A9: Mobile Security - So werden Sie angegriffen!

SWITCH
Serving Swiss Universities

Renato Ettisberger
renato.ettisberger@switch.ch

Zürich, 11. Oktober 2011

Security (SWITCH-CERT)

Derzeit 7 Mitarbeiter, bald 10

Unser Team erbringt Security-Dienstleistungen für Universitäten/ Hochschulen & Schweizer Banken

National und international vernetzt

Langjährige Erfahrung in

- Incident Handling
- Malware-Analyse
- Forensics
- Risk Assessment, Penetration Testing

Smartphone Marktanteile 2010 in CH

Quelle: weissbuch.ch

Anzahl verkaufter Mobilephones : ca. 3‘968‘000

Anzahl an Smartphones: 1‘512‘000 (ca. 40%)
(303 Millionen weltweit; Zunahme von 75%)

50% aller verkauften Smartphones waren iPhones

22.9% der verkauften Smartphones waren Android-basierte Geräte

Der Rest teilt sich auf unter Nokia, Blackberry, Windows Mobile etc.

Wo sind die Risiken?

- Orts- und zeitunabhängiger Zugriff auf wichtige Daten
- Sensitive Daten werden auf den Geräten gespeichert bzw. darüber eingegeben
- Aufzeichnen von Gesprächen / Meetings etc.
- Verlust der Geräte: Daten verschlüsselt?
- Ideal für gezielte Angriffe
- AV-Software?

Alles nur Theorie?

Pwn2own 2011

iPhone 4 und Blackberry Torch gehackt

Am zweiten Tag des Hacker-Wettbewerbs Pwn2own hat Seriensieger C genutzt und das iPhone 4 gehackt. Auch das Blackberry Torch 9800 hat Firefox und Chrome blieben weiter unangetastet.

McAfee Labs :

« Previous post in McAfee Labs Next post in McAfee Labs »

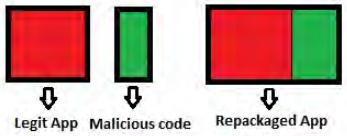
Rooting Exploit for Android Works Silently

Thursday, September 15, 2011 at 9:26am by Arun Sabapathy

In our last blog about Android malware, we discussed the expanding threat landscape for Android malware. Recently, we received an Android package in our collection and observed that this malicious application uses a rooting exploit that targets Android devices running OS Versions 2.3 or earlier to gain root privileges on the compromised device.

The malware binary is packaged with a legitimate application. In this case, the malicious exploit code comes with "Daily Beauties," which showcases pictures of celebrities that are updated periodically. Attackers use this repacking approach to hide their malware within genuine applications, which users will download and install.

The following image represents the repacking a legit application with malicious code. These repackaged applications are made available in Android black markets and third-party markets.



ZeuS attackiert Windows-Mobile-Nutzer

Kaspersky Lab warnt vor Angriffen auf Windows-Mobile-Anwender. Bei diesen handelt es sich um alte Bekannte, allerdings

Zeus-Trojaner nun auf BlackBerry-Smartphones aktiv

07.03.2011 | 16:16 von Ralf Müller

Trend Micro warnt die BB-Besitzer vor drohender Gefahr. Die sei diesmal nicht nur theoretisch, denn der Trojaner sei auf normalen Smartphones gesichtet worden.

Allgemeine Angriffsmöglichkeiten

a) Anhang öffnen / ausführen

b) Schadsoftware via *App Store*, *Android Market* etc.

c) Schwachstellen in Applikationen

Anhang öffnen / ausführen

Bild: http://news.cnet.com/8301-27080_3-20006882-245.html

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

ZeuS ist eine Schadsoftware, die sich gegen Internet-Banking Nutzer richtet.

Der Schädling ist bereits seit mehreren Jahren in unterschiedlichen Ländern aktiv.

Prinzip:

- PC des Opfers wird mit Schadcode infiziert
- Zugangsdaten zum Online-Banking werden abgegriffen

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

1. Angreifer infizieren PC mit Schadsoftware.

2. Zugangsdaten für das Internet-Banking werden mitgeschnitten.

3. Mittels Code-Injection in die aufgerufene Bankenwebseite wird der Benutzer aufgefordert, seine Handynummer einzugeben.

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

Bild: http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-ii.html

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

4. Dank der so gesammelten Handynummer erhält das Opfer ein SMS mit einem Link zu einem „Zertifikat“.

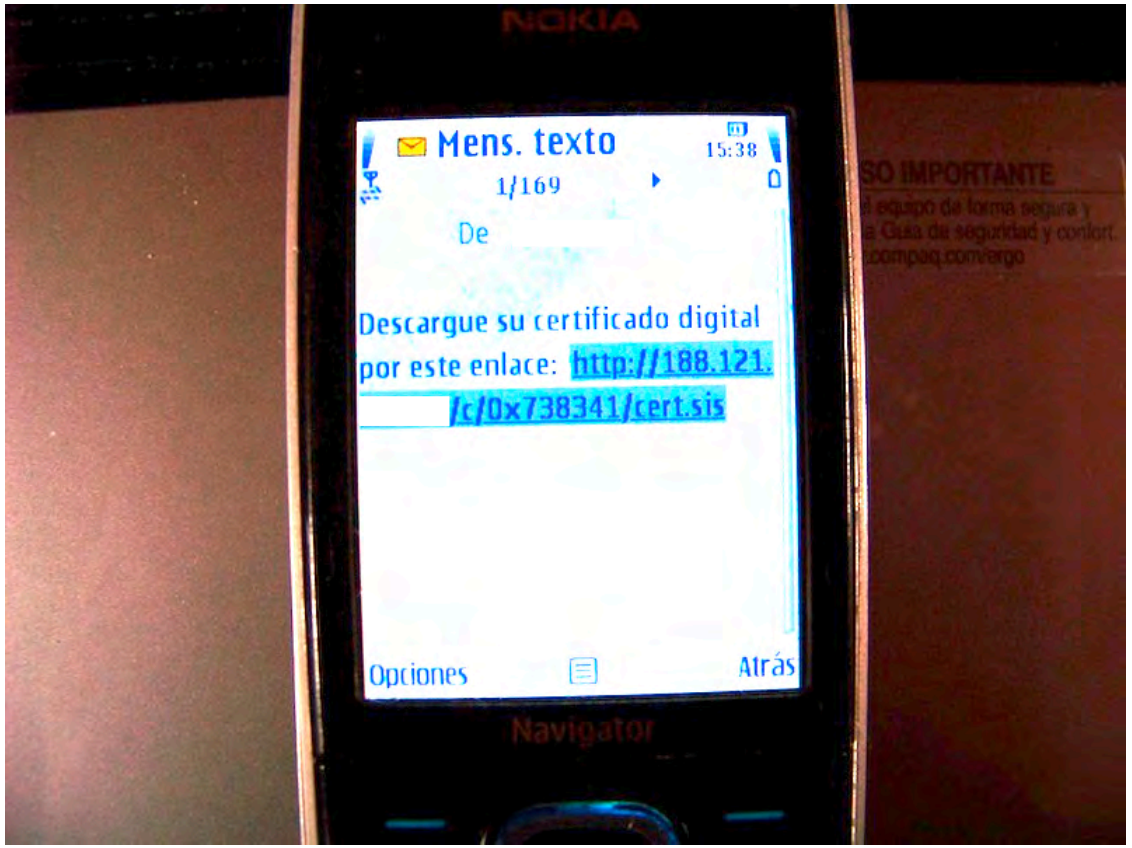


Bild: http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-ii.html

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

5. Das „Zertifikat“ installiert eine Hintertüre auf dem Gerät. Befehle der Angreifer können über eingehende SMS ausgeführt werden. Der Benutzer sieht diese SMS nicht.

6. Sämtliche SMS können an die Angreifer gesandt werden. Diese besitzen nun alle Informationen (Benutzername, Passwort, mTAN), um das Konto zu plündern.

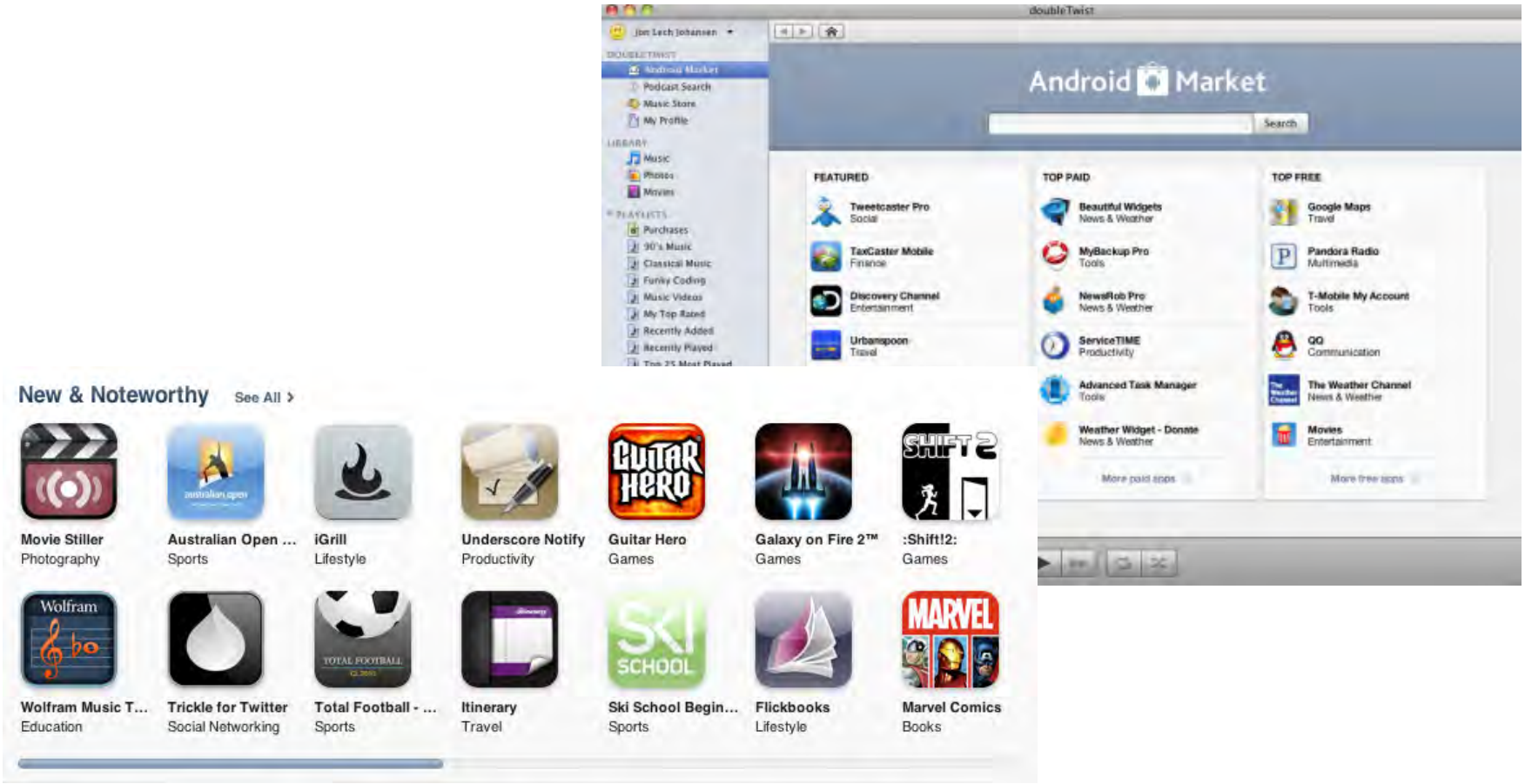
Angreifer unterstützen in diesem Fall vier Hersteller / Plattformen:

- BlackBerry
- Nokia (SymbianOS)
- Windows Mobile
- Android

Anhang öffnen / ausführen

Beispiel anhand von ZeuS in the mobile (Zitmo)

Schadsoftware auf App Store/Android Market



Schadsoftware auf App Store/Android Market

Verschiedene Hersteller bieten so genannte App Store Lösungen an.

Die bekanntesten sind Apples *App Store* sowie Googles *Android Market*.

Dadurch können Benutzer zusätzliche Applikationen auf ihr Smartphone laden.

Jedermann kann Applikationen über diese Stores anderen Nutzern zur Verfügung stellen.

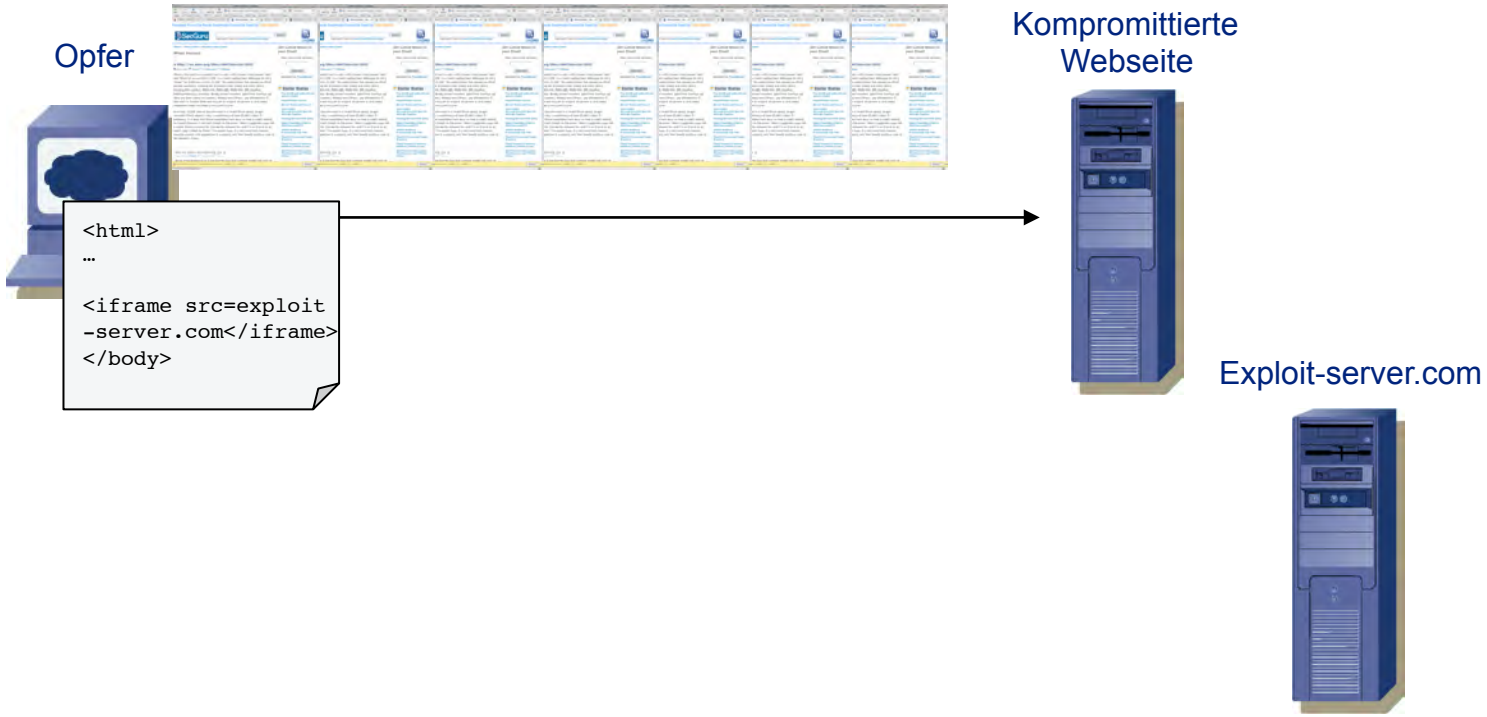
Idealer Verteilweg für Schadcode?

Schwachstellen in Applikationen

Bild: http://www.iphone-ticker.de/2007/08/16/video-ein-blick-auf-launcherapp/

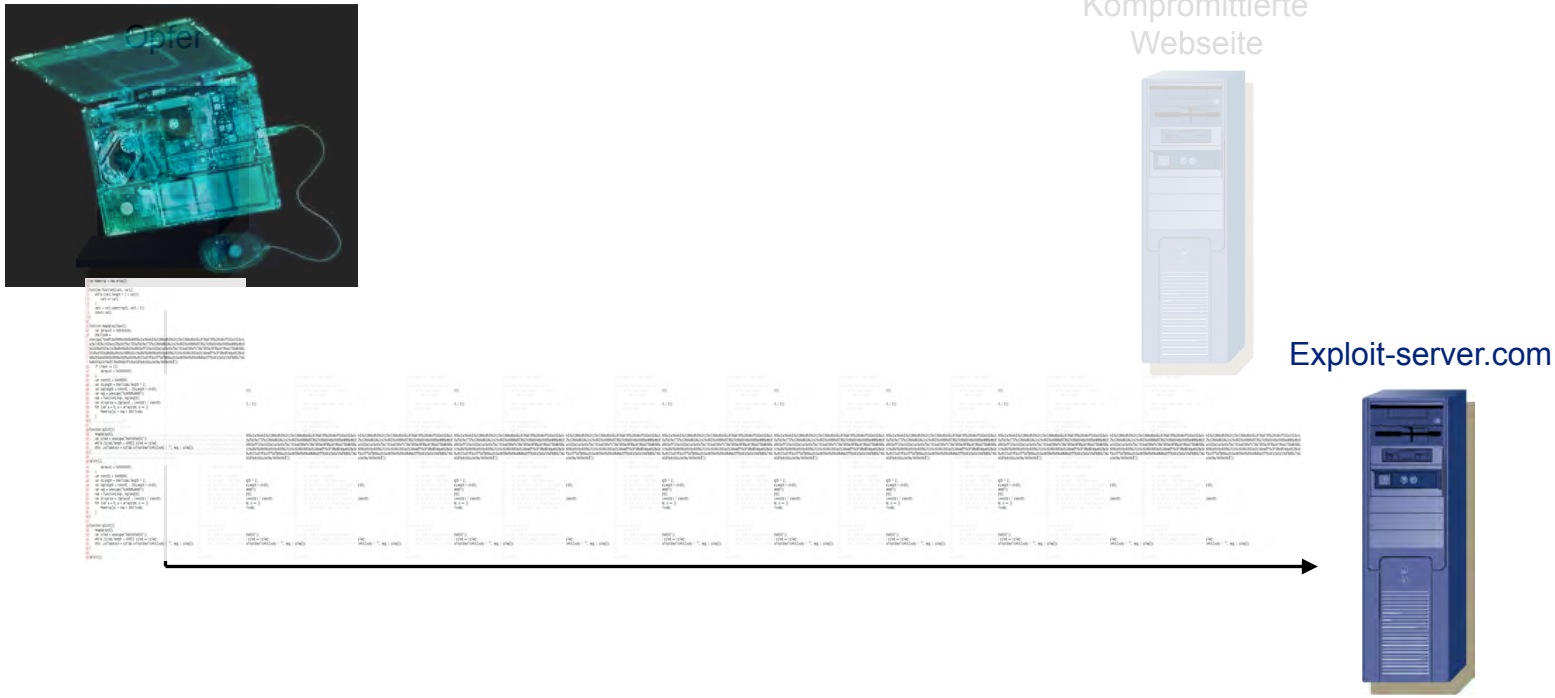
Schwachstellen in Applikationen

Drive-by Infection (1/4)



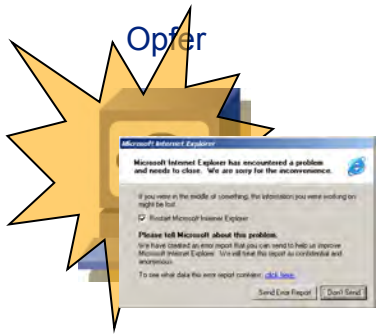
Schwachstellen in Applikationen

Drive-by Infection (2/4)



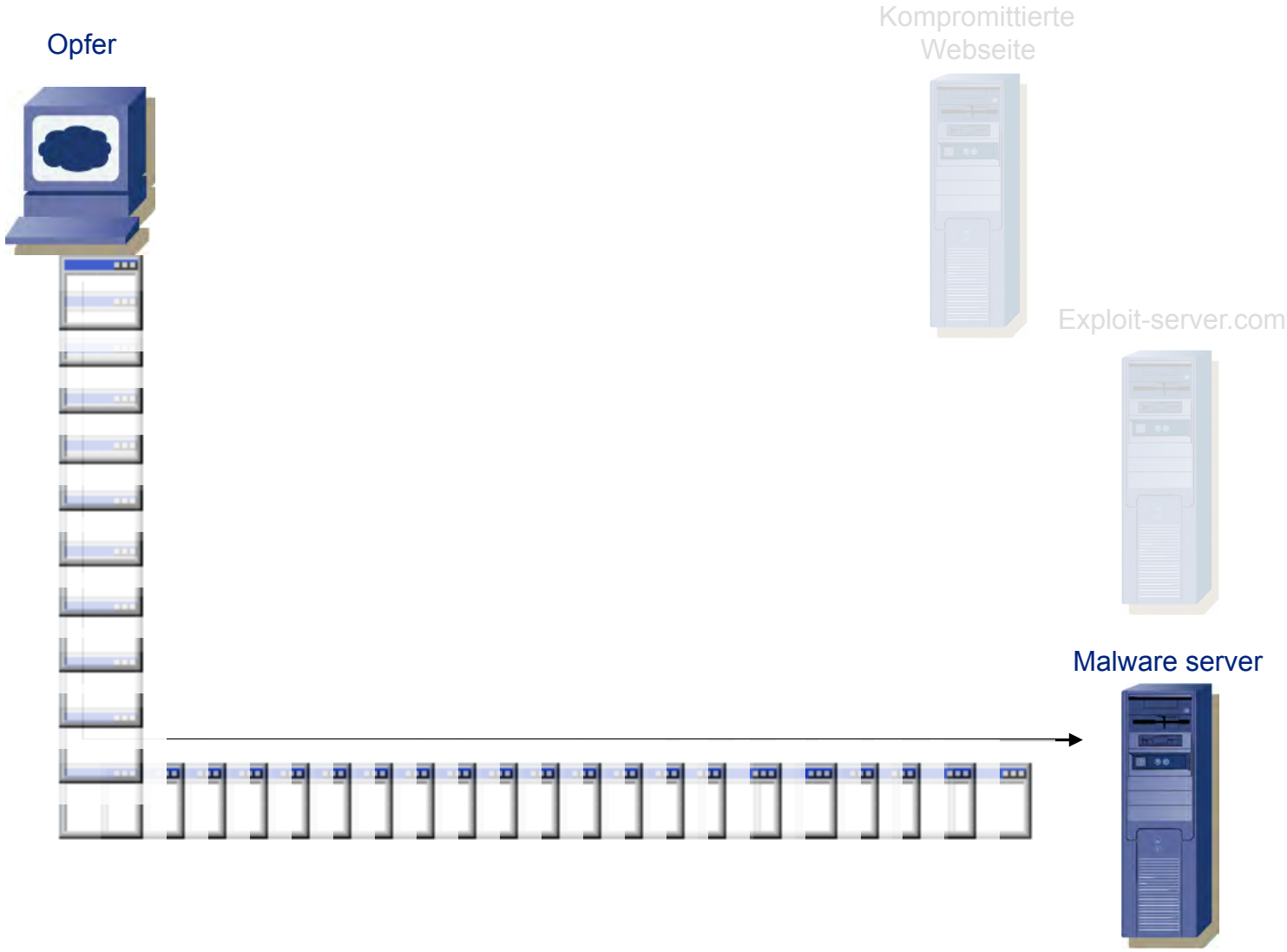
Schwachstellen in Applikationen

Drive-by Infection (3/4)



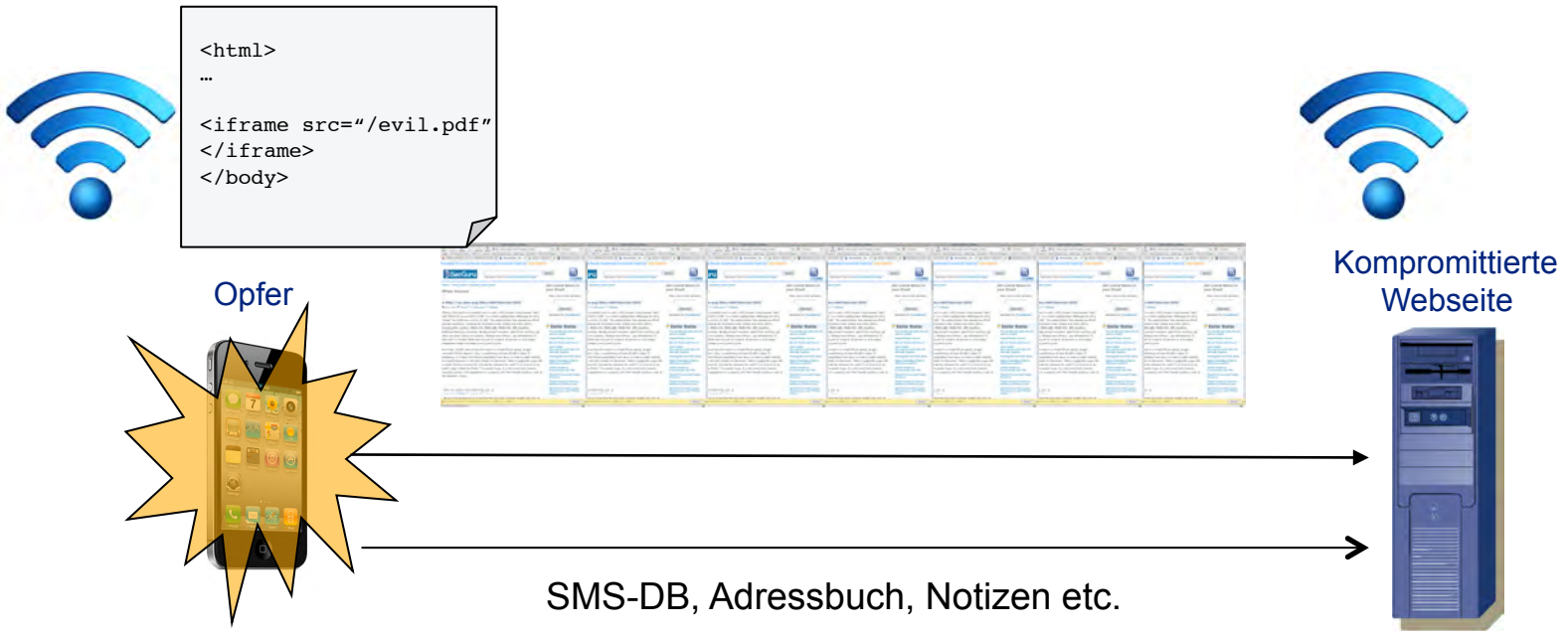
Schwachstellen in Applikationen

Drive-by Infection (4/4)



Schwachstellen in Applikationen

Setup & Ablauf der Demo



Auf dem Server:

- Wireless Access-Point
- DNS-Server
- DHCP
- Webserver
- Fake-Webseite

Fallbeispiel
iPhone vs. Android

Allgemeines

- “Geschlossenes” System
- iOS basiert auf Mac OS X
- Läuft nur auf Apple-HW
- Nur ein App Store (Apple)

- Open Source
- Basiert auf Linux-Kernel
- Verschiedene Anbieter nutzen Android
- Android Market (Google) plus alternative Marketplätze!

Apps

Review & Signierung

- Jeder kann Apps entwickeln
- Jede App wird von Apple analysiert bevor sie auf dem App Store landet
- Apple signiert die App
- Nicht sichtbar, welche Rechte die App einfordert

- Jeder kann Apps entwickeln
- Kein Review-Prozess der App auf Seiten von Google etc. vorhanden
- Entwickler signiert die App
- Benutzer sieht, welche Rechte die App einfordert

Apps

Wer entscheidet, was gut und böse ist?

- Jeder kann Apps entwickeln
- Jede App wird von Apple analysiert bevor sie auf dem App Store landet
- Apple signiert die App
- Nicht sichtbar, welche Rechte die App einfordert

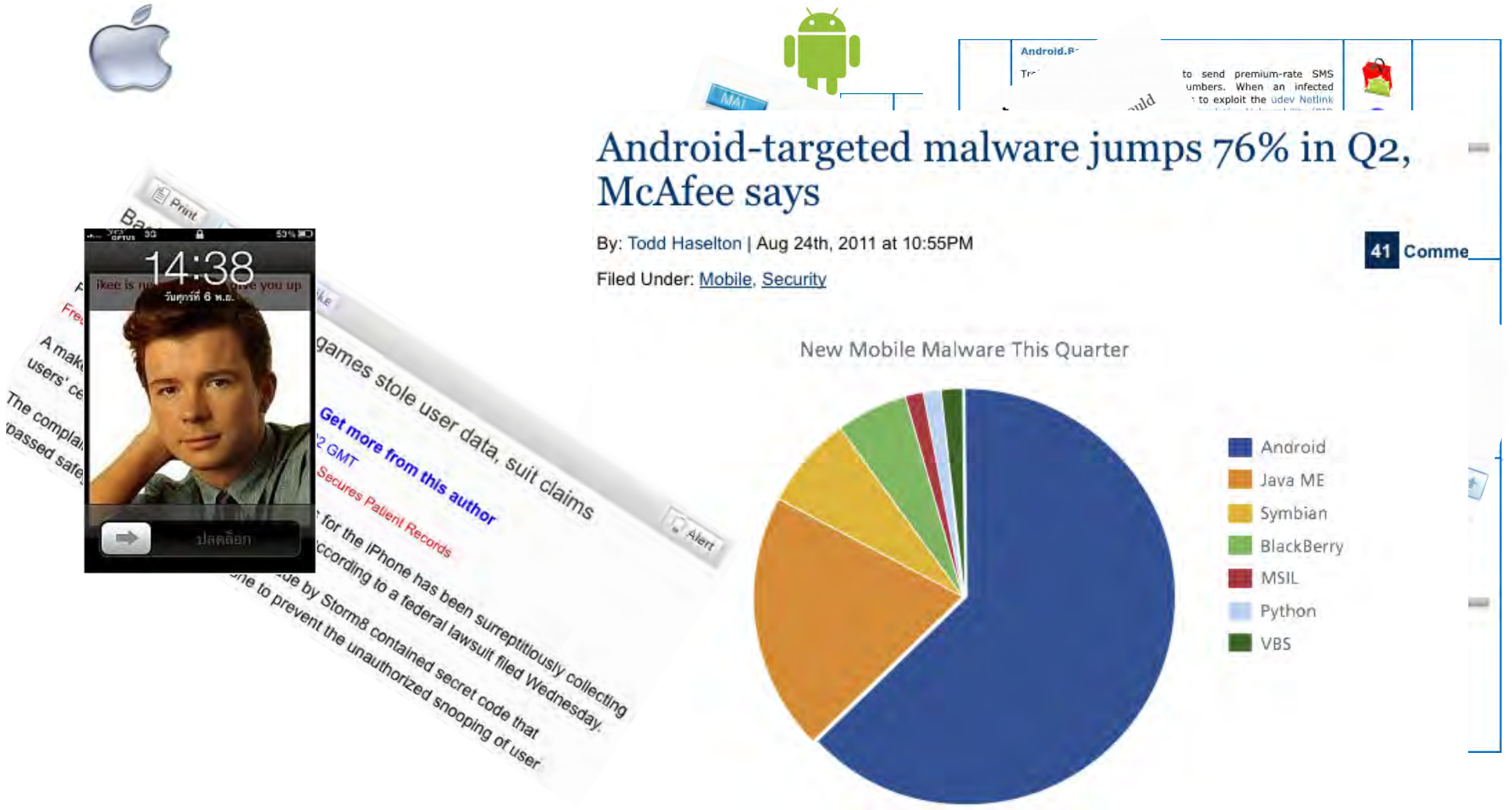
Apple

- Jeder kann Apps entwickeln
- Kein Review-Prozess der App auf Seiten von Google vorhanden
- Entwickler signiert die App
- Benutzer sieht, welche Rechte die App einfordert

Enduser

Ergebnis

Wer entscheidet, was gut und böse ist?



Quelle: https://paulsparrows.wordpress.com/2011/08/11/one-year-of-android-malware-tu… ist/

Update-Mechanismus bei OS

- Automatisch über iTunes
- Wenn Updates da sind, können sie direkt eingespielt werden

- Updates sind verfügbar
- Allerdings haben die einzelnen Hersteller unterschiedliche Update-Strategien
- Auch abhängig vom Service Provider, ob er Updates „frei gibt“

→ Benutzer kann häufig gar nicht updaten

Security-Massnahmen

		
Ja	DEP	Nein
Ja	ASLR	Nein
Ja	Mandatory Code Signing	Nein

XSS in Skype for iOS

Skype for iOS contains an XSS vulnerability that allows attackers steal information.

A Cross-Site Scripting vulnerability exists in the "Chat Message" window in Skype 3.0.1 and earlier versions for iPhone and iPod Touch devices.

Skype uses a locally stored HTML file to display chat messages from other Skype users, but it fails to properly encode the incoming users "Full Name", allowing an attacker to craft malicious JavaScript code that runs when the victim views the message.

To demonstrate the vulnerability, I captured a photo of a simple javascript alert() running within Skype.

Executing arbitrary Javascript code is one thing, but I found that Skype also improperly defines the URI scheme used by the built-in webkit browser for Skype. Usually you will see the scheme set to something like, "about:blank" or "skype-randomtoken", but in this case it is actually set to "file://". This gives an attacker access to the users file system, and an attacker can access any file that the application itself would be able to access.

File system access is partially mitigated by the iOS Application sandbox that Apple has implemented, preventing an attacker from accessing certain sensitive files. However, every iOS application has access to the users AddressBook, and Skype is no exception. **I created a proof of concept injection and attack that shows that a users AddressBook can indeed be stolen from an iPhone or iPod touch with this vulnerability.**

To further demonstrate the issue, I have recorded a video of this scenario. Please use the comments section below for your questions.

XSS in Skype

Fazit & Massnahmen

Erstes Fazit

iPhone

+ Code Signing, nicht-ausführbarer Stack und Heap.

+ Mit der Einführung von ASLR wird die Hürde für Angreifer weiter erhöht (ab iOS Version 4.3).

+ Apples Review-Prozess (wenn er funktioniert).

- Apples Review-Prozess (wenn er nicht funktioniert).

- Apps laufen nicht mit separater UID (siehe Demo).

Erstes Fazit

Android

+ Sandbox-Prinzip durch eigene UID pro App schränken die Auswirkungen eines Angriffes ein.

+ Benutzer sieht, was er installiert bzw. welche Rechte die App einfordert.

+ verschiedene Hersteller (Konkurrenzdruck)

- Kein Review-Prozess (Benutzer muss entscheiden, welche App gut oder böse ist).

- Ausführbarer Stack/Heap; kein richtiges ASLR.

- Verschiedene Hersteller (Hinzufügen von Funktionen, Updates? etc.)

Empfehlungen

Software stets aktuell halten

Zugangscode setzen

Keine Attachments / Links in SMS aus unbekannter Quelle öffnen

Telefonrechnung stets prüfen

Kommentare bei Apps beachten und nicht der Erste sein, der eine neue App aus dem Store installiert

Daten richtig löschen, bevor man das Handy verkauft

Backup!

Links

“ShmooCon 2011: Defeating mTANs for profit”, Axelle Apvrille and Kyle Yang
http://www.youtube.com/watch?v=5X0SGgZtX8w

“Examining the recent Android malware”, Jon Larimer
http://blogs.iss.net/archive/Examining%20the%20recent.html

“Fun and Games with Mac OS X and iPhone Payloads”, Iozzo, Miller
http://blackhat.com/presentations/bh-europe-09/Miller_Iozzo/BlackHat-Europe-2009-Miller-Iozzo-OSX-IPhone-Payloads-whitepaper.pdf

“A Look at a Modern Mobile Security Model: Google's Android Platform”, Oberheide
http://jon.oberheide.org/files/cansecwest09-android.pdf

Security-Seite von SWITCH
http://www.switch.ch/de/all/cert_IT/downloads/