SIGS – Security Interest Group Switzerland

Trends in Mobile Authentication

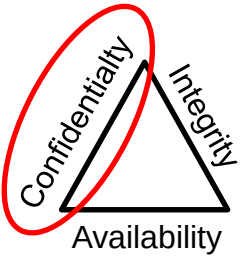
Christian Birchler, cnlab security AG
Esther Hänggi, cnlab security AG
4. November 2014, Basel

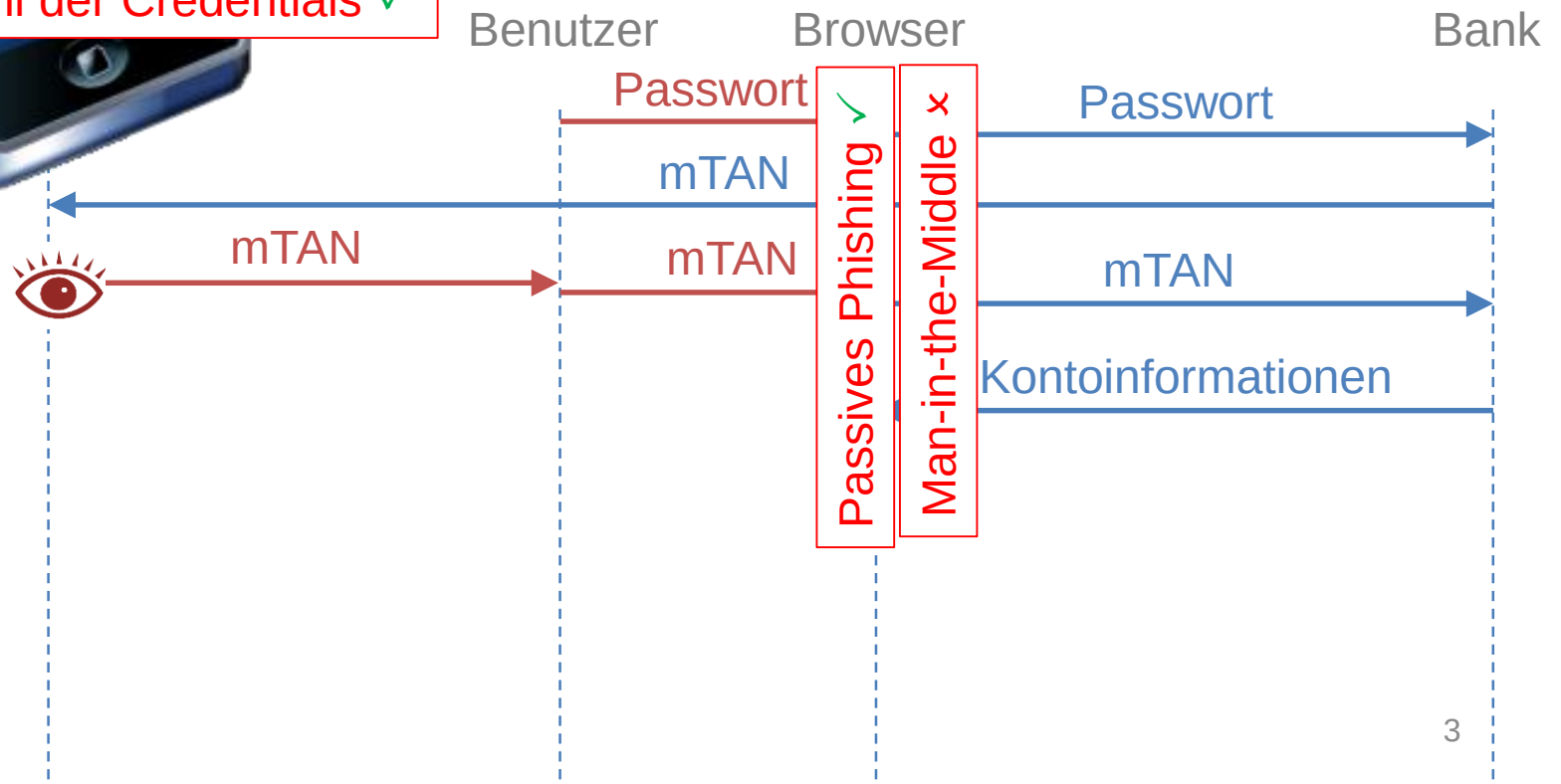
E-Banking-Authentisierungsmethoden

E-Banking-Authentisierung: mTAN

Logincode:
73G833
Letzter Login:
31.03.2014 16:47

Diebstahl der Credentials ✓





E-Banking-Authentisierung: mTAN

Code für Transaktion: 3EH878 50 CHF auf Konto-Nr. 01-145-6

Benutzer Browser Bank

Login

Passwort

Passwort

mTAN

mTAN

mTAN

mTAN

mTAN

Session hijack ✓

Session riding ✓

Man-in-the-Middle ✓

ntoinformationen

Transaktion

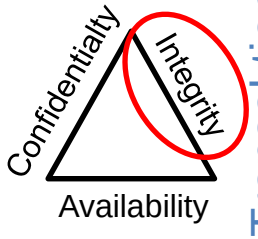
Transaktion

mTAN

mTAN

mTAN

mTAN



- 2 Geräte
- 1 Gerät
- 1 Gerät mit Härtung

Vergleich verschiedener Authentisierungsmethoden

	Streichliste	One-time password	Challenge-Response Token	mTAN (SMS)	Mobile ID	C/R Token mit Display (PhotoTAN, QR-Code)	Sign. App + gehärt. Browser (2 Geräte, mIDentity)	C/R Token + gehärt. Browser	**Massnahmen**
Login + Lesender Zugang									
Diebstahl Credentials									← Physisches Gerät
Passives Phishing									← Beschränkte Gültigkeitsdauer, dynamisches Credential
Man-in-the-Middle									← Client certificate, gehärteter Trust-Store
Malware									← Gehärteter Browser
Transaktion									
Session hijack									Zusätzlich Autorisierung
Session riding									
Man-in-the-Middle									Transaktionsabhängigkeit, Sichtbarkeit der Transaktionsdetails
Malware									

Starke Authentisierung: Definition(en)

- Keine Übertragung des Passwortes über das Netzwerk (Fermilab)
- Challenge-Response-Verfahren (Handbook of Applied Cryptography)
- 2 verschiedene Authentisierungsmethoden (BSI)
- Mindestens 2 Faktoren: (ENISA)
  - Wissen (z.B. Passwort, PIN);
  - Haben (z.B. Bankkarte, Smartkarte);
  - Sein (z.B. biometrische Eigenschaft, Fingerabdruck).

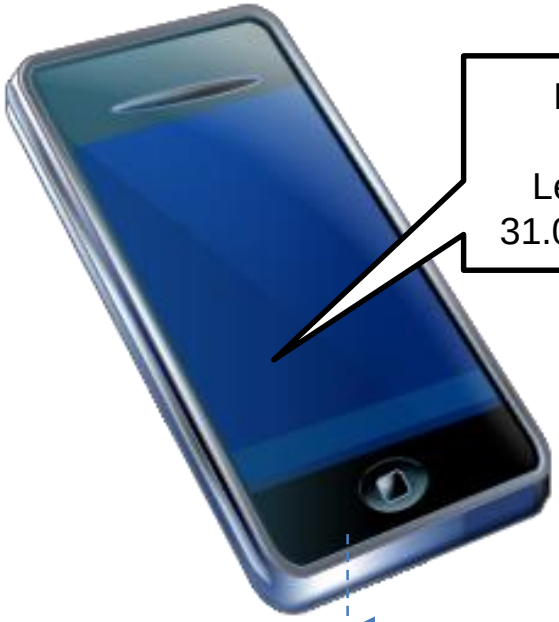
ENISA-Definition + (EZB)

- Unabhängigkeit der Faktoren
- mind. 1 Faktor:
  - nicht wiederverwendbar
  - nicht replizierbar (ausser biometrische Daten)
  - kann nicht über das Internet gestohlen werden

- Abhören der Netzwerkverbindung genügt nicht
- Diebstahl ist schwierig

Häufige zusätzliche Bedingung beim e-banking:
2 Geräte, nicht nur 2 Faktoren!

Mobile Banking



Benutzer Browser Bank

Login

Passwort Passwort

mTAN

mTAN mTAN mTAN

Kontoinformationen

Transaktion

Transaktion

mTAN

mTAN mTAN mTAN

2 Geräte
1 Gerät
1 Gerät mit Härtung

Authentisierungsmethoden von 1 Gerät

Login + Lesender Zugang

Diebstahl Credentials
Passives Phishing
Man-in-the-Middle
Malware

1 Gerät

Transaktion

Session hijack
Session riding
Man-in-the-Middle
Malware

Strategien für sicheres Mobile Banking

Einzelnes gehärtetes Gerät:

Volle Funktionalität auf einem Gerät – zusätzliche technische Massnahmen

Mehrere Authentisierungsstufen:

Eingeschränkter Funktionsumfang abhängig von der Stärke der Authentisierung

2 Geräte
1 Gerät
1 Gerät mit Härtung

Einzelnes gehärtetes Gerät (1/3): Wirkung technischer Massnahmen

Es ist nicht so schlimm wie es aussieht …

Login + Lesender Zugang

Diebstahl Credentials
Passives Phishing
Man-in-the-Middle
Malware

Transaktion

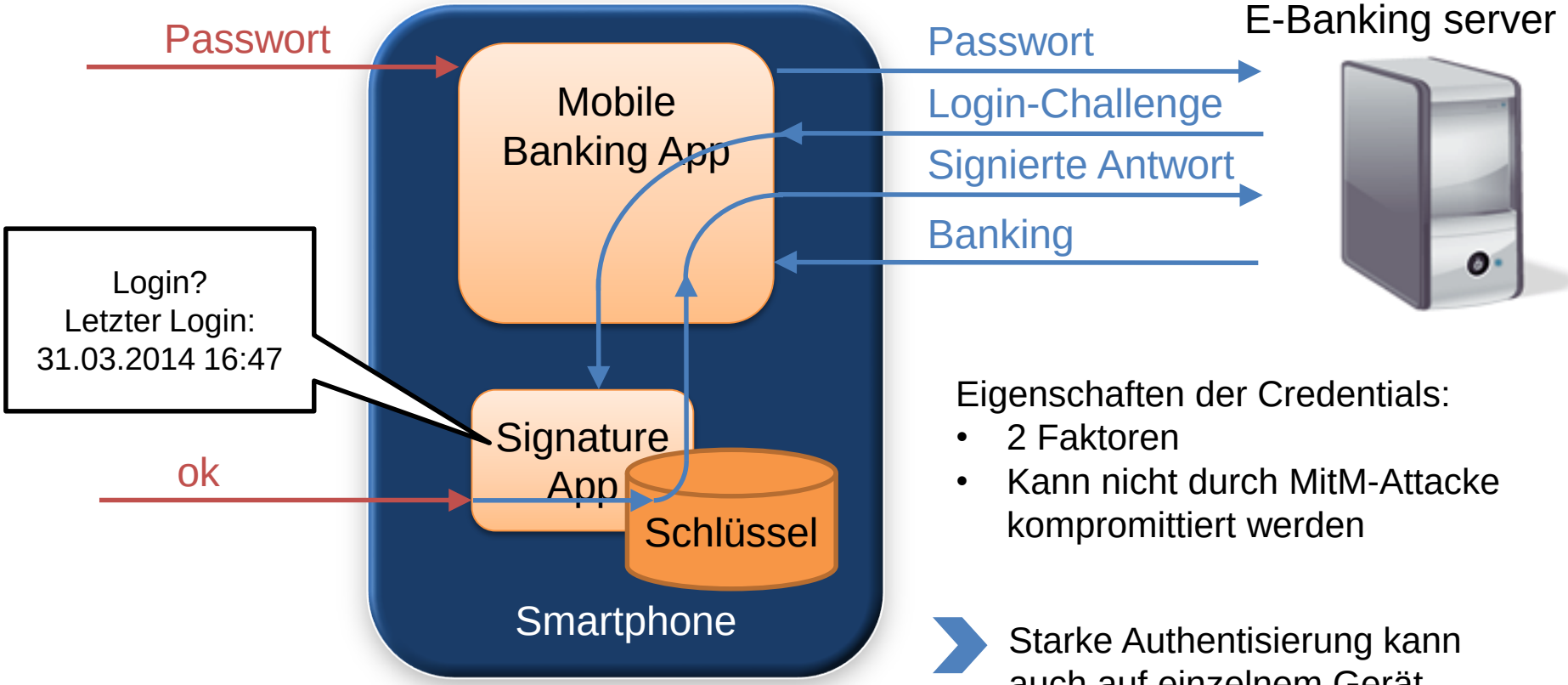
Session hijack
Session riding
Man-in-the-Middle
Malware

Härtung

Eigener Trust-Store der App
Härtungsmassnahmen

Eigener Trust-Store der App
Härtungsmassnahmen

Einzelnes gehärtetes Gerät (2/3):
Beispiel 1 - Integrierte PhotoTAN App der Raiffeisen



Eigenschaften der Credentials:
- 2 Faktoren
- Kann nicht durch MitM-Attacke kompromittiert werden

Starke Authentisierung kann auch auf einzelnem Gerät erreicht werden

- Volles E-Banking vom Smartphone
- Einzelnes Gerät
- Technische Härtungsmassnahmen

Einzelnes gehärtetes Gerät (3/3): Technische Massnahmen

Vorteile von Smartphones gegenüber Desktop-Computern:

- Apps laufen in Sandboxen (Prozesse und Daten)
- Verteilung der Programme (Apps) über Store
- PIN-geschützter Zugang (optional)
- Verschlüsseltes Filesystem (iOS: standard, Android: einige)

Mögliche Härtungsmassnahmen für Apps:

- Zertifikatscheck mittels eigenem Trust-Store
- Schutz der Daten durch Keychain (iOS)
  (inkl. Bindung an das Gerät)
- Schutz der Files durch Zugangsschutz des OS (iOS)
- Verhindern des Backups gewisser Files
- Verhindern von Screenshots
- Detektion von Jailbreak / Rooting
- Versionskontrolle der App / OS

Strategien für sicheres Mobile Banking

Einzelnes gehärtetes Gerät:

Volle Funktionalität auf einem Gerät – zusätzliche technische Massnahmen

Mehrere Authentisierungsstufen:

Eingeschränkter Funktionsumfang abhängig von der Stärke der Authentisierung

Mehrere Authentisierungsstufen (1/3): Eingeschränkte Funktionalität

Benutzer

Bank

1. Schritt

Benutzerauthentisierung
z.B. durch Login

➡ Kontoinformationen +
‘plausible’ Transaktionen

Login

Kontoinformationen

‘plausible’ Transaktionen

2. Schritt

Zusätzliche Autorisierung
z.B. durch mTAN,…

➡ Alle Transaktionen +
Wichtige Änderungen

Transaktion

Autorisierung der Transaktion

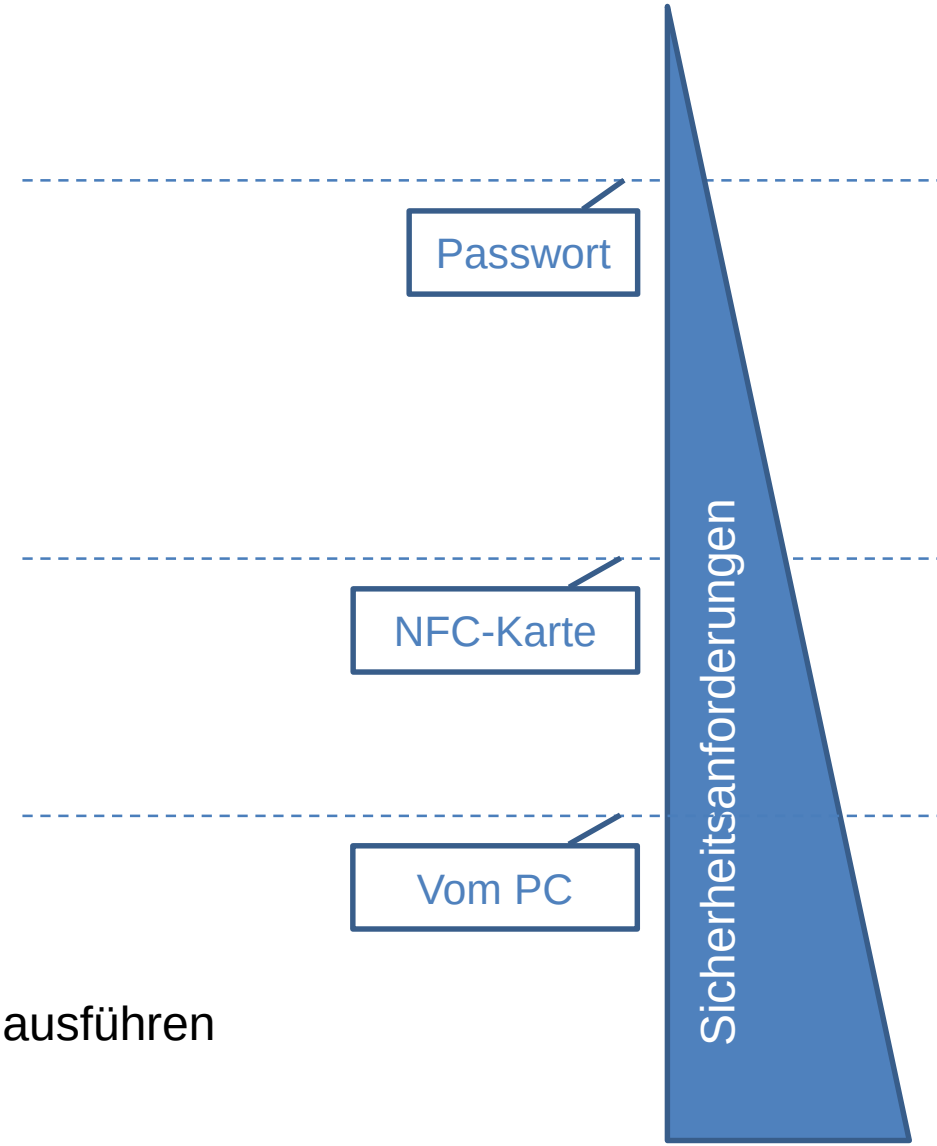
Mehrere Authentisierungsstufen (2/3): Beispiel 1
Mobile Banking UBS

Banking vom Smartphone

- Allgemeine Informationen
- Lesender Kontozugang
- “Personal finance assistant”
- Wertschriftenhandel
- Transaktionen scannen
- E-Rechnungen
- Transaktionen erfassen
- Transaktionen der Whitelist ausführen

Volles E-Banking

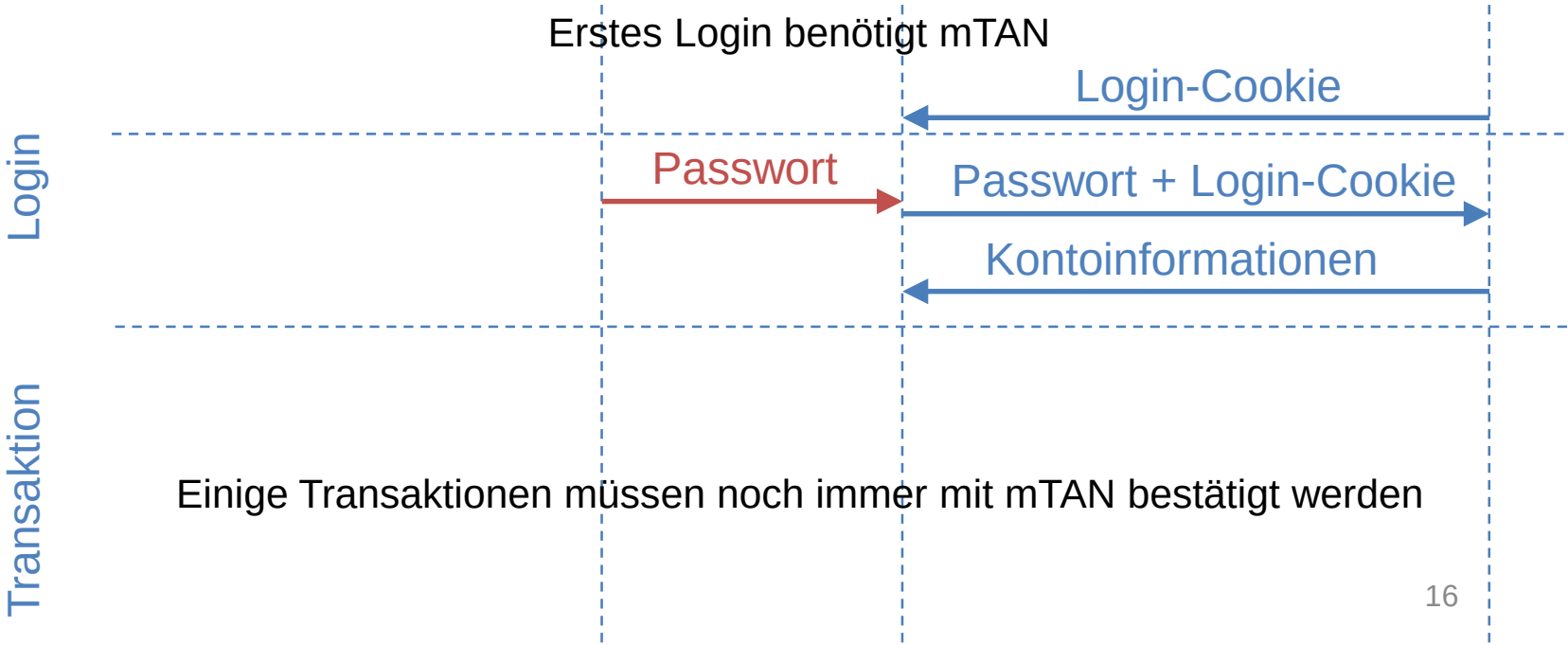
- Registrierte Transaktionen ausführen
- Beliebige Transaktionen erfassen und ausführen
- Kundendaten ändern



Mehrere Authentisierungsstufen (3/3): Beispiel 2

E-Banking mit Langzeit-Cookie

Benutzer Browser Bank



Trends

- Smartphones sind vollwertige Computer
- Lesender Zugang ist weniger heikel als Transaktionen
- Technische Härtungsmassnahmen
- Mehrere Authentisierungsstufen

Danke

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 40

Esther Hänggi
esther.haenggi@cnlab.ch
+41 55 214 33 36

Referenzen

- Fermilab: https://fermi.service-now.com/kb_view.do?sysparm_article=KB0011274
- Handbook of Applied Cryptography: http://cacr.uwaterloo.ca/hac/Technical hardening mechanisms
- BSI: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html
- ENISA: http://www.enisa.europa.eu/publications/archive/how-to-shop-safely-online
- EZB: http://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf
- ISACA: http://www.isaca.org/Journal/Past-Issues/2012/Volume-5/Pages/How-Strong-is-Strong-User-Authentication.aspx