UI-Redressing-Angriffe auf Android

Marcus Niemietz
Ruhr-Universität Bochum

mail@mniemietz.de
http://www.mniemietz.de

OWASP
07. November 2012

The OWASP Foundation
http://www.owasp.org

Über meine Person

- Horst Görtz Institut für IT-Sicherheit
- Buch
  - Clickjacking und UI-Redressing
- Websicherheit:
  Trainings, Penetrationstests
- Speaker auf der BlueHat,
  CONFidence, SIGINT, PHDays, ...
- Twitter: @mniemietz

Überblick

- Einführung
- Angriffe und Gegenmaßnahmen
  - UI-Redressing
    - Tapjacking
- Zusammenfassung und Ausblick

Allgemeines

- In diesem Vortrag werden mindestens zwei wichtige Fragen beantwortet:

1. Welche UI-Redressing-Angriffe und Gegenmaßnahmen lassen sich auf das Betriebssystem Android übertragen?
2. Kann eine Android-Applikation – die *keine* Rechte besitzt – Aktionen wie etwa Telefonanrufe ausführen?

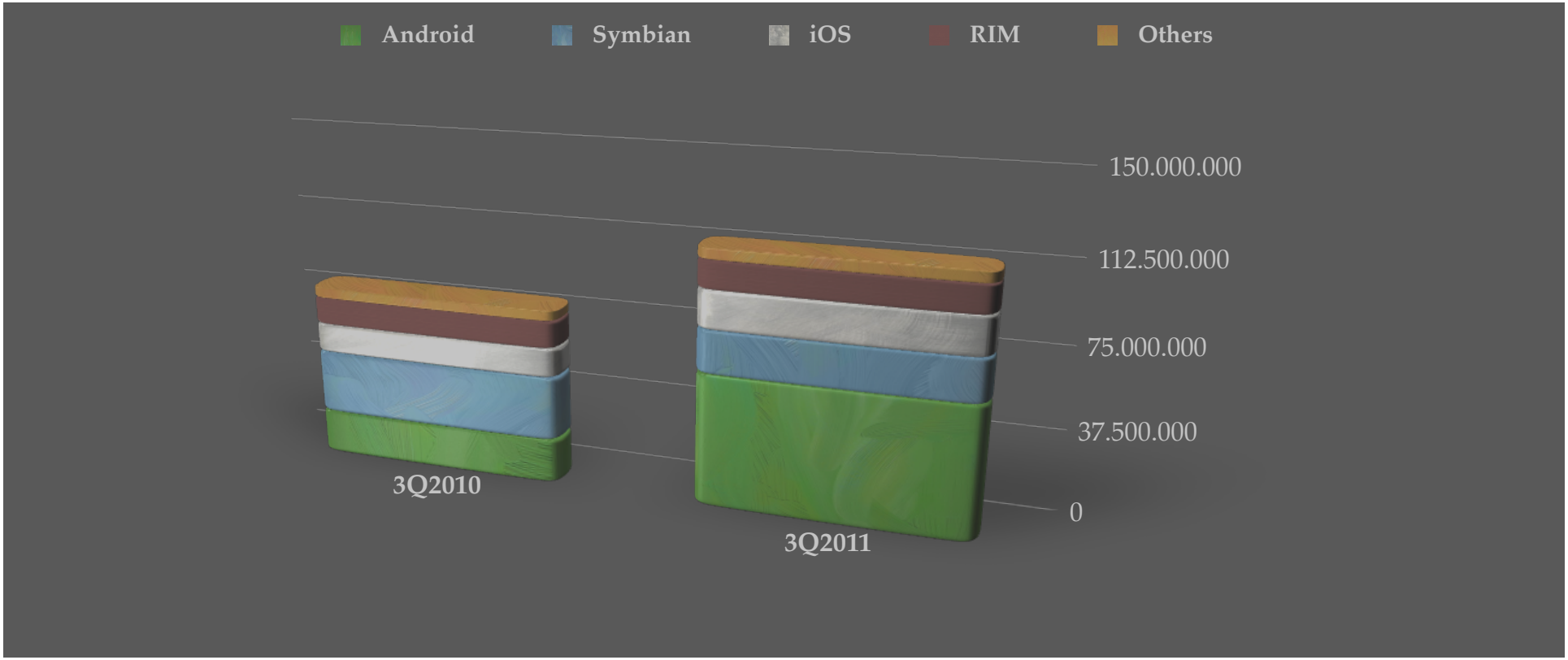
Einführung

Einführung – Android

- Linux-basiertes OS
- Überwiegend für mobile Geräte
- Einsatzbereiche
  - Smartphones
  - Tablet-Computer
  - TV-Geräte
- Entwickler: Open Handset Alliance
- Geführt von Google
- Erste Veröffentlichung im September 2008
- Android 4.0.3 im Dezember 2011

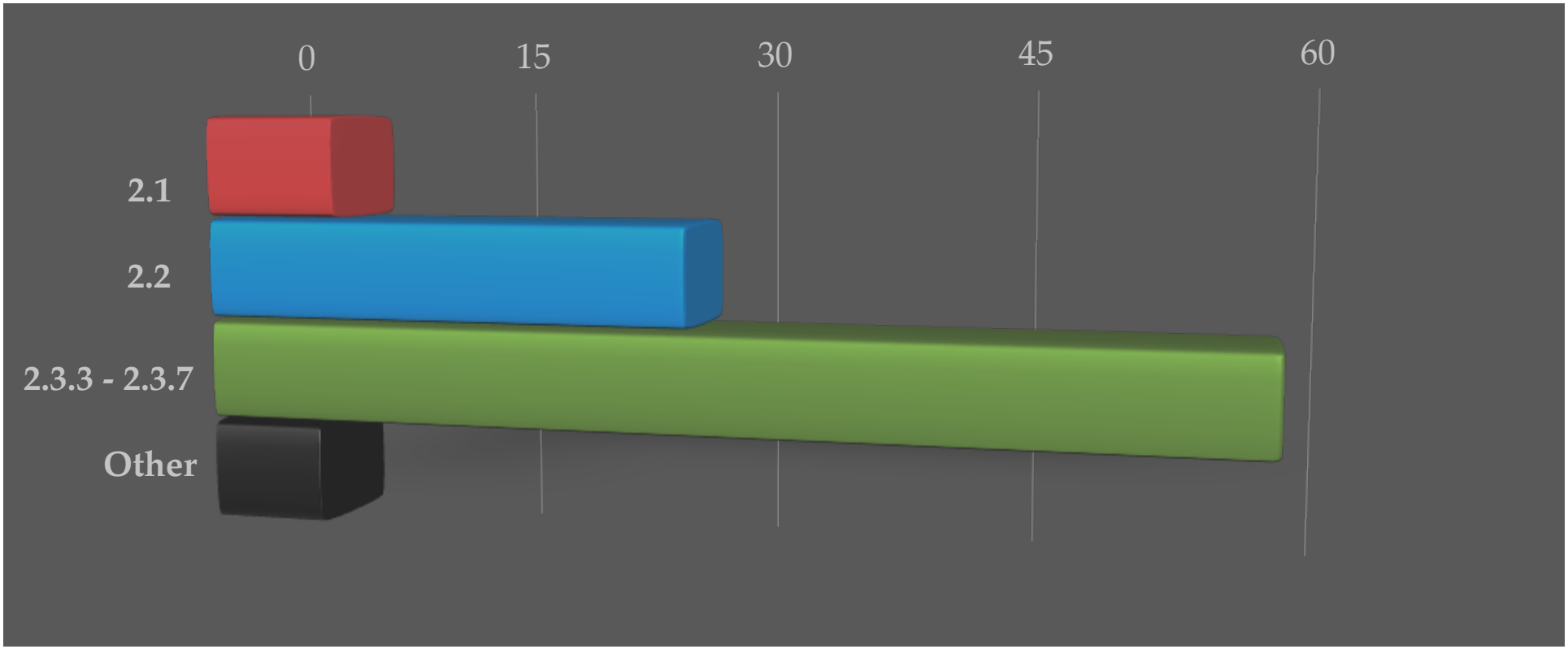
Einführung – Android

- Weltweite Smartphone-Verkäufe
  - Quelle: Gartner (November 2011)

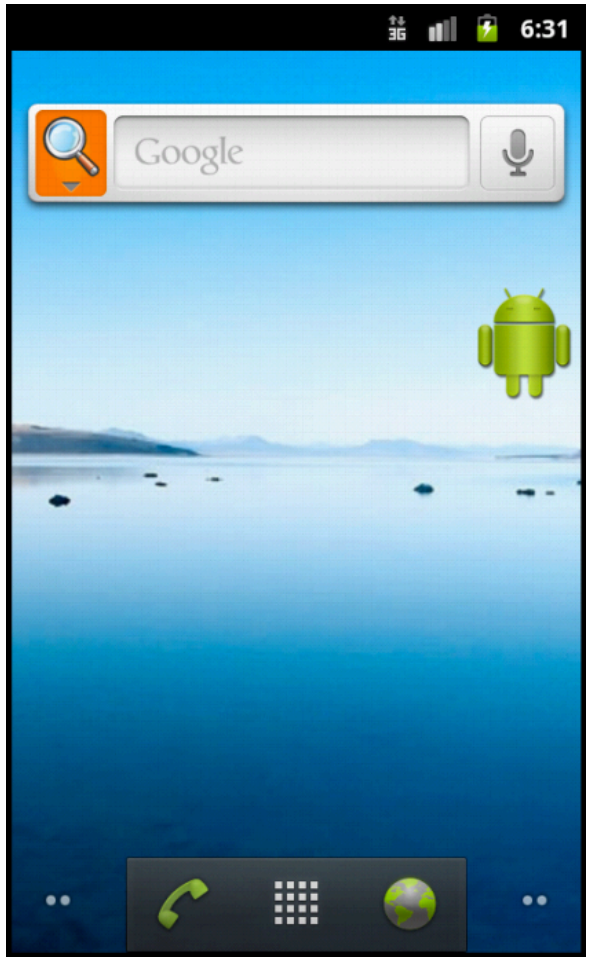


Einführung – Android

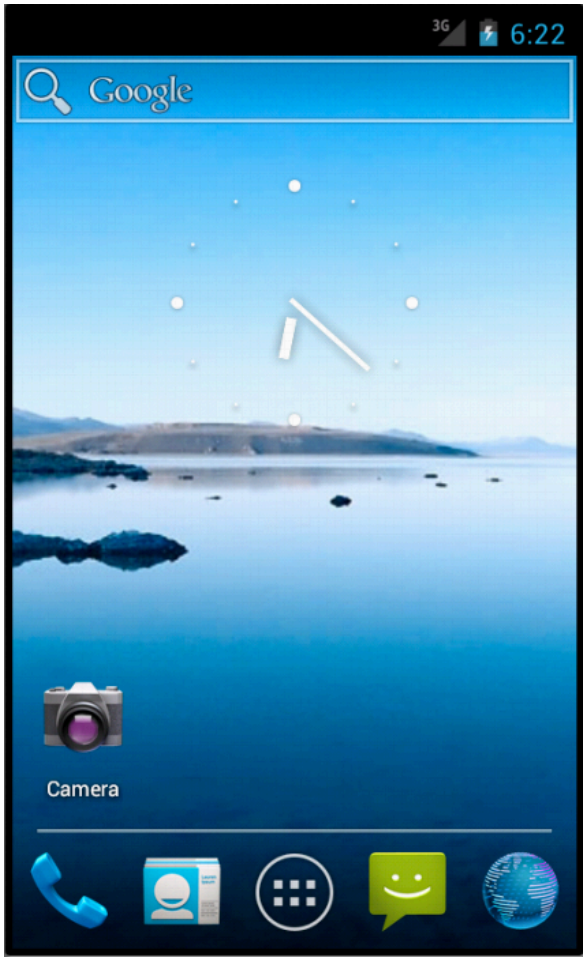
- Verteilung der Android-Versionen
  - Android.com; Zeitraum von 14 Tagen – 01.02.2012



Einführung – Android



■ Android 2.3.3



■ Android 4.0

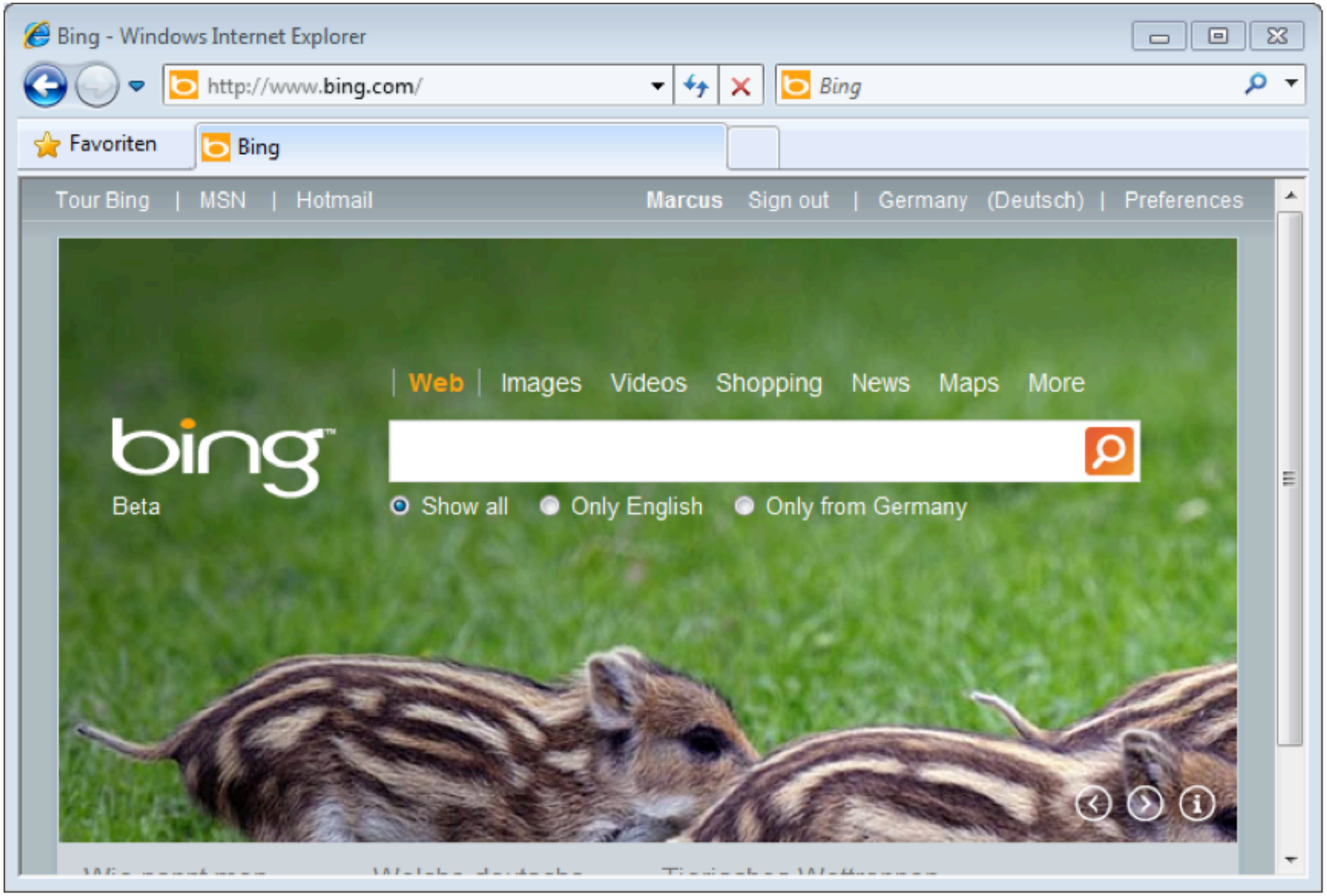
Angriffe und Gegenmaßnahmen

UI-Redressing

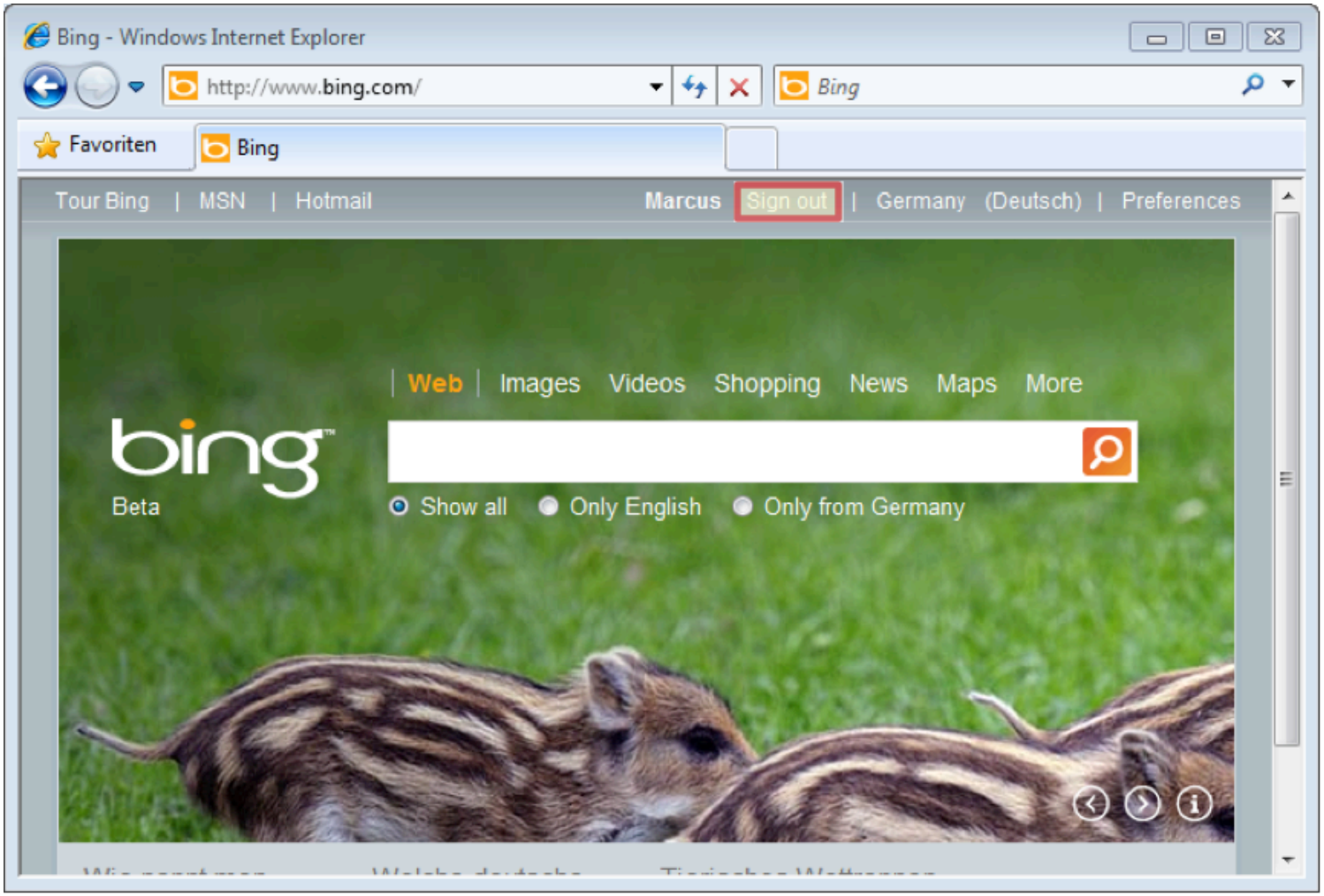
UI-Redressing

- Zitat aus „Clickjackung und UI-Redressing“
  - „UI-Redressing ist eine Technik, die die Veränderung des Verhaltens sowie optional auch des Aussehens einer Webseite beschreibt.“
- Der Ursprung allen Übels: Clickjacking
  - Seit dem Jahr 2002 bekannt
  - Seit 2008 in bewusster Verwendung

UI-Redressing – Clickjacking

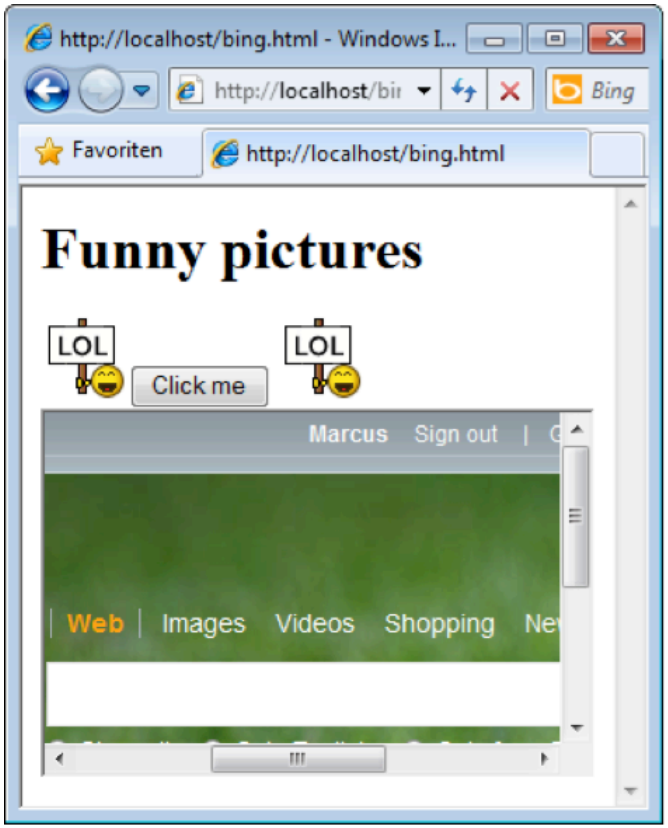


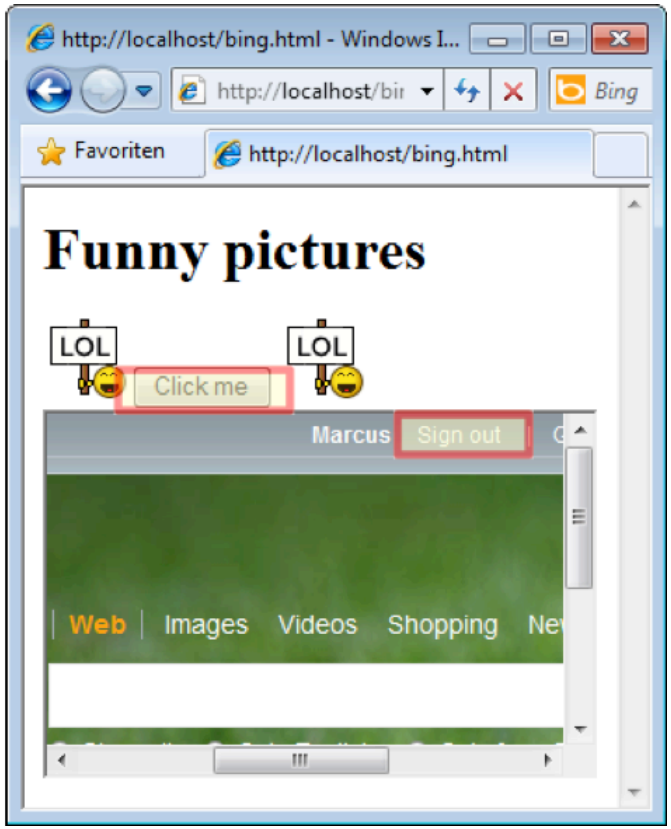
UI-Redressing – Clickjacking



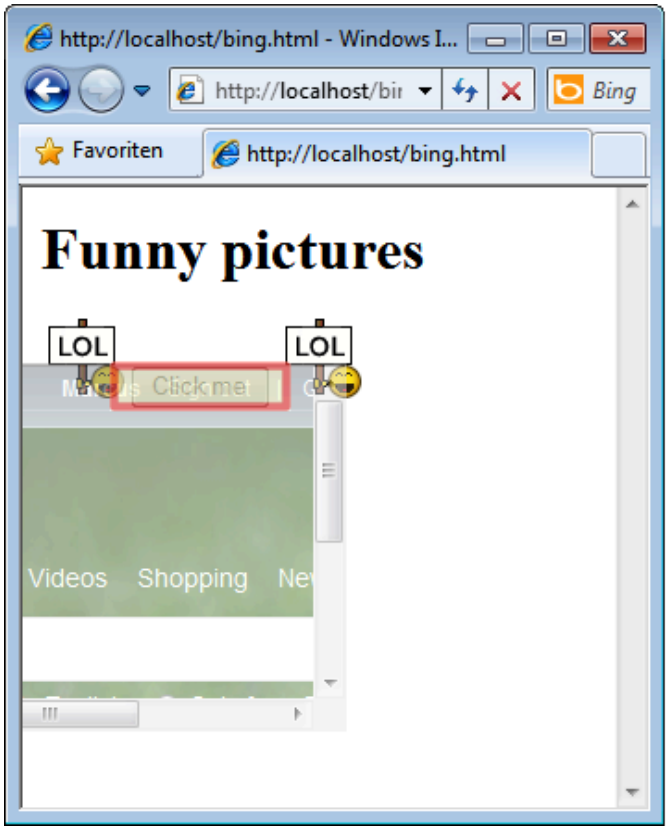
UI-Redressing – Clickjacking

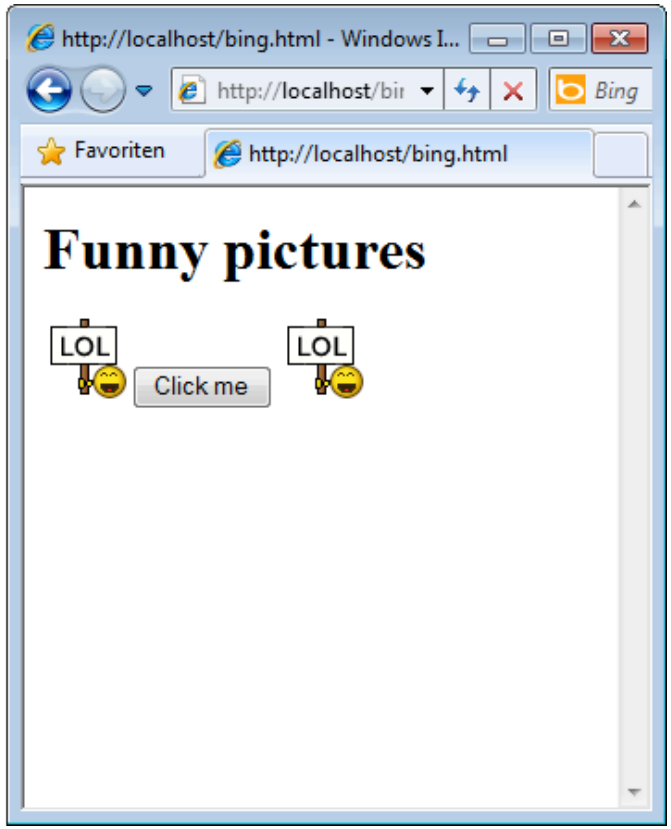
UI-Redressing – Clickjacking





UI-Redressing – Clickjacking





UI-Redressing

- Clickjacking
- Strokejacking
- Text injection per Drag & Drop
- Content extraction
- Pop-up-Blocker umgehen, Event-Recycling
- SVG-Maskierungen

UI-Redressing

- Clickjacking
  - *Classic-Clickjacking*
  - Nested-Clickjacking
  - Likejacking und Sharejacking
  - Cursorjacking
  - Filejacking, Cookiejacking
  - Eventjacking, Classjacking
  - *Tapjacking*, Tabnabbing
  - Double-Clickjacking
  - Kombinationen mit CSRF, XSS und CSS

UI-Redressing

- Gängige Browser unter Android verfügbar
  - Default Android-Brower (WebKit)
  - Dolphin (WebKit)
  - Firefox (Gecko)
  - Opera Mini (Presto)
  - Opera Mobile (Presto)

UI-Redressing

- Genannte UI-Redressing-Angriffe sind alle anwendbar, bis auf
  - Cursorjacking
  - Cookiejacking
  - Double-Clickjacking und Pop-Up-Blocker Bypasses

- Gegenmaßnahmen sind verfügbar
  - X-Frame-Options
  - JavaScript Frame-Buster
  - NoScript

UI-Redressing
Tapjacking

UI-Redressing – Tapjacking

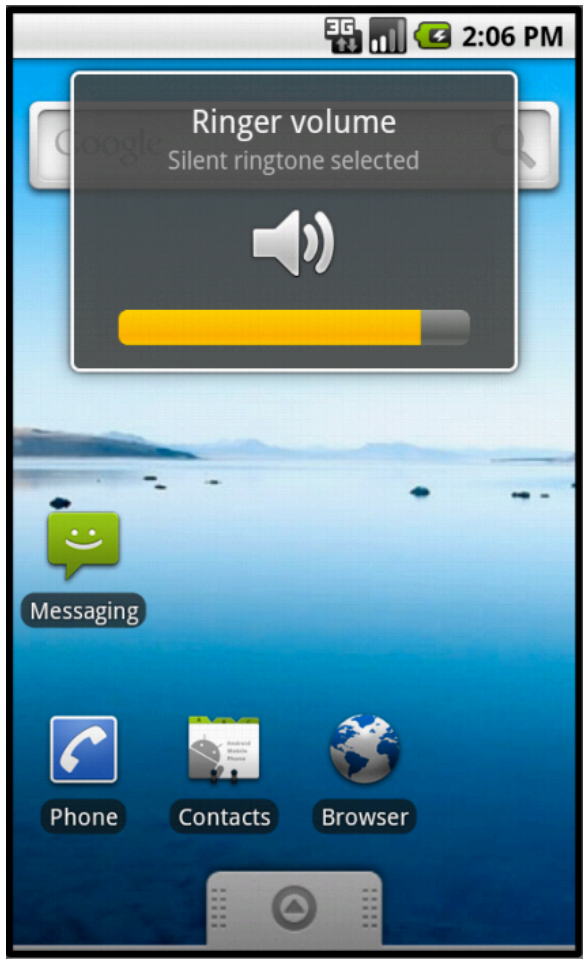
- Vorabwissen
  - Trendmicro hat im Mai 2012 herausgefunden, dass es in Google Play 17 Apps mit über 700.000 Downloads gibt
  - Davon enthielten sechs Anwendungen Malware, der Rest unaufgeforderte Werbung
- Idee
  - Ein Opfer soll eine Aktion ausführen, die ursprünglich nicht geplant war
    - Bösartige Applikation hochladen, die „keine" Rechte hat
    - Etwa als Computerspiel getarnt

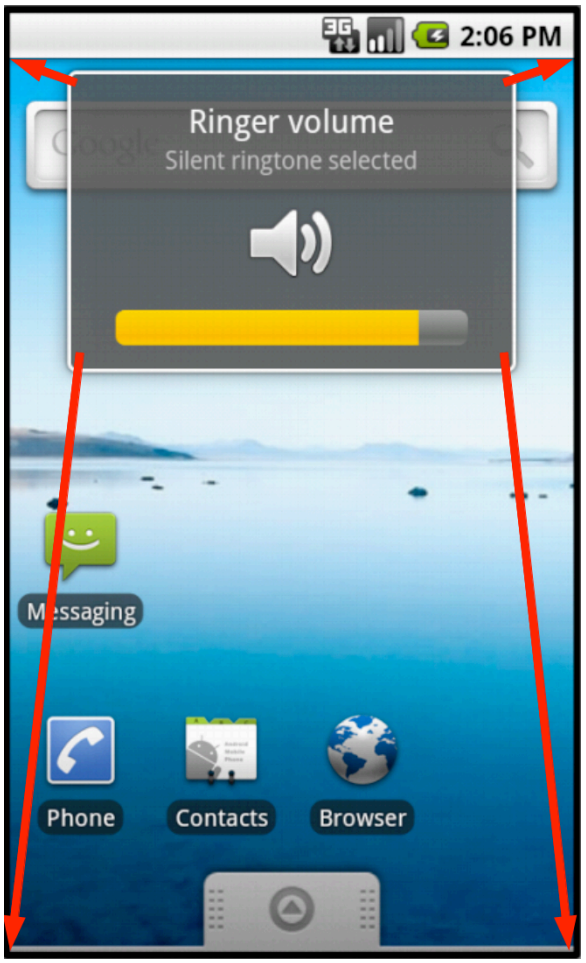
UI-Redressing – Tapjacking

- Android Trust-Modell
  - Eine Anwendung darf eine Anwendung öffnen, allerdings darf sie nicht mit dieser interagieren

- Idee
  - Pop-up-Fenster für Feedbacks nutzen
    - „Message saved as a draft“
    - Lautstärkeregler
  - Feedbacks sind über `toast`-Objekte generierbar

UI-Redressing – Tapjacking

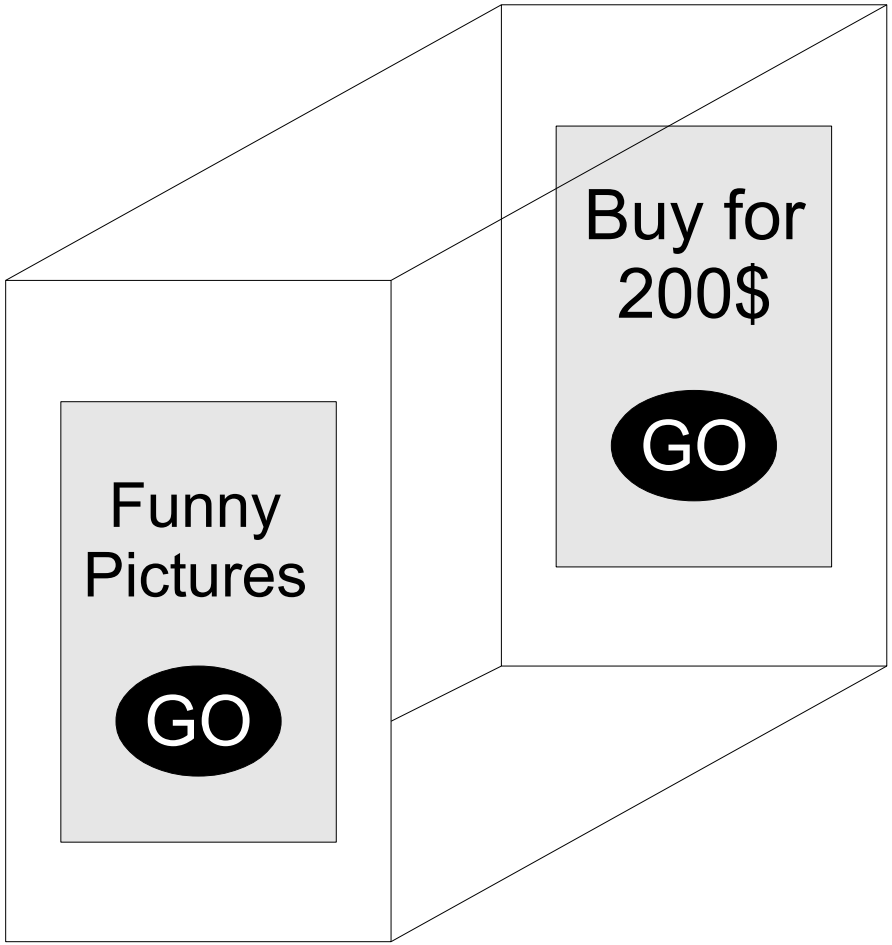




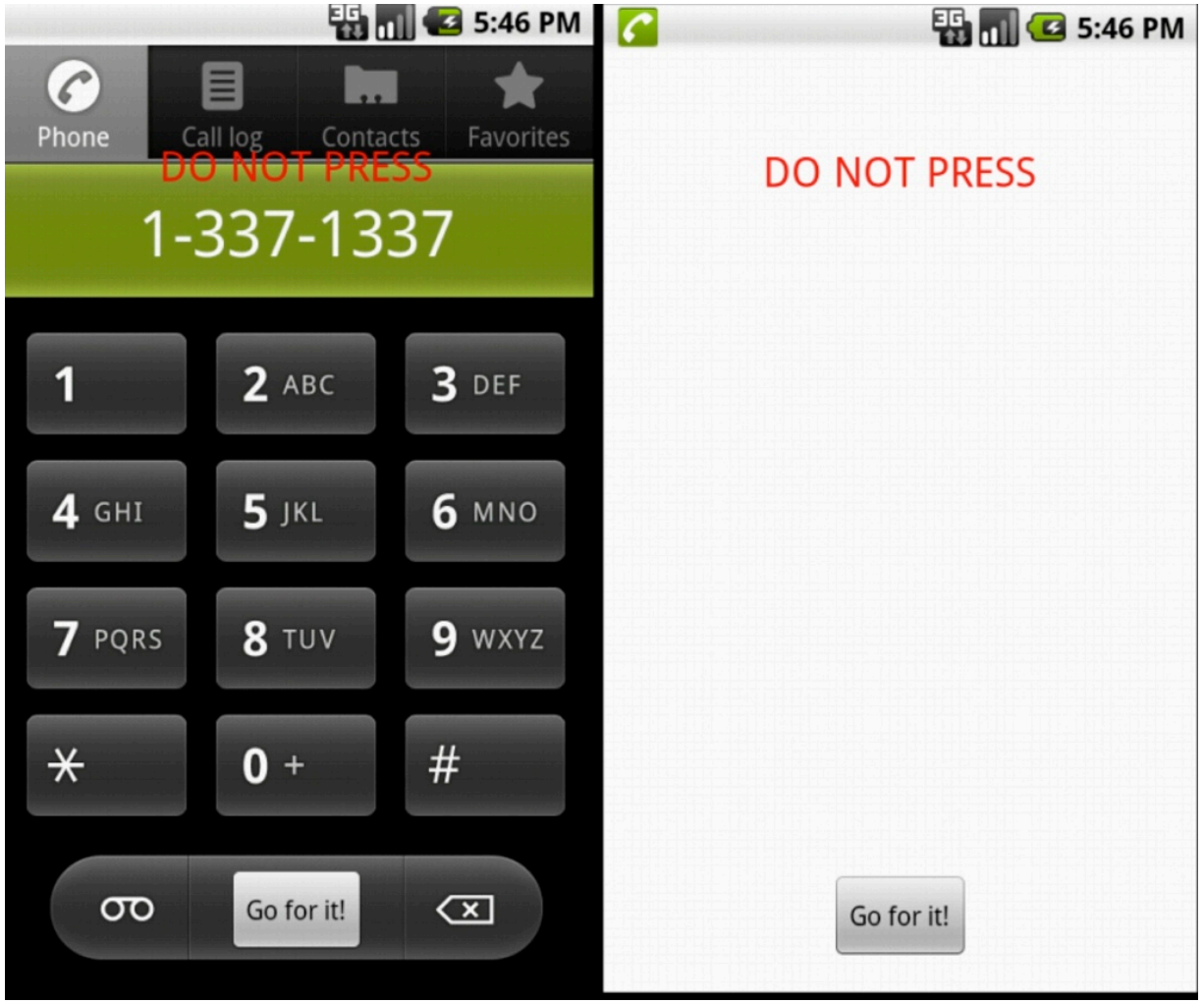
UI-Redressing – Tapjacking

- Jack Mannino hat im Jahr 2011 einen Machbarkeitsnachweis publiziert
- Toast-Objekt mit der Konstante `LENGTH_LONG` verwendet
  - Die Nachricht wird für wenige Sekunden angezeigt
  - Künstliche Verlängerung durch ständiges Neuladen
- Die Nachricht sieht aus wie eine normale Applikation – inkl. Dummy-Buttons

UI-Redressing – Tapjacking



UI-Redressing – Tapjacking



UI-Redressing – Tapjacking

- Kontaktdaten verändern
- Browser sowie Webseiten manipulieren
  - Code Injections möglich
  - Cross-Device Scripting
- Touch-Gesten können geloggt werden
- Vordefinierte Telefonanrufe
- Applikationen im Hintergrund installieren

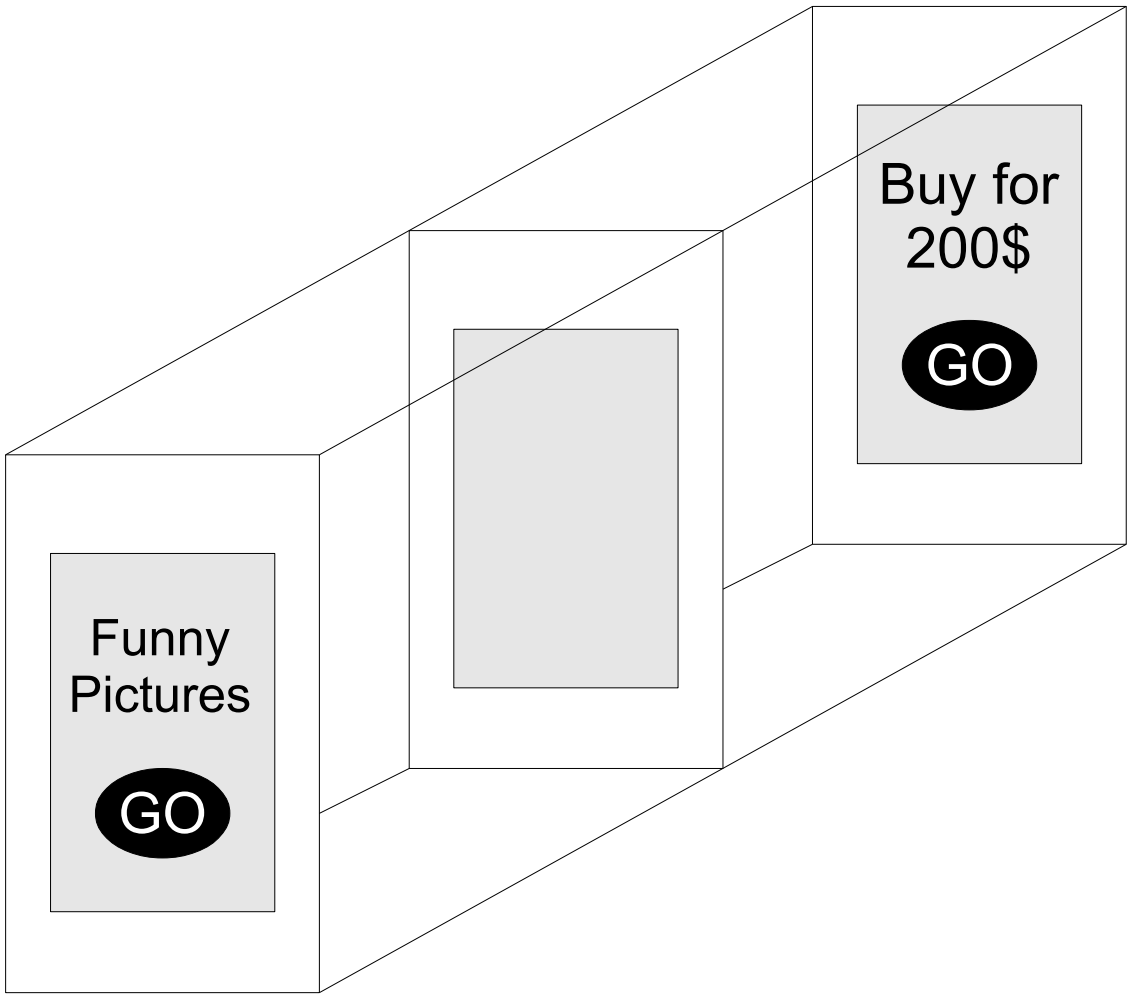
UI-Redressing – Tapjacking

- Vorhandene Gegenmaßnahme
  - `setFilterTouchesWhenObscured()` oder das Attribut `android:filterTouchesWhenObscured`
  - Nur eigene Applikationen können geschützt werden
- Schwerwiegendes Problem
  - Der Home-Screen ist angreifbar
  - Vorhandene nativ implementierte Applikationen sind nicht geschützt

UI-Redressing – Tapjacking

- Idee: Drittes Layer zum Schutz
  - Blockt alle Touch-Gesten die von „oben“ kommen
  - Wird immer im Hintergrund einer Applikation geladen
- Problem
  - Änderung im System notwendig sind
  - Vom Android-Team zu implementieren

UI-Redressing – Tapjacking



Zusammenfassung und Ausblick

Zusammenfassung und Ausblick

- UI-Redressing und insbesondere Clickjacking ist gefährlich
- Bekannte UI-Redressing-Angriffe sind größtenteils auf Android übertragbar
- Es gibt browserbasierende und browserlose UI-Redressing-Angriffe
- Es gibt auf beiden Seiten Schutzmechnismen, die jedoch insbesondere bei Android unzureichend sind
- Zukünftig wird es mehr Angriffe geben

Referenzen

- *http://developer.android.com/resources/dashboard/platform-versions.html*
- Framing Attacks on Smart Phones and Dumb Routers:Tap-jacking and Geo-localization Attacks, *http://seclab.stanford.edu/websec/framebusting/tapjacking.pdf*
- Marcus Niemietz (Mai 2012), Clickjacking und UI-Redressing
- Michal Zalewski (Dez. 2011), The Tangled Web: A Guide to Securing Modern Web Application

Vielen Dank für die Aufmerksamkeit.

Fragen?