

# Anmerkungen zur Verwundbarkeit mobiler Web-Browser

Michael Becher

Universität Mannheim, becher@informatik.uni-mannheim.de

Die Sicherheit mobiler Endgeräte mit SIM-Karte und durch Fremdsoftware erweiterbarem Betriebssystem (*Smartphones*) ist heute ein aktives Feld, denn die mobile Welt unterscheidet sich von der heutigen PC-Welt durch die immer vorhandene Möglichkeit, schnell hohe Kosten für den Mobilfunkbenutzer zu erzeugen. Die einfachste Maßnahme zur Erhöhung der Sicherheit ist das vollständige Schließen des Betriebssystems gegenüber Fremdsoftware. Doch die Erfahrung hat gezeigt, dass dies keine durchsetzbare Lösung ist.<sup>1</sup> Ein anderer Ansatz stellt Funktionen nur über Anwendungsrahmenwerke bereit. Beispiele sind J2ME oder Dotnet, die nicht alle Funktionen des Betriebssystems zugreifbar machen. Eine weitere Maßnahme ist das kryptographische Signieren von Anwendungen, die den Zugriff auf sicherheitskritische Funktionen oder sogar deren Benutzung ohne Rückfrage an den Benutzer erlauben.

Neue Entwicklungen in der Mobilfunkwelt rücken den mobilen Web-Browser in eine exponierte Position. Einerseits nimmt die Nutzung von mobilen Datendiensten stetig zu und damit auch die Nutzung des mobilen Browsers. Andererseits werden mobile Browser zur Zeit mit vielen Funktionen erweitert, die sie selber zu einem vollständigen Anwendungsrahmenwerk machen.<sup>2</sup> Die Erfahrung zeigt, dass bei solchen Aktivitäten zumeist die Funktionalität der Sicherheit untergeordnet wird. Der mobile Browser wird damit ein weiterer Angriffsvektor für das mobile Endgerät. Beispiele für erfolgreich ausgenutzte Schwachstellen sind verschiedene Denial-of-Service-Angriffe auf den Internet Explorer Mobile<sup>3</sup> und prominent der Jailbreak des iPhones für Firmware-Version 1.1.1, der trotz Behebung der alten Umgehung die Installation von Fremdsoftware wieder ermöglichte, allein durch Aufruf einer Web-Seite.<sup>4</sup>

Es stellen sich dabei zwei Fragen: 1. Können gefundene Schwachstellen des Browsers effizient behoben werden? 2. Wie kann der Benutzer Schaden gegen seine persönlichen Schutzinteressen abwenden?

Bei aktuellen Smartphones ist die entfernte Behebung von Schwachstellen möglich. Das ist zum einen die entfernte Behebung angestoßen durch Benutzeraktion (am PC oder auf dem Gerät laden und Aktualisierung ausführen) oder angestoßen durch den Mobilfunkbetreiber (Push). Die erste Frage kann somit für aktuelle Smartphones bejaht werden.

Die zweite Frage ist nicht leicht zu beantworten. Denn der Benutzer sieht sich einer Vielzahl von Technologien mit ihren eigenen Schutzmechanismen gegenüber, aktuell die Initiative „BONDI“<sup>5</sup>, die auch zum Ziel hat, den mobilen Browser zu einem Anwendungsrahmenwerk auszubauen, allerdings mit deutlichem Fokus auf der Sicherheit des Benutzers. Vielleicht wäre eine Lösung besser, die dem Benutzer die vollständige Macht über sein Gerät gibt bezüglich seiner Sicherheitsinteressen, und zwar unabhängig von einer speziellen Technologie, geräteweit in der Art einer erweiterten persönlichen Firewall zum Schutz vor finanziellem Schaden und vor dem Verlust der Vertraulichkeit seiner persönlichen Informationen auf dem Mobiltelefon. Doch das ist nicht mehr Teil der reaktiven Sicherheit und soll deshalb an anderer Stelle vertieft werden.

<sup>1</sup>Orange SPV: <http://developer.orangews.com/orgspv/comdefq.aspx>,  
iPhone: <http://www.heise.de/newsticker/meldung/97556>

<sup>2</sup>Opera Widgets: <http://www.opera.com/products/mobile/widgets/>

<sup>3</sup>z.B. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0685>

<sup>4</sup><http://jailbreakme.com>, <http://blog.metasploit.com/2007/10/cracking-iphone-part-1.html>

<sup>5</sup><http://www.omtp.org/News/Display.aspx?Id=9e9a5f27-a57e-4804-b736-379b1d98b169>

# Anmerkungen zur Verwundbarkeit mobiler Web-Browser

SPRING  
Mannheim  
08.08.2008

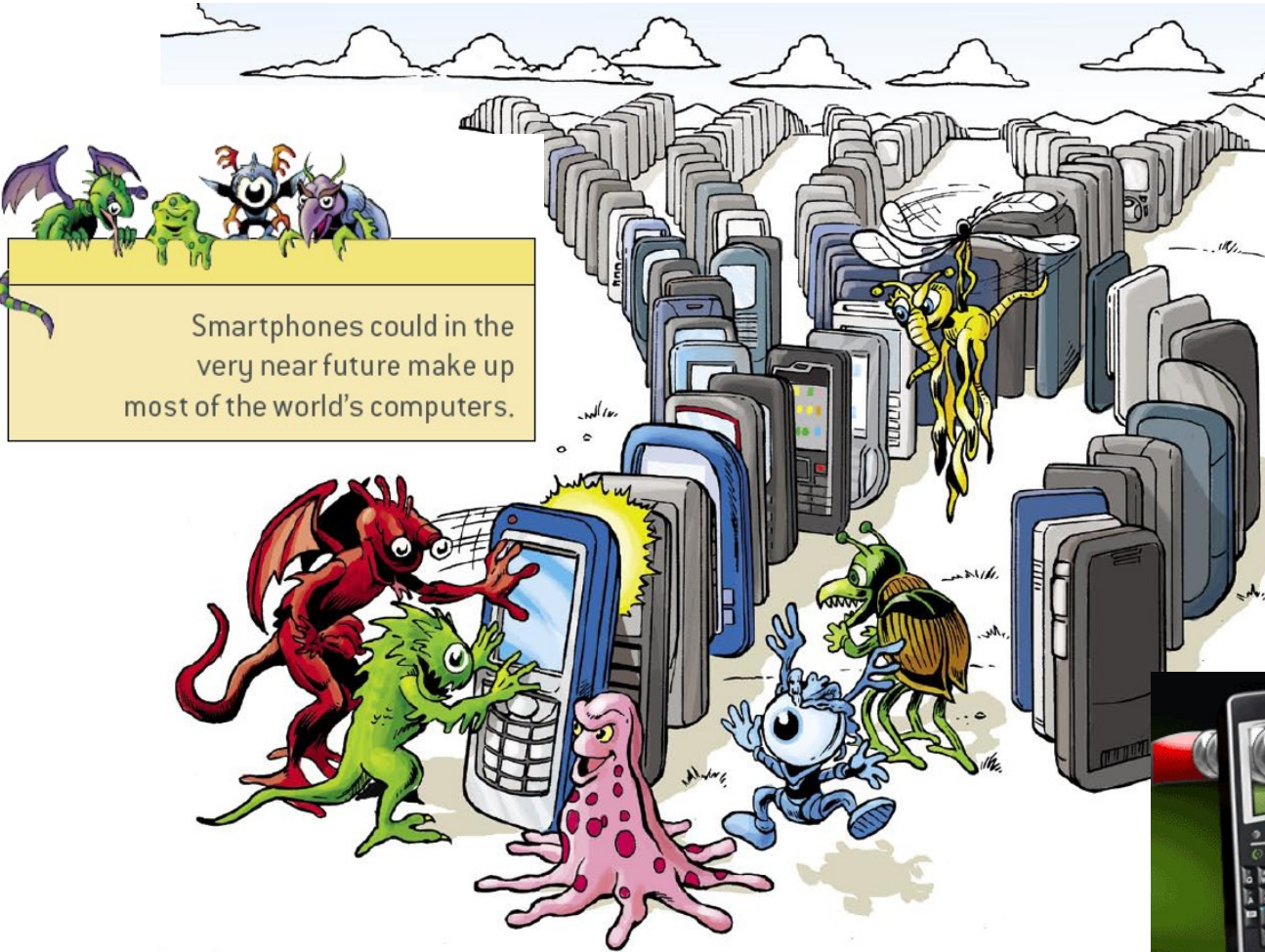
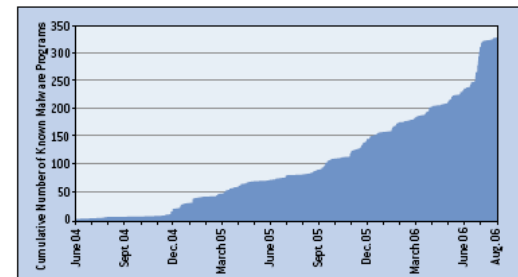


# Mobile Sicherheit



Computers do not have a built-in billing system; mobile phones do. The bad guys will exploit this feature before long.

GROWTH IN MOBILE MALWARE



Smartphones could in the very near future make up most of the world's computers.

# Die mobile Welt (1/2)

Unterschiede mobile Sicherheit vs. herkömmliche Sicherheit

- Inhärente Möglichkeit, Kosten zu erzeugen
  - Dialer-Problematik auf PCs ist rückläufig (nur noch DSL)
- Engere Verbindung des Netzbetreibers zu den Endgeräten
  - Mehr Möglichkeiten durch SIM („trusted module“)
- Dadurch auch Reputation des Netzbetreibers
- Begrenzte Ressourcen (Prozessor, Akkulaufzeit)
  - Wird im mobilen Umfeld immer der Fall sein
  - Rechenintensive Operationen vermeiden
  - Auslagern ins Netz? (Aber nächster Punkt!)
- Luftschnittstelle immer teuer
  - Lösungen/Protokolle/Algorithmen sollen Kommunikation vermeiden
  - Nicht im Sinne von „Kosten für den Benutzer“

# Die mobile Welt (2/2)

- Offene (erweiterbare) Systeme werden sich durchsetzen
  - Beispiele: Orange SPV, Apple iPhone
- Fremdsoftware („3<sup>rd</sup> party“) durch Anwendungsrahmenwerke („application frameworks“) erlauben
  - Nicht alle Funktionen des Betriebssystems zugreifbar machen
  - Beispiele: J2ME, Dotnet
- Kryptographisches Signieren von Anwendungen
  - Bestimmte APIs nur zugreifbar bei entsprechender Signatur
  - Verteilung der Zertifikate (wie immer) logistisches Problem
  - Z.B. in J2ME, Symbian OS „Capabilities“

# Behebung von Schwachstellen

- *Lokale* Behebung (d.h. Flash beim Service - früher)
- Entfernte Behebung durch Benutzer-*Pull*  
(im mobilen Browser oder am PC laden und ausführen, Bsp. iPhone)
- Entfernte Behebung durch *Push*  
(Bsp. Danger Sidekick)
  
- Update „over-the-air“ erzeugt Kosten
- Update am Rechner erfordert manuelles Eingreifen
- Dauerhaftigkeit der Updates heute tendenziell eher gegeben
- Gerät mit dem Rechner verbinden
  - Ist üblich beim iPhone: Update über iTunes
  - Regelmäßigkeit kann aber nicht vorausgesetzt werden

# Mobile Browser

- Internet Explorer Mobile
  - JScript, Flash
- Opera Mobile
  - Portierung für Windows Mobile und Symbian OS
  - Alle Features der Desktop-Version, Flash/FlashLite, Netscape Plugins
  - Opera stellt keine Updates zur Verfügung
  - „Opera Mini“ ist Java-Version (J2ME)
- WebKit Browser Engine
  - Basierend auf KHTML
  - Quelloffen
  - Benutzt in: iPhone, Nokia Series 60, Android
- Firefox Mobile
  - Linux (Nokia N800), Windows Mobile

# Browser als Application Framework

- Web-Anwendungen populär (schnelle Entwicklung)
- Funktionalität vor Sicherheit?
- Stichwort „Widgets“
  - Prominent: Opera Widgets
- OMTP BONDI
  - Aktuelle Initiative viele Netzbetreiber (seit Juli 2008)
  - „will provide a consistent and secure web services interface that can be used by all web developers across multiple device platforms.“
  - „will be engineered in such a way as to prevent fraudulent and malicious activity through unauthorised access to functions or sensitive personal information“

# Bekannt gewordene Schwachstellen

- CVE-2007-0685
  - „cause a denial of service (application crash and device instability) via unspecified vectors, possibly related to a buffer overflow.“
- CVE-2007-0878
  - „allows remote attackers to cause a denial of service (loss of browser and other device functionality) via a malformed WML page“
- Mögliche Übertragbarkeit von Schwachstellen der PC-Browser
  - Funktionalität der Browser-Varianten gleicht sich an, Code-Basis gleich
  - Patch-Prozesse sind (teilweise) noch unklar
- Month of Browser Bugs (Juli 2006)
  - Hauptsächlich Schwachstellen in ActiveX-Controls
  - ActiveX im IE Mobile vorhanden
  - Allerdings keines der verwendeten Controls installiert

# iPhone Jailbreak

- iPhone Firmware-Version 1.1.1 konnte über den Browser entsperrt werden ([jailbreakme.com](http://jailbreakme.com))
- Alte Version von libtiff benutzt mit bekannten Schwachstellen
  - Behoben in Mac OS X schon 08/2006
  - Behoben im iPhone durch Firmware-Version 1.1.2 erst 11/2007
- Übertragung eines alten Exploits von PSP möglich
- Interessante Frage: Hat diese Schwachstelle langfristige Auswirkungen? Oder war es ein kalkuliertes Übel?
- Lehren für die mobile Sicherheit:
  - Sobald eine Plattform genügend Aufmerksamkeit bekommt, geht das Finden von Schwachstellen sehr schnell

# Zukunft

- Wie Schaden abwenden von den Benutzern?
  - Dieser Teil nicht mehr reaktive Sicherheit...
- Gebt den Benutzern die Macht über ihr Gerät (zurück)
  - ... unabhängig von einer benutzten Technologie ...
  - ... geräteweit durchgesetzt ...
  - ... „erweiterte persönliche Device Firewall“ ...
  - ... zum Schutz vor finanziellem Schaden ...
  - ... zum Schutz vor dem Verlust von Vertraulichkeit ...
- Aber:
  - Kommt in den Bereich von (teilweise existierenden) Policy-Produkten
  - Deshalb fraglich, ob wissenschaftliche Beschäftigung damit lohnend
  - Besonderheit des „vertrauenswürdigen Moduls“ SIM-Karte benutzbar?

# Zusammenfassung

- Mobile Browser
  - werden immer mehr benutzt
  - ihre Schwachstellen werden mehr Aufmerksamkeit bekommen
  - gleichen immer mehr ihren Desktop-Verwandten
  - werden ausgebaut zu vollständigen Application Frameworks
- Diese ***Verschiebung der Grenzen*** herkömmlicher Schutzmechanismen zu beobachten ist jetzt interessant!

Frage:

Hat jemand Erfahrung mit Verwundbarkeiten von PC-Browsern?

# Danke für die Aufmerksamkeit!

Michael Becher

`becher@informatik.uni-mannheim.de`