Fachhochschule Gelsenkirchen

Restrisikoanalyse Online-Authentisierung

Zwischenbericht: „Restrisiken beim Einsatz der AusweisApp auf dem Bürger-PC zur Online-Authentisierung mit Penetration-Test“

Prof. Dr. (TU NN)
Norbert Pohlmann
Christian Rossow
Christian J. Dietrich

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

Ausgangssituation
→ Dilemma: Passwort-Authentisierung

- **Passworte, Passworte, … sind das Authentisierungs-Mittel im Internet!**
  - Passwort-Probleme
    - Verwendung von schlechten Passwörtern, oder
    - ein gutes Passwort wird für viele Dienste verwendet
    - Passworte werden im Klartext in HTTP-Sessions und in E-Mails über das Internet übertragen!
    - Passwort-Reset-Mechanismen sind sehr unsicher

- **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld!**
  - D.h. neben unterschiedlichen Passworten müssen wir uns auch oft noch unterschiedliche Identitäten merken!

- **Phishing-Problem** verursacht einen sehr großen Schaden (BKA)

Neuer Personalausweis – nPA
→ Vorteile der eID-Funktion

- **Deutlich höheres Sicherheitsniveau** im Vergleich zur herkömmlichen Passwort-Authentisierung im Internet!

- **Gegenseitige Authentifizierung**
  - nPA prüft das Berechtigungszertifikat
  - eID-Server prüft die Authentizität des nPAs
  - Die AusweisApp prüft die Domäne des Dienstanbieters (Hash des SSL-Zertifikats) aus dem Berechtigungszertifikat
  - → **Weniger Phishing-Angriffe!**

- **Zweifaktor-Authentisierung: Wissen (PIN) und Besitz (nPA)**
- Berechtigungszertifikat beschränkt die auszulesenden Merkmale
- Personenbezogene Daten gehen im Rahmen der eID-Funktion nie im Klartext über die Leitung

- **Hinweis:**
  Die eID-Funktion ersetzt die **Identitätsfeststellung** (nicht die Signatur!)
  - **Die eID-Funktion ist kein Verfahren zur Autorisierung einer Transaktion!**

Institut für Internet-Sicherheit
→ Aufgabe (1/3)

- Studie 2007: Demo-Implementierung der eID-Funktion

- **Aktuelle Aufgabenstellung**
  - Restrisiko-Analyse der eID-Funktion des neuen Personalausweises
  - Szenario: Der Nutzer verwendet die eID-Funktion über das Internet

- **Untersuchungsgegenstand: eID-Komponenten Stand Winter 2009**
  - Webshop als Diensteanbieter (mit eID-Server im Hintergrund)
  - 3 Test-Ausweise (BDr)
  - Kartenlesegerät (Basisleser, SCM SDI010)
  - OpenLimit AusweisApp (Bürgerclient v.1.0.0beta)

- Aufwand: 150 PT, 4 Monate bis März 2010 (Präsentation im BMI)

Institut für Internet-Sicherheit
→ Aufgabe (2/3)

TR Lesegerät: 58 Seiten
TR Personalausweis: 42 Seiten

Nutzer (Bürger-PC mit AusweissApp)

Authentisierung

Diensteanbieter

TR EAC: 117 Seiten

Auth.-Ergebnis

Authentisierung

eID - Server

TR eCard API: 492 Seiten
TR Kryptoverfahren: 112 Seiten
TR EAC-Box: 39 Seiten
TR PKI: 121 Seiten

→ Mehr als 1000 Seiten Spezifikationen!

TR eID - Server: 106 Seiten

Institut für Internet-Sicherheit
→ Aufgabe (3/3)

- **Vorgehensweise**
  - Wir haben die Rolle des Angreifers eingenommen
  - Wir hatten Zugriff auf sehr viele Informationen
  - Wir haben unsere Empfehlungen absichtlich sehr weit gefasst

- **Ergebnisse**
  - 11 Empfehlungen
  - Die meisten Empfehlungen wurden schnell umgesetzt (TR, Implementierung, …) oder wurden nach intensiver Diskussion
  - als nicht risiko-relevant eingestuft (z.B. PIN Eingabe).
  - Davon werden einige in den nächsten Wochen von uns nochmals überprüft.

→ **Summa summarum: Wir identifizieren 4 wichtige Restrisikobereiche!**

Restrisikobereich (1)
→ Kartenlesegeräte

- 3 Kategorien an Lesegeräten für den nPA (BSI TR 03119)
  - Basisleser (Cat-B)
  - Standardleser (Cat-S)
  - Komfortleser (Cat-K)

Logo für zertifizierte Lesegeräte

Merkmal	Basisleser	Standardleser	Komfortleser
Kontaktlose Schnittstelle	x	x	x
Kontaktbehaftete Schnittstelle	o	o	x
Pinpad	o	x	x
Zweizeiliges Display	o	o	x
Qualifiz. Signatur	–	–	x

Restrisikobereich (1)
→ Restrisiko: Basisleser (1/2)

- **Risiko: Abgriff der geheimen PIN**
  - Bei Lesegeräten ohne Pinpad (Basisleser) UND
  - Infektion des PCs mit Schadsoftware

➔ Eingabe der PIN am Pinpad eines Kategorie S- oder K-Lesegeräts (Standard- oder Komfortleser) viel sicherer!

Für die Online-Authentisierung sollten Lesegeräte mit sicherem Pinpad bevorzugt verwendet werden (Standard- und Komfortleser).

Restrisikobereich (1)
→ Restrisiko: Basisleser (2/2)

- **Bei bekannter PIN und aufliegendem nPA: Identitätsmissbrauch per entferntem Zugriff möglich!**

- **Ablauf der Online-Authentisierung kann automatisiert werden**
  - Vollständig bei Basislesern
  - Nur eingeschränkt bei Standard- und Komfortlesern (PIN-Eingabe muss manuell erfolgen!)

Standard- und Komfortleser schützen nicht nur vor dem Auslesen der PIN am PC, sondern darüber hinaus auch vor einem automatisierbaren Missbrauch der Online-Authentisierung.

Restrisikobereich (1)
→ Die Vorteile des Komfortlesers

- Der Komfortleser verfügt zusätzlich über ein Display und unterstützt die QES
- Authentisierungs-Gegenstelle wird verlässlich im Display angezeigt
- Darstellung von Berechtigtem und den Berechtigungen ist **authentisch**
- Erfordert die **manuelle Interaktion** (PIN-Eingabe) des Benutzers bevor eine Online-Authentisierung abgeschlossen werden kann

Restrisikobereich (1)
→ Empfehlungen beim Einsatz: Basisleser

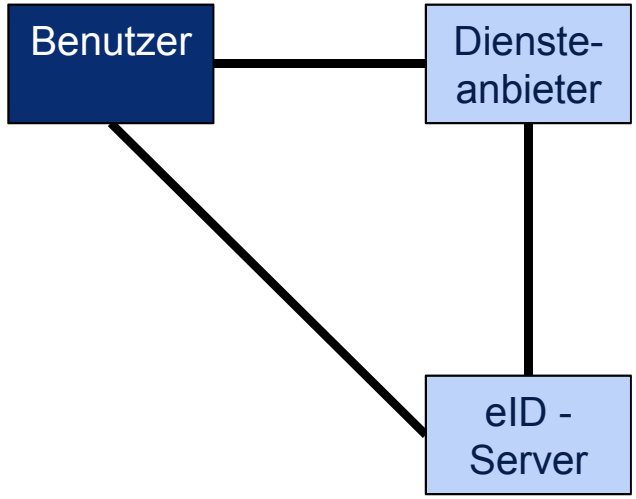
- Der Benutzer sollte eine **starke PIN** verwenden!
- Es sollte sichergestellt werden, dass der **nPA nur während einer Online-Authentisierung auf dem Lesegerät** aufliegt und danach vom Lesegerät genommen wird.
- Die Integrität und Vertrauenswürdigkeit des Bürger-PCs muss mit gängigen Grundschutztechniken wie **Firewall, Antivirus-Programmen und Software-Updates** gewahrt werden.
- Der Benutzer sollte bei der Verwendung eines Basislesers durch ein **optisches und/oder akustisches Signal** darauf hingewiesen werden, dass eine Online-Authentisierung gestartet wird.

Vor der Installation der AusweisApp sollte die Integrität des PCs sichergestellt werden. Siehe auch: www.botfrei.de

Restrisikobereich (2)
→ Sicherheit des Kommunikationsmodells

- Spezifikationen sind ausgereift und wenig Potential für Schwachstellen
- Die Authentikation gegenüber dem eID-Server ist sehr stark

- **Der eID-Server muss als letzten Schritt dem Diensteanbieter (z.B. Webshop, Bank, …) das Authentisierungsergebnis (nPA-Attribute) mitteilen**
- **Schwachstelle in einer frühen Implementierung des Diensteanbieters und eID-Servers ermöglichte Zugriff und Manipulation der personenbezogenen Daten (Ergebnis wurde über den Bürger-PC gesendet)**



➔ Empfehlung:
Test der Implementierung des eID-Servers auf Einhaltung der Spezifikation

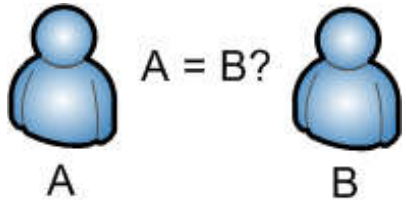
Restrisikobereich (2)
→ Sicherheit des Kommunikationsmodells

- **Session-Hijacking**
  - Schafft es ein Angreifer, sich als Man-in-the-Middle zwischen Diensteanbieter und Benutzer zu bringen, so kann er zwar die Ergebnisse der Authentisierung nicht mitverfolgen, kann aber möglicherweise die vom Diensteanbieter erstellte Session nach erfolgreicher Authentisierung übernehmen und missbrauchen.

- ***Reaktion***
  - Hash des SSL-Zertifikats (Domäne) steht im Berechtigungszertifikat.
  - Die AusweisApp des Bürger-PCs überprüft im Berechtigungszertifikat den Hash des SSL-Zertifikats!
  - Änderung in drei „Technischen Richtlinien (TRs)“ durchgeführt!
  - **➔ Empfehlung: Test der Implementierung der AusweisApp auf Einhaltung der Spezifikation!**

Restrisikobereich (3)
→ Tracking des nPA

- **Der eID-Server muss Sperrlisten-Prüfung durchführen**
  - Das verwendete Merkmal identifiziert einen nPA eindeutig
  - nPA kann vom eID-Server prinzipiell wiedererkannt werden



- Anbieterspezifisches Wiedererkennen ist zwar technisch möglich, aber
  - Personendaten bleiben unbekannt
  - **Daten für die Sperrlisten-Prüfung dürfen nicht gespeichert werden (gesetzliches Verbot des Trackings)!**
- **Anbieterübergreifendes Tracking ist nicht möglich!**

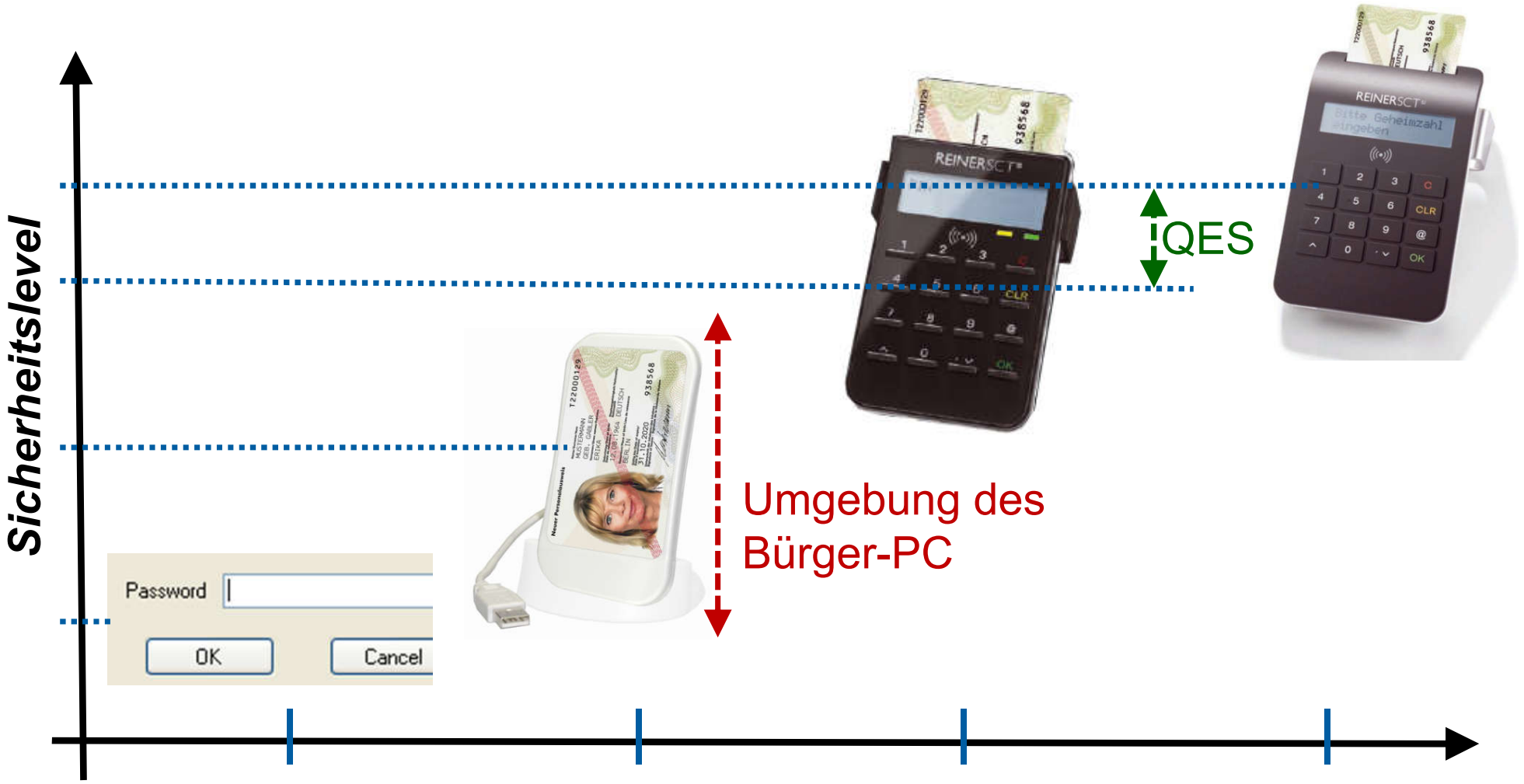
Der Benutzer sollte sich bewusst sein, dass ein nPA vom eID-Server wiedererkannt werden kann, auch wenn keine personeneindeutigen Merkmale übermittelt werden (z.B. Altersverifikation).

Das gesetzliche Verbot des Trackings muss überprüft werden!

Restrisikobereich (4)
→ Aufklärung (z.B. Missbrauch / Verlust)

http://www.personalausweisportal.de

Einschätzung der Restrisiken
→ Sicherheitslevel



Zusammenfassung

- **Die eID-Funktion des neuen Personalausweis ist sicherer als Benutzername und Passwort!**
- Phishing-Angriffe werden bei der Verwendung der eID-Funktion sehr aufwändig!
- Standard- und Komfort-Leser sind deutlich sicherer als ein Basis-Leser!
- **Der Benutzer muss Kompetenzen entwickeln, um seinen Computer (PC, Notebook, SmartPhone, …) sicher einzurichten, unabhängig vom neuen Personalausweis!**
- Wir brauchen eine höhere Sicherheit, um die neuen Möglichkeiten vertrauenswürdig nutzen zu können.
- Der nPA ist ein Schritt in die richtige Richtung!
- **Jeder sollte seinen Betrag dazu leisten, um die Zukunft sicher zu gestalten!**

Fachhochschule Gelsenkirchen

Restrisikoanalyse Online-Authentisierung

Vielen Dank für Ihre Aufmerksamkeit
Fragen?

Prof. Dr. (TU NN)
Norbert Pohlmann
Christian Rossow
Christian J. Dietrich

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Fachhochschule Gelsenkirchen

Detailfolien

Prof. Dr. (TU NN)
Norbert Pohlmann
Christian Rossow
Christian J. Dietrich

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Ausprobieren der PIN

- Beliebte PINs erraten
  - Nur wenige Versuche notwendig
  - Kandidaten: 123456, 111111, TTMMJJ...

Dem Bürger sollte an geeigneter Stelle in der AusweisApp die Festlegung einer starken PIN empfohlen werden.

Sicherheitskritisches Scripting

- Aktuelle Integration erfordert JavaScript
- Benutzer muss JavaScript im Browser aktivieren
- Generelle Aktivierung von JavaScript nicht empfehlenswert
  - Das BSI empfiehlt, JavaScript generell zu deaktivieren
  - Andernfalls ist Einschleusung von Schadcode möglich

Der Ablauf der Online-Authentisierung sollte die Ausführbarkeit von aktiven Inhalten nicht voraussetzen.

Missbräuchliche Verwendung des nPAs

- Großflächiger Missbrauch denkbar
- Vorbereitungen helfen, sich auf diese Situation einzustellen
- Im Notfall schneller Kontakt mit verantwortlichen Personen
- Gemeinsame Position nach außen

Aus Vertretern aller Stakeholder des nPA sollte ein Notfall-Konsortium gebildet werden, das im Falle eines großflächigen Missbrauchs eine schnelle, unkomplizierte Kommunikation unter den Parteien ermöglicht.

Fachhochschule Gelsenkirchen

Restrisikoanalyse Online-Authentisierung

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)
Norbert Pohlmann
Christian Rossow
Christian J. Dietrich

Institut für Internet-Sicherheit – if(is)
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.