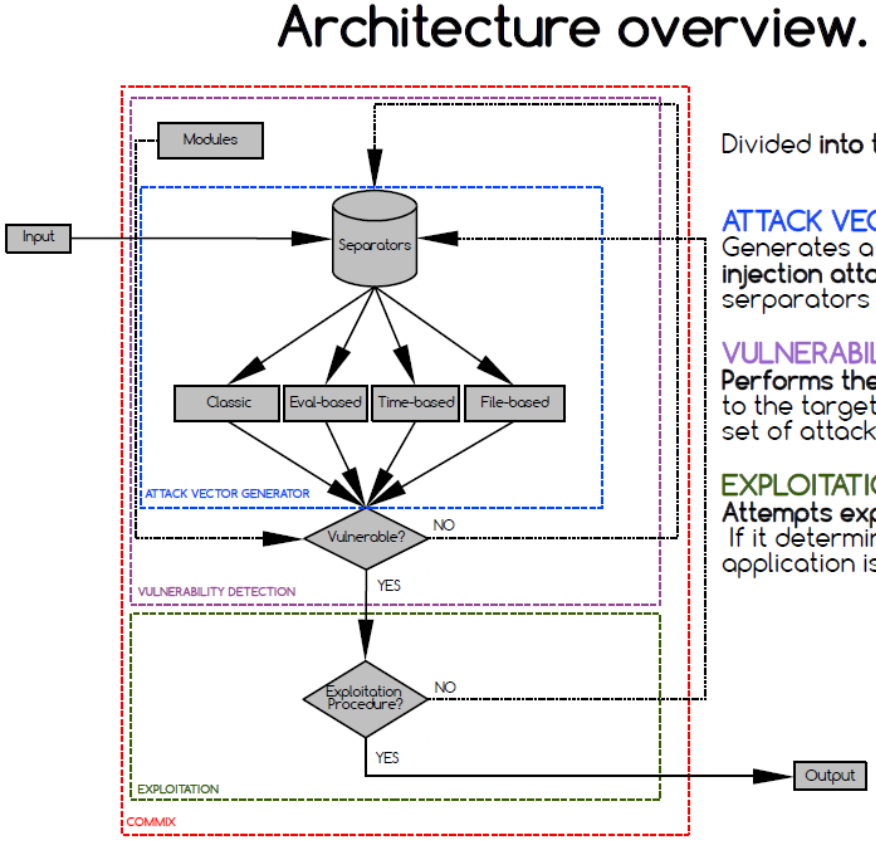
(University of Piraeus)

- Commixというツールの紹介。
- アタックベクタを生成し脆弱性を検出する。

```
ping -c 4 127.0.0.1 ; ls
```

デリミタでペイロード付加

ブラインド：invisibleにする
タイム：1秒sleepさせる
ファイル：tmp経由で・・・

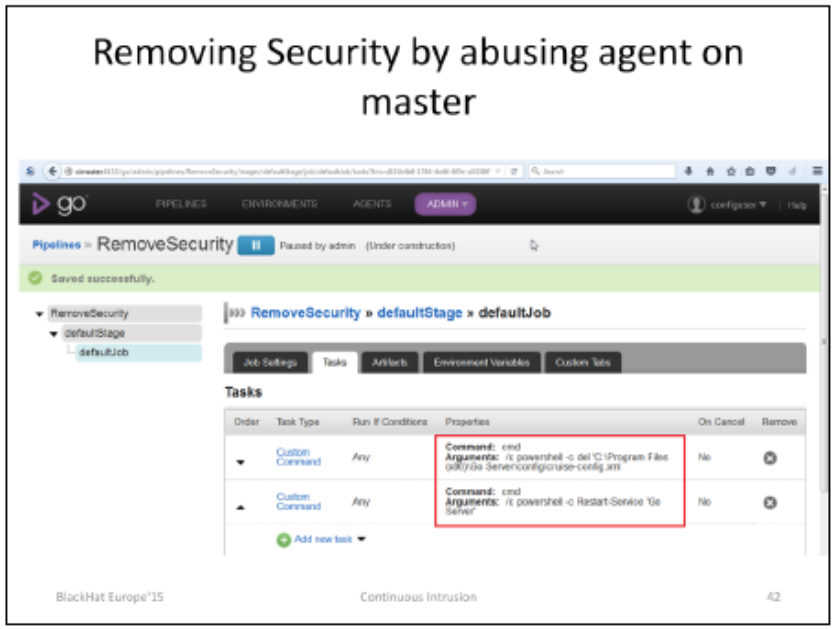


https://www.blackhat.com/html/archives.html

black hat トピックス

Why CI tool are an attacker's best friends (Hacker)

- Continuous Integrationというツール。本来はソフトウェアデリバリ、インテグレーションの自動化ツール。
- CIにはJenkins, Team City, GOなどがあるが、インストール時に認証がなく、かつ特権モードで動作するため、アタッカーが開発マシンにアクセスできれば、ソースやビルドに改変が可能。



In above, the command cmd /c powershell -c del 'C:\Program Files (x86)\Go Server\config\cruise-config.xml' will remove the configuration file of Go.
The command cmd /c powershell –c Restart-Service 'Go Server' will restart the Go Server service.
After this, all security will be removed from the Go dashboard and anyone who knows the URL will have admin rights.

Instead of removing the cruise-config.xml file, we can also remove only the <security></security> part of it and restart the Go Server service for same effect.

Or we can add the current user to <admins> in the <security> part of cruise-config.xml

https://www.blackhat.com/html/archives.html

black hat トピックス

Defending Against Malicious Application Compatibility Shims (iSIGHT)

- 普通のユーザはMSによるパッチ、EMETによるinput/outputチェックなどでShimsツールを使っている。
- Shimsが使う＊.sdbファイルを使うと偽パッチによる改ざんが可能。

```
!sdbpatch
APP=explorer.exe
DBNAME=explorer calc
# Windows 7 x86
P:explorer.exe,0x287
    R:explorer.exe,0
    R:explorer.exe,0
# Windows 7 x64
P:%windir%/explorer.exe,0x2c8af6
    MR:explorer.exe,0x202dc,48895C2410,E91F890900
    R:explorer.exe,0xB8C00,905053515256574150415...
# Windows 8 x86
P:explorer.exe,0x20e478
    R:explorer.exe,0x18408,e8f3f50d00ebf9
    R:explorer.exe,0xf7a00,906081ec8000000031c03...
!endsdbpatch
```

```
!sdbpatch
APP=malware2.exe
DBNAME=malware2
# Target:    P:  target name, checksum
# Replace:   R:  module, RVA, hex of bytes to write
# Match      MR: module, RVA, bytes to find, bytes to write
P:malware2.exe,0x13a48a90
    R:malware1.exe,0x2020,0c4b8b581c01d38b048b01d0894424ea0
!endsdbpatch
```

https://www.blackhat.com/html/archives.html

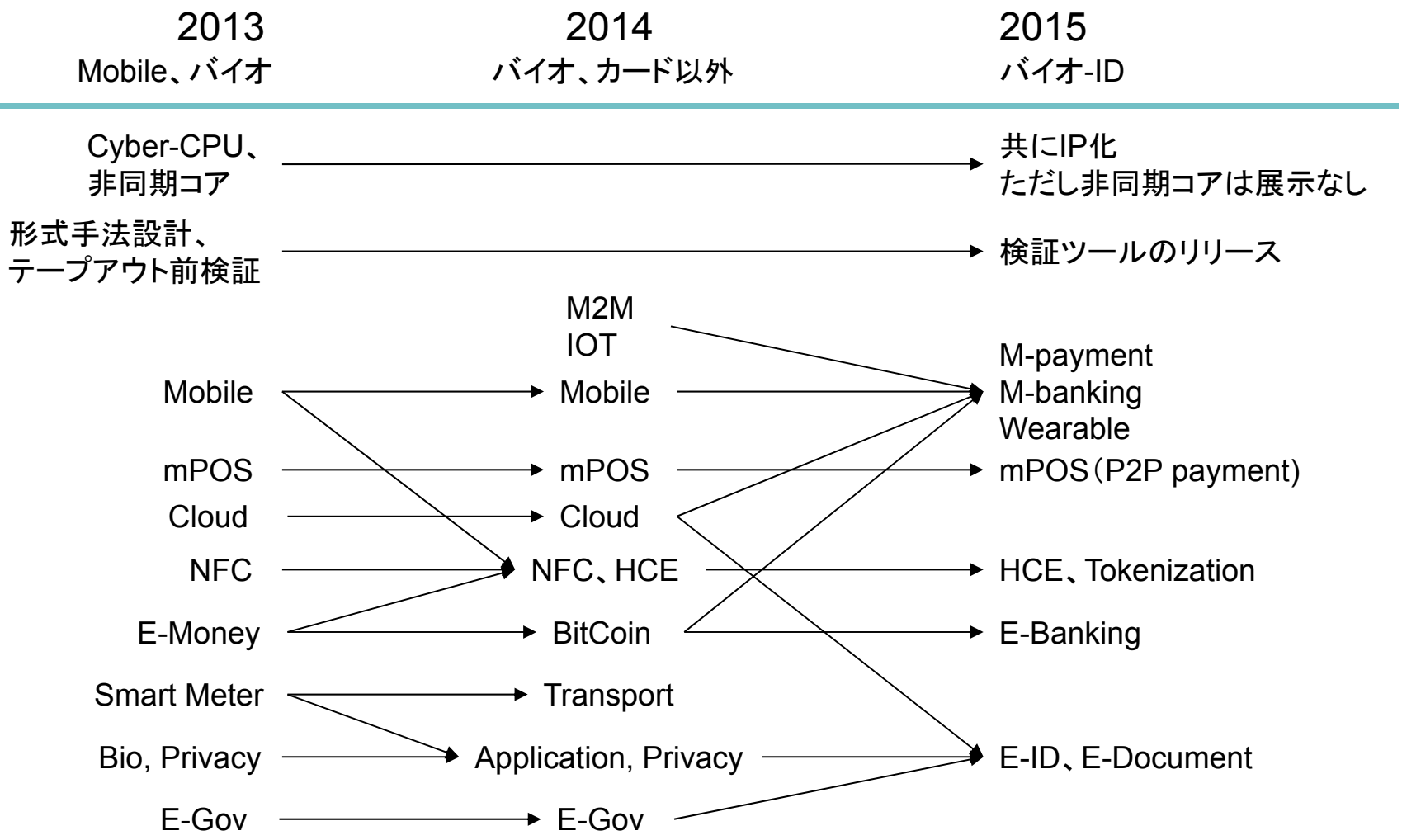
black hat トピックス

Bypassing Local windows Authentication to Defeat FDE (Synopsys)

- パスワードは暗号化して保存されている。ブート時の入力パスワードはドメインコントローラが比較し、OKならマシンパスワード（秘密鍵）を生成して共有する。
- ドメインコントローラはドメイン変更をケアしていないので秘密鍵が共有されたまま。Windows7、8.1、10でテストした。
- Microsoftからパッチがリリースされているのでアップデートすること。

https://www.blackhat.com/html/archives.html

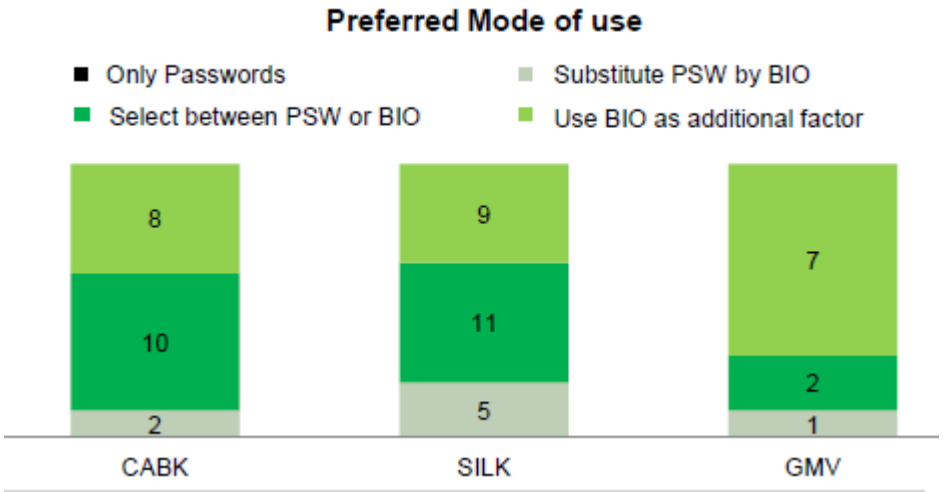
CARTES トピックス
2013年～今回までの話題の傾向



CARTES トピックス
Biometrics in Financial Services (CaixaBank)

- 指紋認証のトライアル
  - 最大の障害は何か？
    - プロバイダの技術
    - プライバシー
    - Bio認証の正確さ
    - 規制
    - 標準化
    - 脆弱性が不明

これらをリスクと感じている



Conclusions:

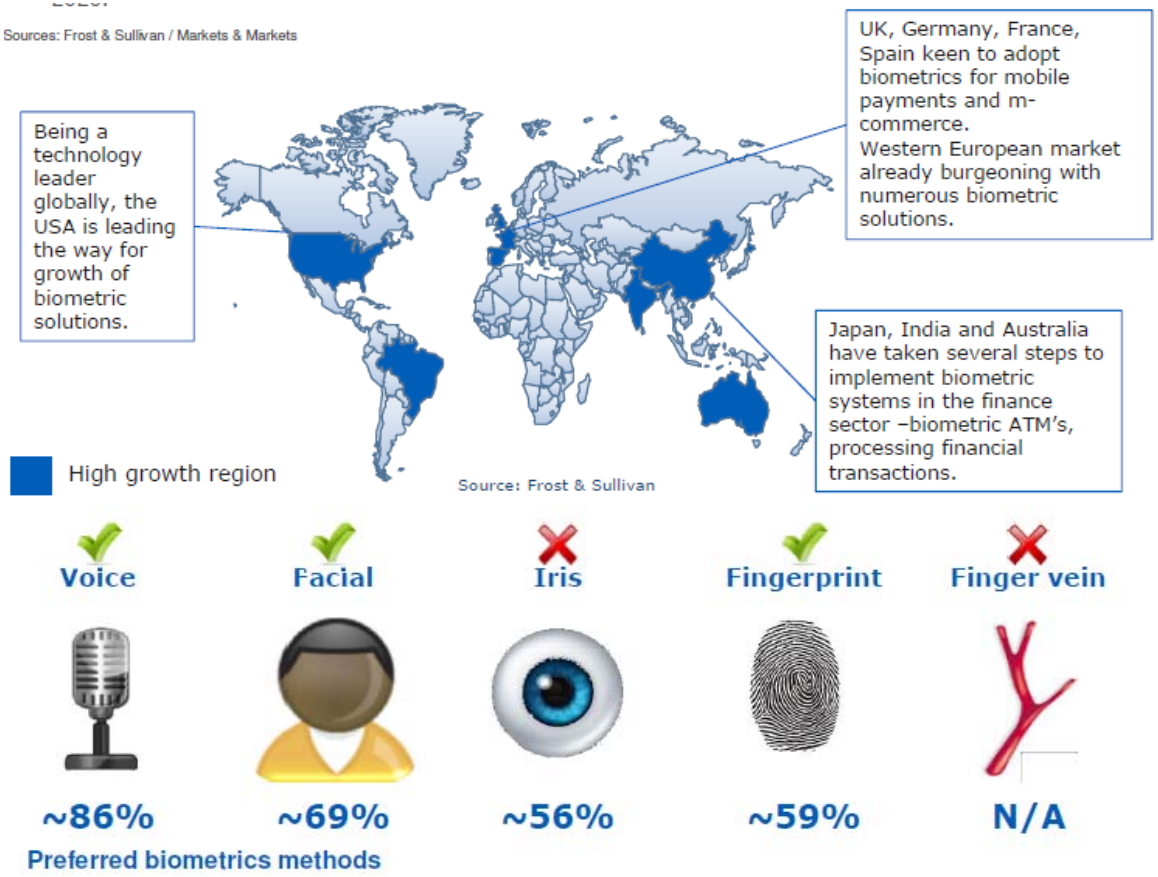
- Everyone accepted use of biometrics to improve security of passwords.
- Majority of respondents selected biometrics as more faster than passwords.
- Everyone consider biometrics easy to use.

出展：CARTES2015カンファレンス資料

CARTES トピックス

Biometric Authentication to Replace Password (United Biometrics)

- 認証全体の20%がバイオ認証。
  - パスワードより強いものをユーザは望んでいる。
  - 利便性ではビヘイビア（音声）にアドバンテージあり。
  - コストでは指紋。
  - 銀行、大企業で独自導入のため、標準化するには対処すべきアプリが多い。



出展：CARTES2015カンファレンス資料

CARTES トピックス
Revolutionizing Consumer Authentication (oberthur)

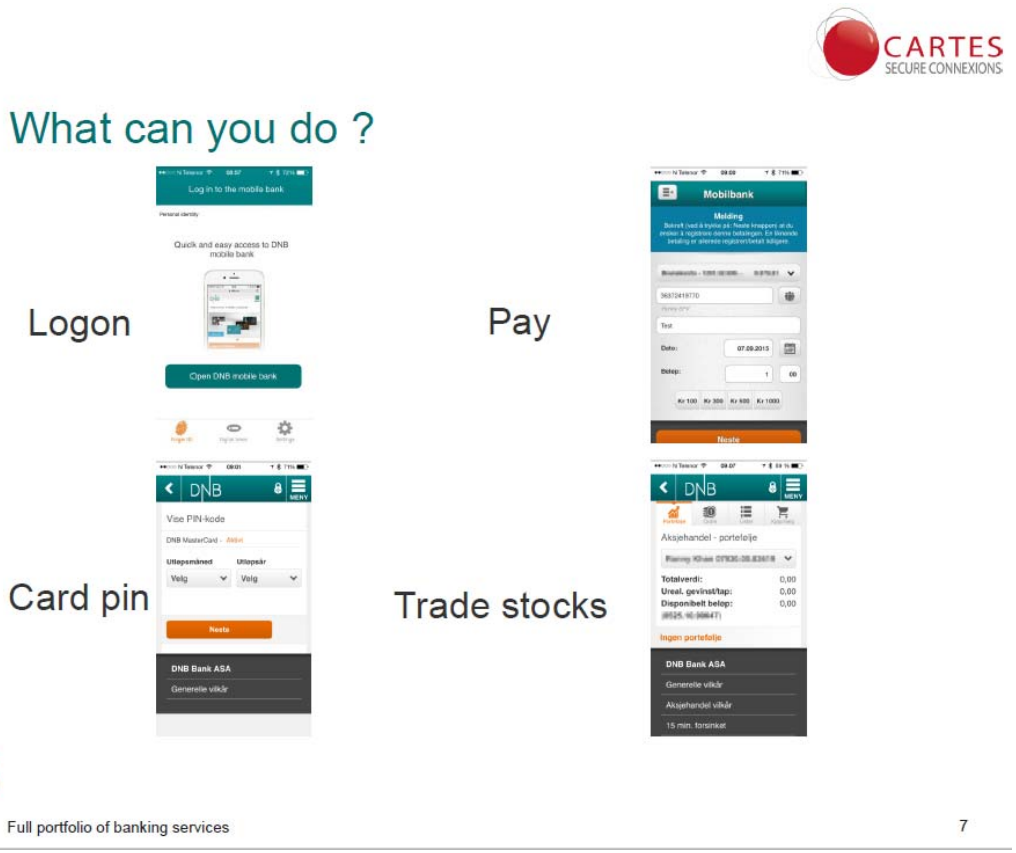
- バイオでも攻撃される。
  - ユーザ視点では「今のPINより悪くならないこと」。
  - 他人でもPIN入力可能。これを避けたい。
  - ビヘイビア（声、サイン）と物理（虹彩、顔、指紋）に対する評価基準が必要。

出展：CARTES2015カンファレンス資料

CARTES トピックス

How DNB is Using Biometrics to Win Customer Trust in Mobile Banking (DNB)

- ノルウェイの銀行でアプリを提供
  - 盲目の人でも使えるように、スマホで音声ガイド、どのボタンを押すのかガイド。
  - カスタマのリアクションを聞く。Habit（習慣）に従ってアプリ動作を切り替える。



出展：CARTES2015カンファレンス資料

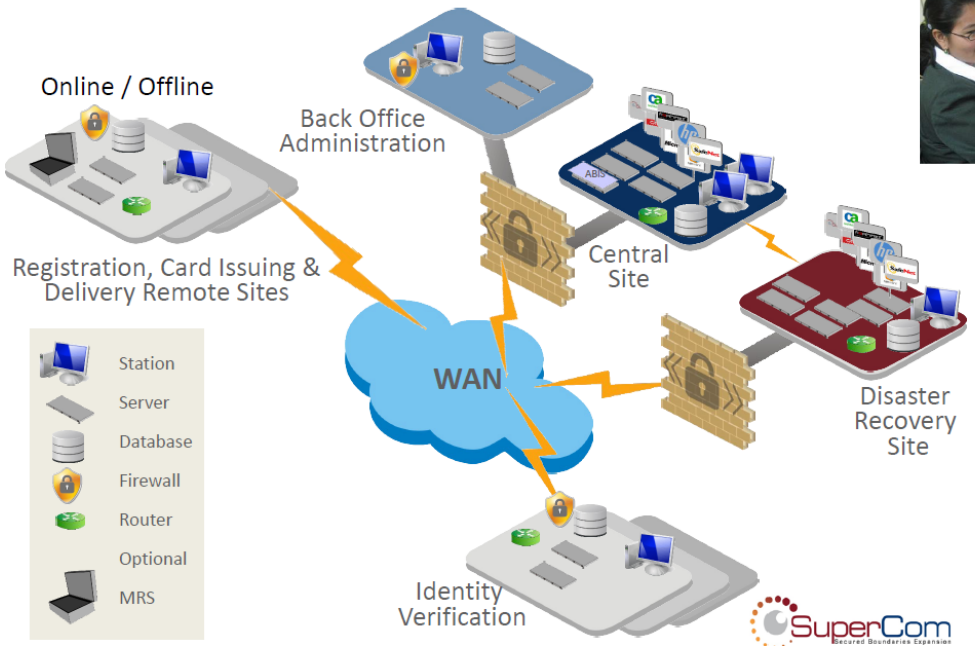
CARTES トピックス

The Civil Revolution is on the GO (SuperCom)

- エクアドルでのeIDプロジェクト
  - 3ヶ月で立ち上げる要求に応えるためオンライン、オフラインでキャプチャ。85%のレジストが完了。

A 30 Mins While you Wait Solution …

Top Level Project Architecture



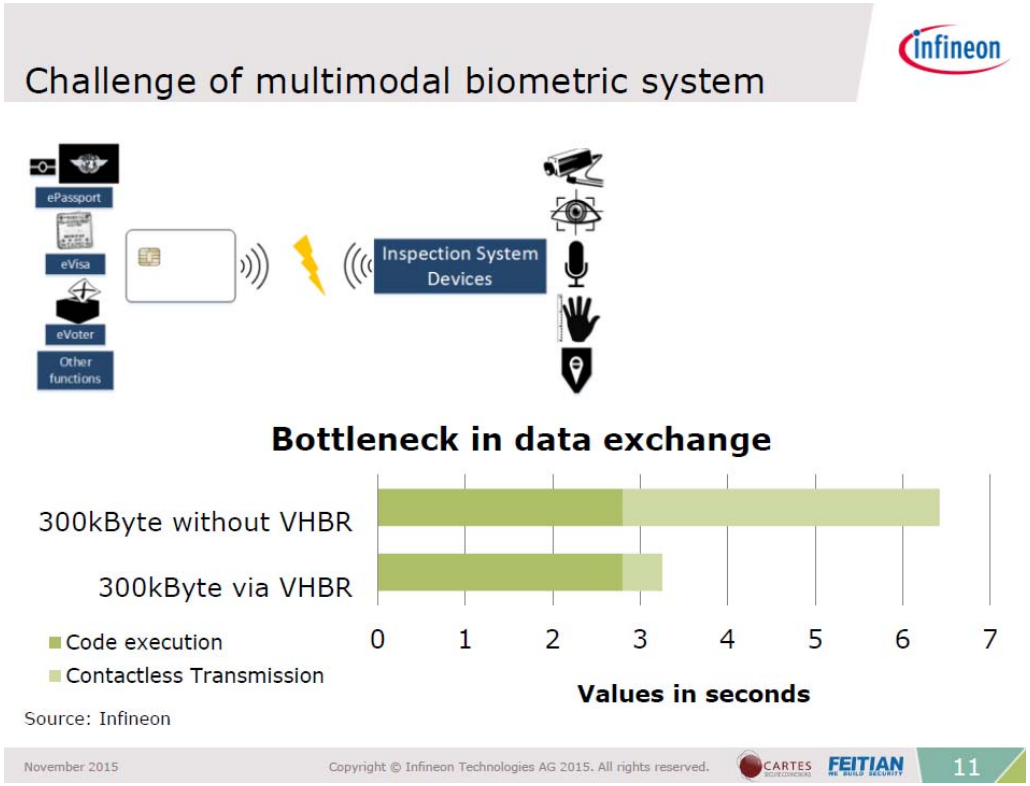
出展：CARTES2015カンファレンス資料

CARTES トピックス

High-speed Multimodal Biometric ID System (Infineon)

- データ量を減らして高速通信
  - Bioデータは盗まれる
  - トークン化して保存
  - 生よりデータ量が減る
  - サーバ間通信量、クライアント容量は減る

CARTES2013ではVHBRでe-passport処理を1.5秒から0.8秒にしたと言っていた。ICAO標準でBioも可能とも。

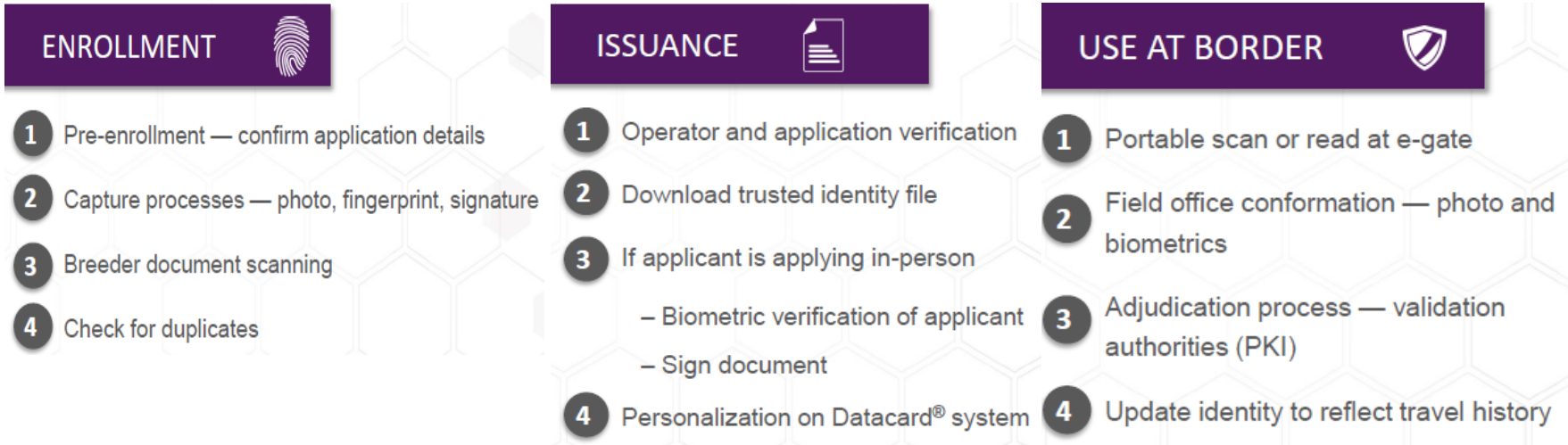


出展：CARTES2015カンファレンス資料

CARTES トピックス

The Leading Edge of Border Security (Entrust Datacard)

- 技術はあるのに実現しない・・・標準化が遅い
  - ひとつの信頼できるIDがあればパスポート、国民ID、免許などのエコシステムに使用できる
    - 空港のキャパは60～70million人
    - WHO、WHAT、WHEREを判断する
    - ID登録→パスポート発行→国境での使用



出展：CARTES2015カンファレンス資料

CARTES トピックス
Europe And Identity Credentials (IHS)

- EU内の人の移動問題
  - Schengen areaは協定あるがEU内は三分割。
  - ドイツ：eIDに賛成
  - フランス：16年にIC化。プライバシーに懸案
  - イギリス：未決
  - ハンガリー、トルコ：16年にeID完了
  - オーストリア：eGovで利用可能だが必須でない。

  ⇩

  - ドイツとオーストリアはIDカードの標準化へ
  - ボーダーレスEU

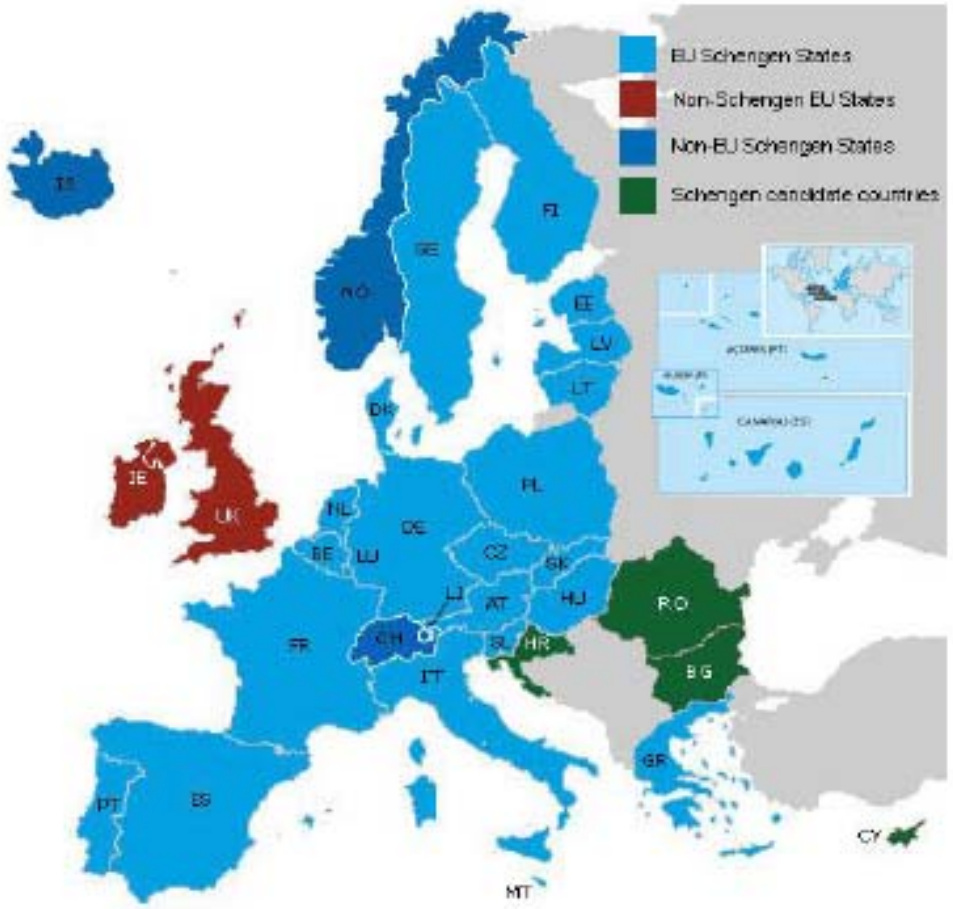


Image taken from The European Commission Migration and Home Affairs website and can be found at : http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen/index_en.htm

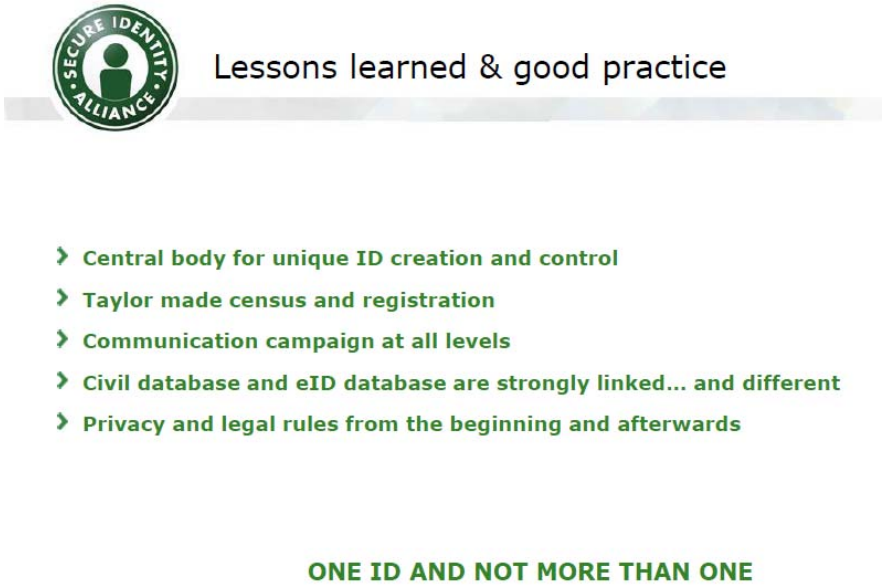
出展：CARTES2015カンファレンス資料

CARTES トピックス

Civil Registry consolidation through digital identity management (SIA)

- 2030年の人口8.5billion

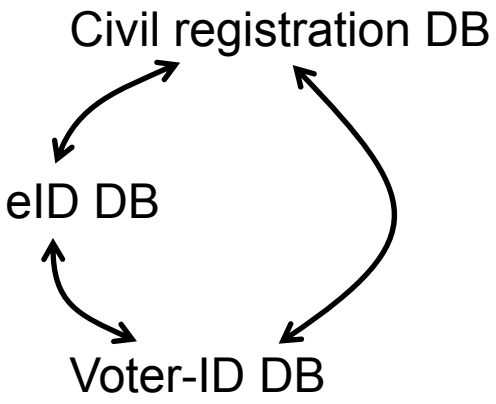
- 全員をID化し登録する
  - 市民台帳とeIDデータベースの相互互換性を確保
- パキスタンの例
  - 2004年、NADRAカード
  - 2009年、IDとpaymentサービスを付加
- マリの例
  - 2008～2010年に国勢調査
  - RAVEC（登録)、NINA（ID）



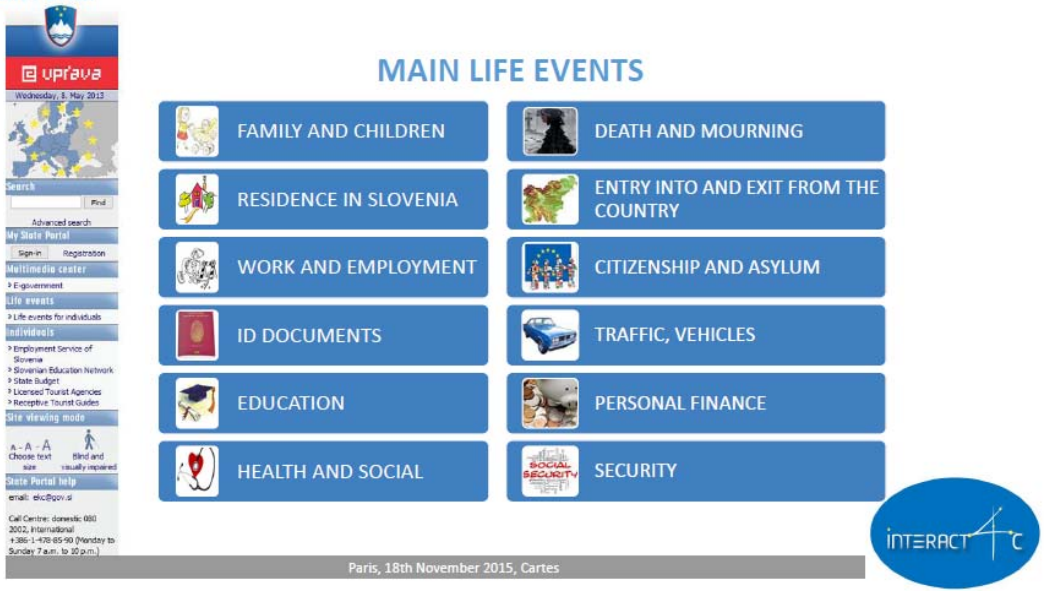
出展：CARTES2015カンファレンス資料

CARTES トピックス
From CRVS to eGovernment (Interact4C)

- スロバキアのケーススタディ
  - 1976年、住民登録の導入
  - 1981年、個人IDの導入
  - 1990年、個人データ保護法
  - 2005年、DB化



全てのデータを
全てのサービスにデリバリ



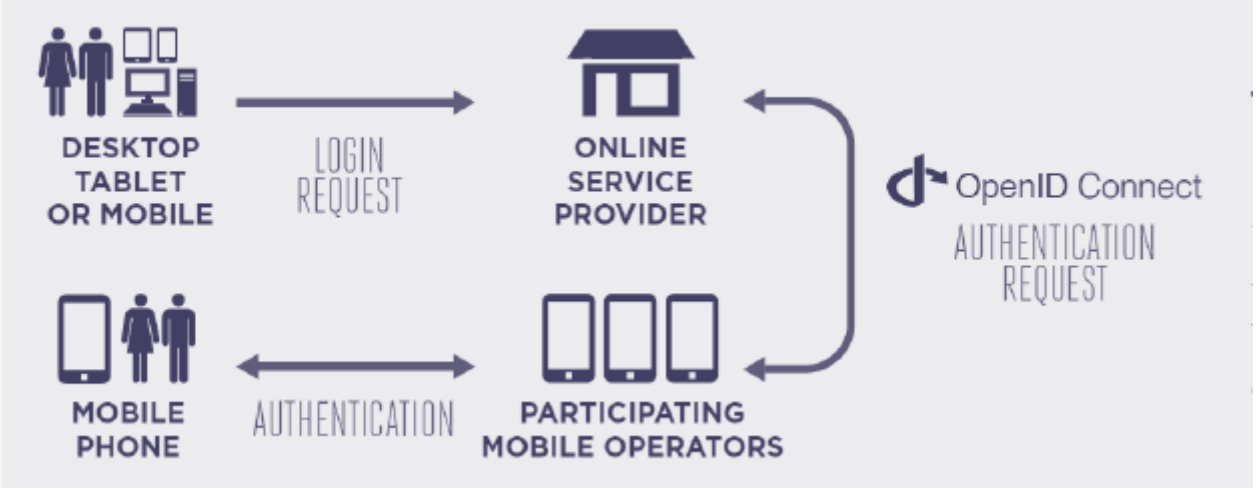
出展：CARTES2015カンファレンス資料

CARTES トピックス

Enabling Trust and Creating Value Through Mobile Identity Solutions (mobile connect)

- セキュリティを向上し「使う大義」をつくる
  - パスワード運用のコストを下げるべき
  - スマホは使い慣れているし、SEでセキュア
  - オペレータに信用があり、支払いシステムも既存
- 認証ステップ
  - Simple
    - I have
  - Two factor
    - I have
    - I know

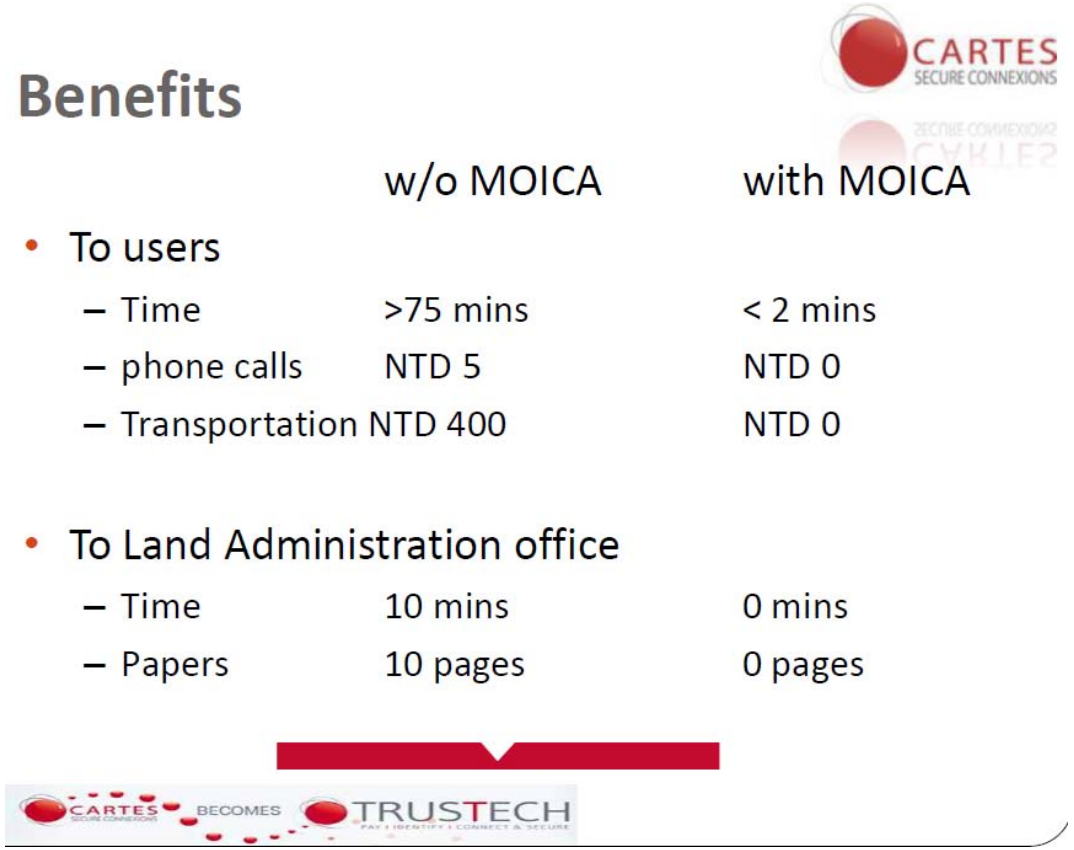
PCからWebにログインするとき、スマホでワンクリック



出展：CARTES2015カンファレンス資料

CARTES トピックス
Taiwan Case Study (Chunghwa Telecom)

- メリットを明示する。
  - 国民一人当たりの導入コストは$8（内ソフトウェアが$4）。
  - メリットはTAX申請時の時間、手間、書類の量
- 課題
  - 政府系、企業系、市民系の区分



出展：CARTES2015カンファレンス資料

CARTES トピックス

Online Identity; A new Security Check challenge (oberthur)

- STATE（国境、警察）とCITIZEN（銀行、入退室）
  - F2Fサービス：国境、警察、銀行
  - オンラインサービス：銀行サービス、TAXサービス
  - どちらも
    - カード　vs　カメラ
    - 文書　vs　カメラ

の画像比較で
持ち主確認

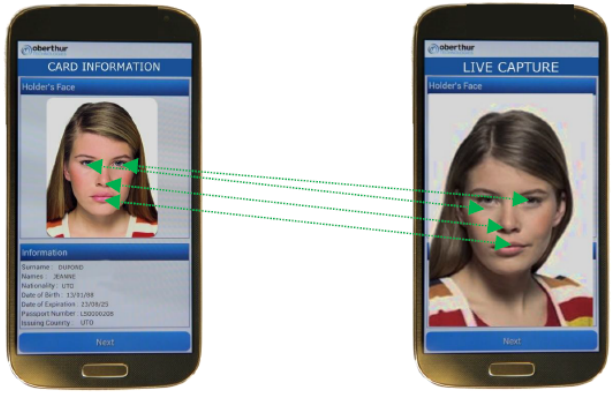
oberthur TECHNOLOGIES THE M COMPANY

Professional checks third party identity → Contactless

Face matching

Holder authentication

Image in the chip **VS** Live capture

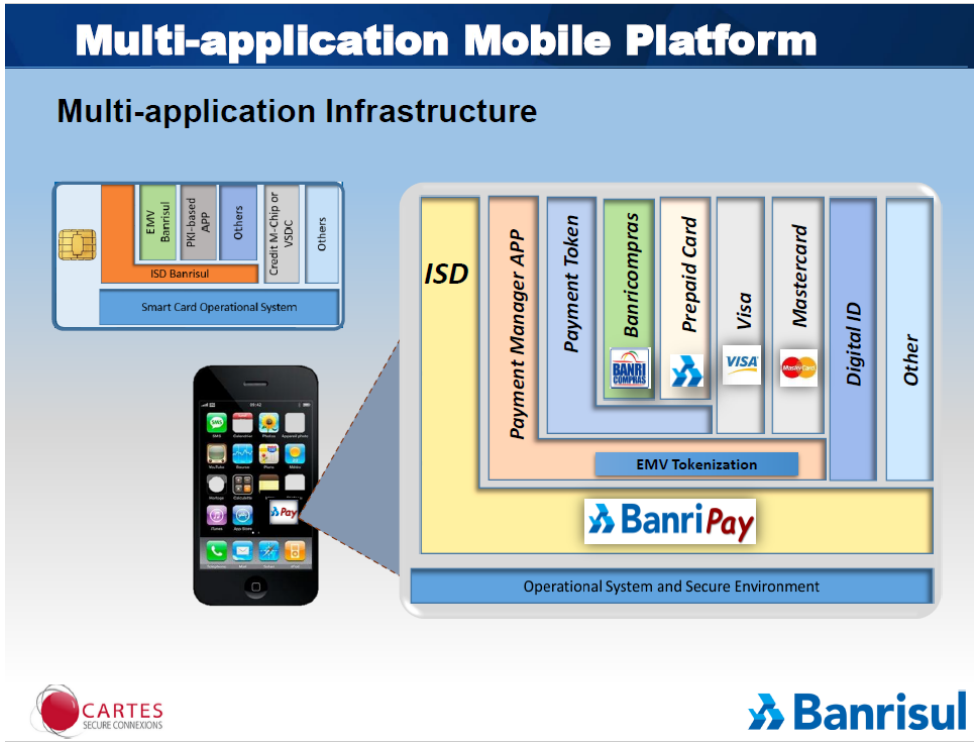


CARTES2013では
電子チケットをミュン
ヘンで買ってパリで
使う、が話題。

出展：CARTES2015カンファレンス資料

CARTES トピックス
Connecting the points (Banrisul)

- eCommerceのモバイルトランザクションが増大
  - 2013年→2014年（+127%）→2015年（+249%）
  - クレジット会社の協力でマルチアプリカードにBanriを開発
  - 支払いにEMVトークン
  - これを支える328のアプリは、カードと同じライフサイクルのマネジメントが必要。
  - 今は顔認証だが、次は音声？
  - 今はローカル認証、次はサーバ認証？



出展：CARTES2015カンファレンス資料

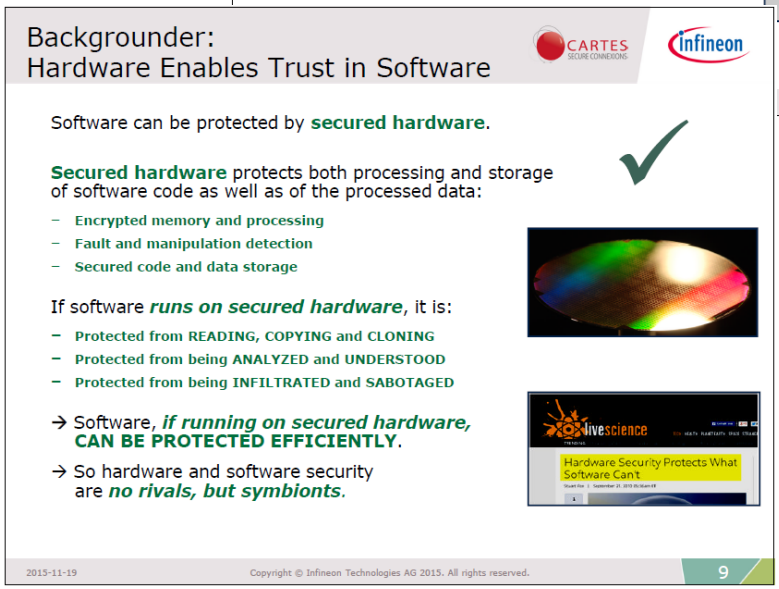
CARTES トピックス

Trusted Solution for Identification and Authentication (Infineon)

- 25人に一人がインターネットアカウント
- 1人が6.5個のパスワード
- 1つのパスワードが15文字
  - User know PIN
  - User has cards
  - User is Bio

CARTES2013では80デバイス/秒が2020年には250デバイス/秒になると言っていた。車のリモートアップデートにも言及 byOberthur

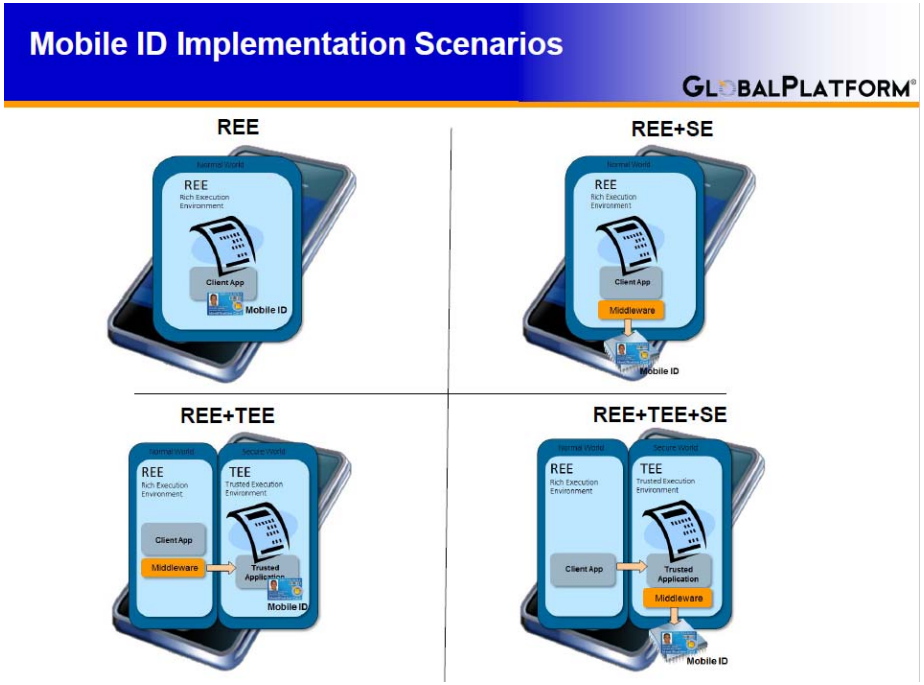
出展：CARTES2015カンファレンス資料



CARTES トピックス

The Role of Mobile Device in Identity (Global Platform)

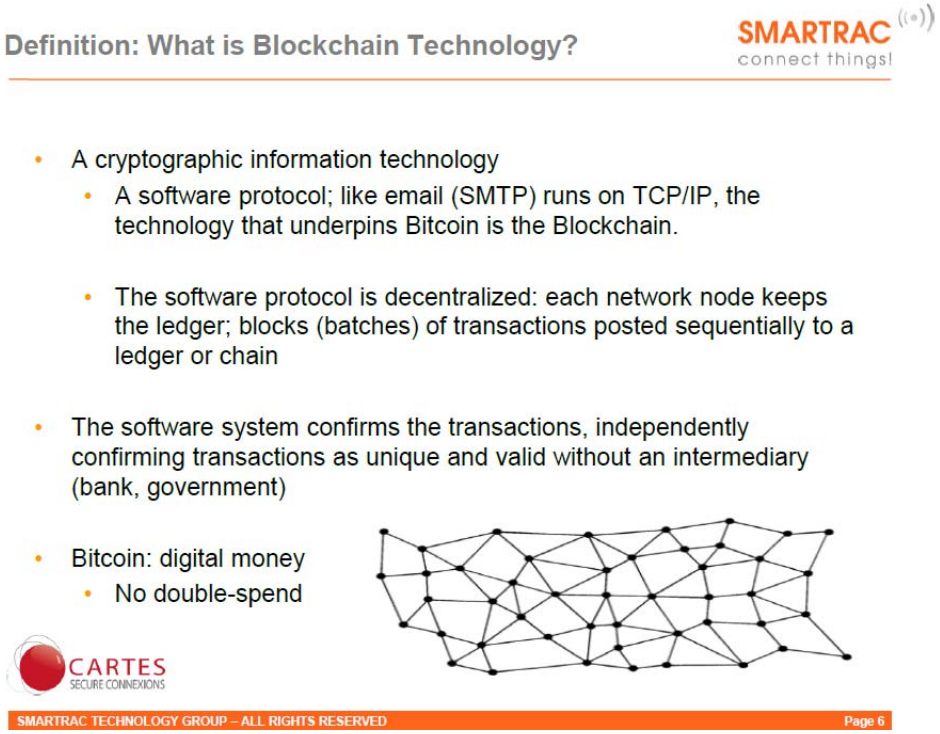
- プラスチックカード→チップカード
  - ユーザーの目的は「支払い」。手段に興味ない。
  - チップカードのキラーアプリがない。今より便利にしないとスイッチしない。
- モバイルの課題
  - ビジネスとパーソナル、両方の用途がある。
  - 事故などによるID交換ができること
- 実装
  - 右の4種。
  - eIDASをSE+TEEで実装＝FIDOアプリ



出展：CARTES2015カンファレンス資料

CARTES トピックス
Is Identity the New Money? (Smartrac)

- どうやって信頼する？
- Blockchain IDを提案
  - 各サイトにIPアドレス
  - 顔写真を入手
  - その他（住所、有効期限）などを含めID化
  - 生成したPGP鍵に署名
  - タイムスタンプをつける
  - BitCoinのBlockchainにKeyIDを付加
  - システムがロバストになる

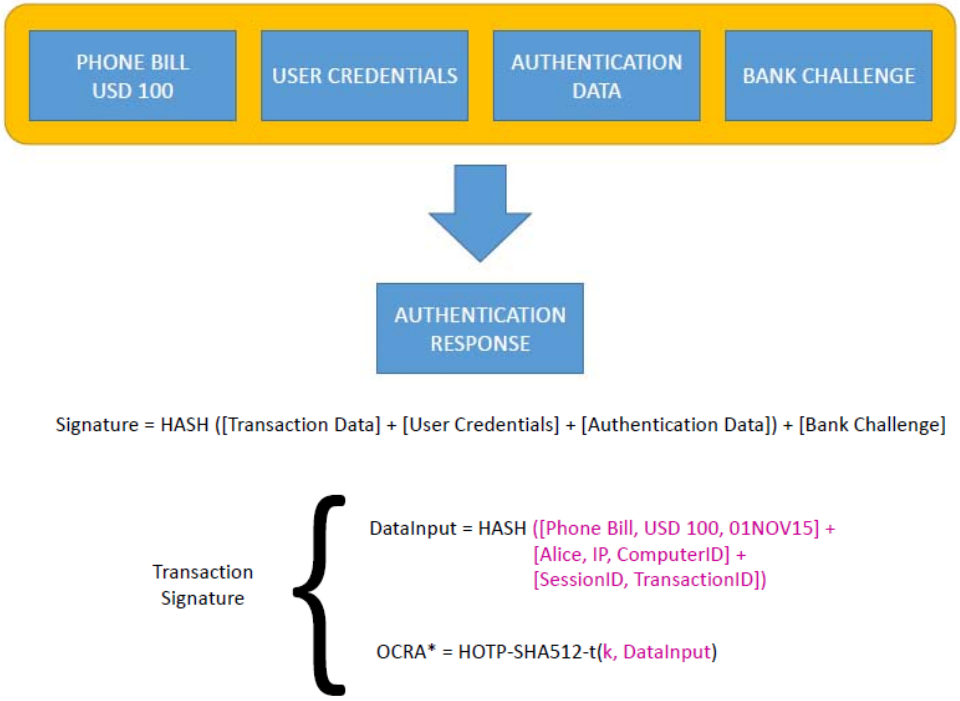


出展：CARTES2015カンファレンス資料

CARTES トピックス

CNP; How to enable Secure transactions in Non-secure environments? (Watchdata)

- CNP起因の脆弱性
- どうやって認証するか？
  - クッキーでPC固定
    →MITM可能
  - OTP
    →Online直後に侵入可能
  - BioでPC認証
    →トランザクションにBioは使わないので守られない
  - トークン化（偽物防止）
    →credentialにアクセスされたら悪用可能
  - Off channel transaction signatureの提案
    →OTPとトランザクションをリンク



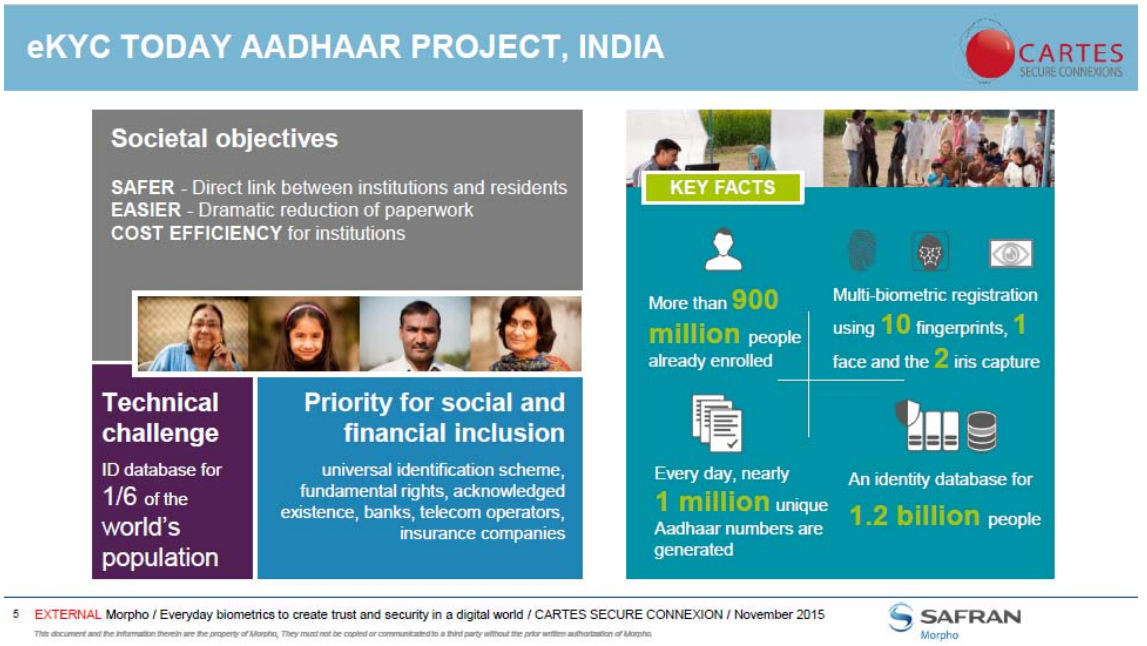
出展：CARTES2015カンファレンス資料

CARTES トピックス

Everyday biometrics to create trust and security in a digital world (SAFRAN)

- ID認証をBioでセキュアに
  - What I Have
  - What I know
  - What I am
- インドプロジェクト
  - 個人番号+指紋の2ファクタでモバイル接続
  - 顔認証の1ファクタでネット接続

  の2段階認証



出展：CARTES2015カンファレンス資料

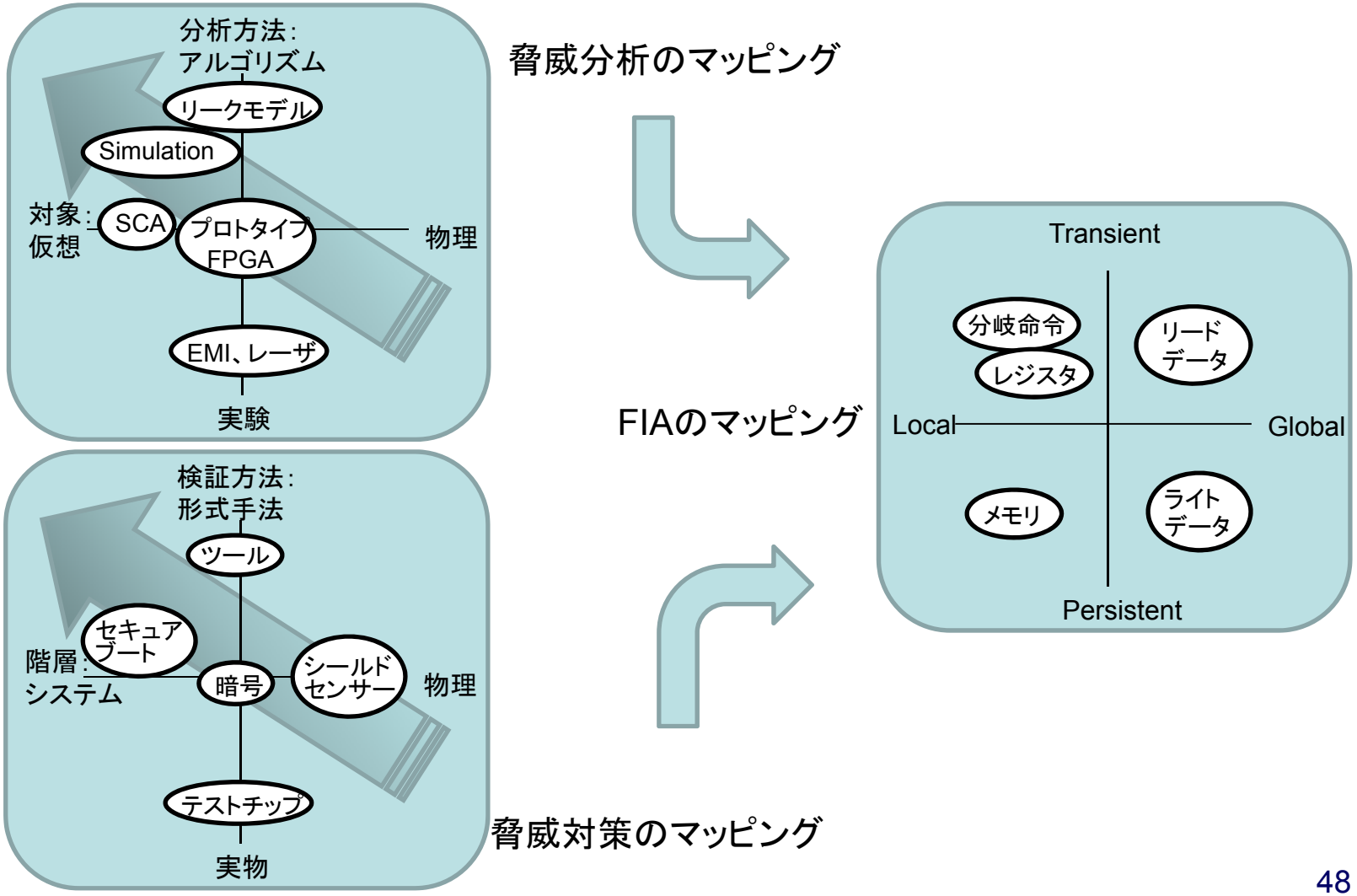
まとめ

まとめ

- JHASやJTEMSは情報をメンバー内に限定する閉鎖的な会合であるがblack hatやCARTESは開放的であり、参加者が攻撃事例を見ることで脅威を感じてもらう、あるいは適用事例を見ることで実用上の課題をあらかじめ知るには良い機会。事例紹介や実習はIPAでのハードウェアセキュリティセミナーでも行っている。
- CARTESにおいて生体認証の事例として話されたのは、生体情報のセンサー（ハードウェア）だけでなく、データ処理のソフトウェア及びそれらを求めるOS、利用するインフラ（サーバやネットワーク）など多岐にわたる。いずれも非生体認証とのセキュリティ強度、利便性の差異を明確にする必要性を強調していた。
- 「セキュリティポリシーが製品に反映されていない」との言及がblack hatであった。「ソフトウェアでソフトウェアは守れない、ソフトウェアはセキュアなハードウェアで守る、ソフトウェアとハードウェアは共生すべき」との言及がCARTESであった。セキュリティコミュニティで経験と技術を広く共有すべきであると思う。

まとめ

- 脅威分析→対策→FIA　のフローに変化が出てきた



参考文献

- BLACK HAT EUROPE 2015 資料のArchive
  https://www.blackhat.com/html/archives.html#europe
  プレゼンテーションスライド、ホワイトペーパー、ソースコードがダウンロード可能

- CARTES 2015 Program
  http://www.cartes.com/Programme/Conference-programme
  プログラムの概要を見ることができる

- シミュレーションによる電力評価手法
  http://www.dvlsi.jst.go.jp/list/SCIS2013/pdf/SCIS2013_1E1-1.pdf
  https://opus4.kobv.de/opus4-fau/frontdoor/deliver/index/docId/1289/file/diss_gstoettner.pdf

IPAの取り組み

IPAの取り組み

- ハードウェア脆弱性評価に関する人材育成
  - 新しい攻撃への耐性を評価する最先端のツールを整備して、日本の半導体ベンダ、ICカードベンダ、評価機関、大学などの研究機関が利用できる評価環境の整備を進めている。
    - 最先端の評価ツール及びテストビークル(評価対象のIC)を使用し、脆弱性を評価することで新しい攻撃手法を修得
    - ICカードの開発過程で利用し、対抗策を検証することで、高い攻撃耐性を持った製品開発が可能
    - 将来的な攻撃手法の研究活動に活用
    - 興味深い攻撃については、IPA所有の装置での再現実験の実施を検討

IPAの取り組み

- ハードウェアセキュリティに関する技術セミナーの開催

2015年6月8日 2015年6月30日	ハードウェアセキュリティセミナー (導入コース) 終了
2015年8月27日 2015年9月7日	ハードウェアセキュリティセミナー (技術コース・入門編) 終了
2015年12月16日 2016年1月13日 2016年2月23日	ハードウェアセキュリティセミナー (技術コース・実践編) 実際にレーザー装置を使用した攻撃と、その対策の実装 満員御礼。

- 2016年度も開催予定
- 実践編では、レーザー攻撃以外の攻撃 (サイドチャネル攻撃など) を取り上げた講座開催も検討中

セミナー情報: https://www.ipa.go.jp/security/jcmvp/seminar/

ご清聴ありがとうございました。

当セミナーに関する質問は以下のメールアドレスまでどうぞ。

hwsec-seminar@ipa.go.jp