ePerso und AusweisApp: Angriffe und Kritik

Jan Schejbal

AusweisApp

- Ermöglicht Einsatz des Ausweises im Internet
  - verbindet Benutzer, Leser, Chip und Server
- Entwickelt von OpenLimit für das BMI
- sollte ursprünglich Open Source sein
  - zweite Version ist obfuscated
- ca. 70 bzw. 50 MB, langsam, „Mischmasch“
  - zum Vergleich: Firefox ca. 8 MB

AusweisApp

ANGRIFFE

CCC-Angriff

- Keylogger kann PIN ausspähen (Basisleser)
  - keine Überraschung
  - braucht Schadsoftware auf dem Rechner
  - trotzdem von Medien aufgegriffen
- Schadsoftware kann Ausweis dann missbrauchen
- „Der Ausweis ist sicher“*

*) solange der Nutzer seinen Computer sicher hält

Mein „AusweisApp-Hack“

- AusweisApp hat ein Auto-Update
- Das Auto-Update hat ‘ne Lücke
- Angreifer kann Schadsoftware aufspielen
  - vollständige Kontrolle über den Computer
  - Daten, Passwörter, Onlinebanking, Keylogger…
- „Der Ausweis ist sicher“
  - „betrifft ja nur die App“

Updatevorgang

- AusweisApp fragt Server:
  „Was ist die aktuelle Version?“
- Server antwortet:
  „v1.0.2, Download unter https://...“
- AusweisApp lädt Update herunter und installiert es

Sicherheitsmaßnahmen (1)

- Anfrage und Download laufen über HTTPS
  - wie Onlinebanking, etc.
  - Identität des Servers über Zertifikat bestätigt
  - verschlüsselt und fälschungssicher
- Angreifer kann Updateanfrage nicht umleiten oder Antwort fälschen
  - könnte sonst Virus als „Update“ anbieten

Zertifikate

- von vertrauenswürdiger Stelle ausgestellt
- bestätigen „der Schlüssel X gehört zu Server Y“

Sicherheitschecks bei SSL/HTTPS

- Gültig (Datum, Signatur)?
- Von vertrauenswürdiger Stelle ausgestellt?
- Server hat Schlüssel?
  - Angreifer hat Schlüssel nicht
    → kann Originalzertifikat nicht nutzen
- Name im Zertifikat = Name des Servers?
  - *uuuuuuuuuuuuuuuuuups*, **wird nicht geprüft**

Angriff (1)

- Verbindung umleiten
  - viele Wege (ARP, WLAN, DNS, …)
  - Fälle sind bekannt
- Eigenes Zertifikat vorzeigen
  - bestätigt, dass mein Schlüssel zu janschejbal.de gehört
  - bekomme ich (da janschejbal.de mir gehört)
  - wird akzeptiert (Fehler: janschejbal.de != bund.de)

Angriff (1)

- eigene Antwort auf Versionsanfrage senden
  - enthält falsches Update
- Update wird angeboten
  - für Benutzer nicht von echten Updates unterscheidbar
  - wird installiert

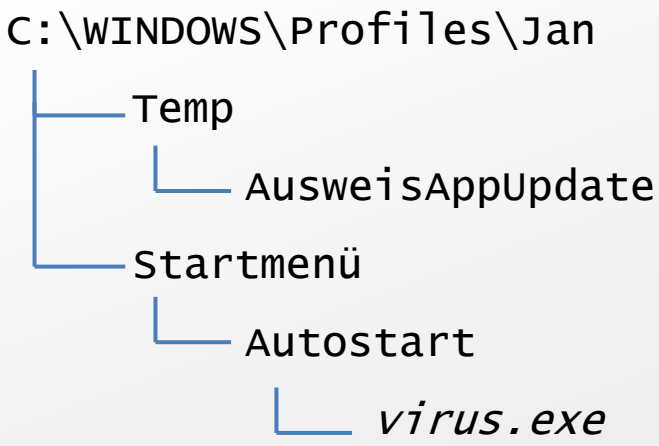
Sicherheitsmaßnahmen (2)

- Update ist eine ZIP-Datei
- enthält (unter anderem):
  - das eigentliche Update
  - digitale Signatur für das Update
    - kann nicht gefälscht werden
- ZIP-Datei wird entpackt
  - Signaturprüfung
  - ungültige Signatur → Update wird gelöscht

Angriff (2)

- ZIP wird vor der Prüfung entpackt
- Manipulierte ZIP-Datei mit „..“ in Ordnernamen
  - „..“ steht für „ein Verzeichnis höher“
- Daten werden außerhalb des vorgesehenen Verzeichnisses entpackt (Fehler!)
  - werden nicht gelöscht
  - Autostart-Ordner

Angriff (2)



(Pfade vereinfacht)

- Dateien werden entpackt nach
  `C:\WINDOWS\Profiles\Jan\Temp\AusweisAppUpdate`
- ZIP enthält Virus im „Ordner“
  `..\..\Startmenü\Autostart`
- Wird entpackt nach:
  `C:\WINDOWS\Profiles\Jan\Temp\AusweisAppUpdate\..\..\Startmenü\Autostart`
- Und das ist:
  `C:\WINDOWS\Profiles\Jan\Startmenü\Autostart`

Zusammenfassung

- Zwei gute Sicherheitsmaßnahmen
- Zwei dumme Programmierfehler
- Angreifer, der die Updateanfrage umleiten kann, kann Viren einspielen
  - komplette Kontrolle über den Rechner!
  - Keylogger-Angriff möglich
- inzwischen behoben

Einschätzung

- realistischer Angriff
  - Umleiten der Updateanfrage möglich
  - nur bedingt „massentauglich“
- schwere Folgen
  - Vollzugriff auf System!
  - ePerso-Chip und Protokolle nicht betroffen
    - bringt dem Opfer wenig
- Fehler: peinlich, aber kann passieren

Zweiter Angriff: PIN-Klau

- PIN klauen ohne Virus auf dem Rechner

DEMO

https://fsk18.piratenpartei.de

Laaaangweilig

- Bunte Bilder auf einer Website
  - Screenshots der AusweisApp
  - ein wenig JavaScript
- Nutzer erkennt falsches Fenster nicht
  - Sicherheitsmerkmale vorhanden
  - Nutzer müssten aufgeklärt werden
  - AusweisApp wird von fremden Websites gestartet

Beurteilung

- Eher peinlich-billig
  - aber: CCC-Angriff war auch relevant
  - billig, **aber funktioniert**
  - kein Programmierfehler, fehlende Aufklärung
- Eingeschränkter Effekt
  - PIN nutzt wenig ohne Zugriff auf Ausweis
  - Ausweis kann drahtlos ausgelesen werden

Sicherheit allgemein

- Es wurde nachgedacht
- Protokolle z. T. formal verifiziert
  - erfolgreiche „Frontalangriffe“ unwahrscheinlich
  - um die Ecke denken!
- „Der Ausweis ist sicher“ → **nein!**
- **Sicher nur wenn PC sicher**
  - zum Teil auch bei besseren Lesegeräten

KRITIK

Unnötig

- „alter“ Perso fälschungssicher
- Ausweisfunktion im Internet mit existierenden Technologien möglich
  - als separate Karte sinnvoller
  - existierende Standards
  - billiger

Basislesegeräte

- billig
- PIN wird am PC eingegeben
  - PC muss sicher sein
- unsicher
- 1,5 Mio. Stück kostenlos verteilt
- Sicherheit vs. Akzeptanz

Unterschied QES/eID

- Qualifizierte Elektronische Signatur = hoher Sicherheitsstandard
  - geht mit ePerso oder normaler Signaturkarte
  - sicheres Lesegerät vorgeschrieben
- eID-Funktion = niedriger Sicherheitsstandard
  - Basisleser
  - anfälligere Technik

eID-Funktion

- eID soll QES nicht ersetzen
- soll zum Identitätsbeweis, nicht zur Bestätigung von Transaktionen dienen
  - oder doch?
- eID als Anscheinsbeweis bei Bestellungen
- Für Händler super, für Nutzer gefährlich
- QES-Zertifikat über eID holen? (gefährlich!)

Wirtschaftsförderung, Kosten

- Bundesdruckerei **GmbH**
- Hardwarehersteller
- 28,80 € statt 8 €
- 1,5 Mio. Basisleser an Firmen verschenkt
- Richtige Lesegeräte: 169 EUR pro Stück
- Signaturzertifikate nicht inklusive (20 €/Jahr)

Technologieexport

- Hoffnung, neuen internationalen Standard zu schaffen (=Exportmöglichkeiten)
- Entscheidungen davon beeinflusst?
  - Eigene Technik statt bewährter Standards
  - Drahtlos statt mit Kontakten

  Klasse 3 Kartenleser (normal): 40 EUR
- Regierung + IT-Projekt = …

Sicherheit

- Sicherheit wird übertrieben
- Neue Angriffswege?
  - Ausweis 10 Jahre gültig!
  - RFID fingerprinting?
- Theoretische Möglichkeit von Backdoors

Politische Missbrauchsgefahr

„Vermummungsverbot im Internet“

Axel E. Fischer (CDU),
Vorsitzender der Enquete-Kommission
Internet und digitale Gesellschaft (!)

„Es kann nicht sein, dass sich viele Bürger in Foren oder anderen Einrichtungen des Netzes hinter selbstgewählten Pseudonymen verstecken (…). ***Der neue elektronische Personalausweis bietet eine ideale Möglichkeit****, sich im Internet zu identifizieren. Das betrifft nicht nur* ***die Beteiligung des Bürgers an der politischen Willensbildung****, sondern ebenso seine Möglichkeit zu wirtschaftlicher Betätigung im Netz.“*

CeBIT 2011

- Erster (!) Komfortleser erst jetzt zertifiziert
  http://heise.de/-1202270
  - lieferbar ab April
  - Standardleser gibt es schon länger
- AdHoc-Signaturen (QES!) über eID
  http://heise.de/-1201103
  - Gelddruckmaschine (10-20 €/Sig.)
  - Komfortleser sollen billiger werden: „nur“ 100 €

CeBIT

- Kostenloser Eintritt
  - PIN an fremdem Lesegerät eingeben?
  - könnte als normales Szenario geplant sein
  - gefährlich!

Zusammenfassung

- fast nur Nachteile für Bürger
  - Kosten
  - Haftung
  - mangelhafte Sicherheit
  - wenig Nutzen
- politische Missbrauchsgefahr

Empfehlungen

- Bürger
  - vermeiden
  - Alufolie hilft
- Politik
  - einstampfen
  - ggf. existierende Standards fördern

Vielen Dank für Eure Aufmerksamkeit!

Fragen?