Phishing on Mobile Devices

Adrienne Porter Felt & David Wagner

University of California, Berkeley

PHISHING

Ingredients for phishing

1. Users conditioned to enter passwords
2. A convincing spoof of the user interface

PHISHING RISK

1. When are users conditioned to enter their passwords or payment information?
2. Can those scenarios be convincingly spoofed?

THREAT MODEL

- Sender ⇒ Target
- **Direct attack:** false control transfer
- **Man-in-the-middle attack:** subverted control transfer

MOBILE PHISHING

- Phones lack trustworthy security indicators
- Interaction between web & mobile apps
- Mobile login screens are simple

OUR APPROACH

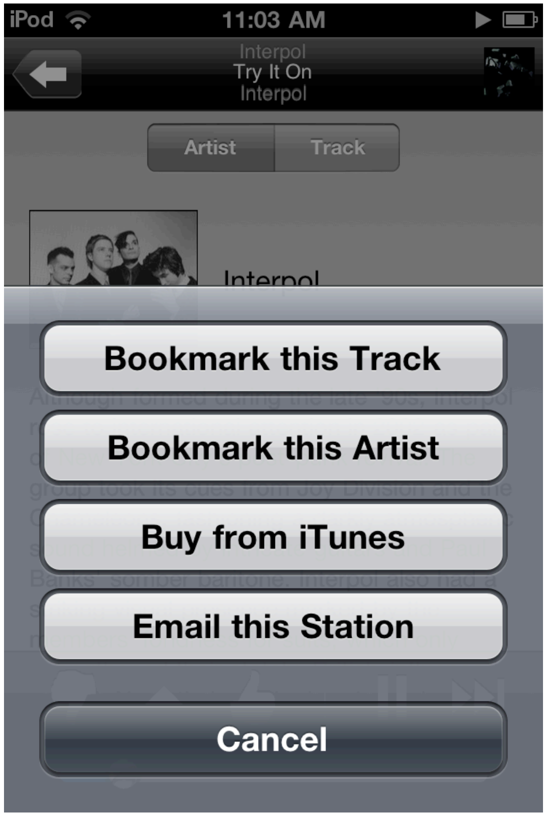
1. Survey how applications condition users
    - 50 most popular Android & iOS apps
    - 85 popular web sites on Android, iOS
2. Evaluate avenues for spoofing
    - Direct
    - Man-in-the-middle

CONTROL TRANSFERS

- Mobile sender ⇒ Mobile target
- Mobile sender ⇒ Web target
- Web sender ⇒ Mobile target
- Web sender ⇒ Web target

MOBILE ⇒ MOBILE

- Social sharing
- Upgrades via store
- Music purchases
- Game credits (iOS)

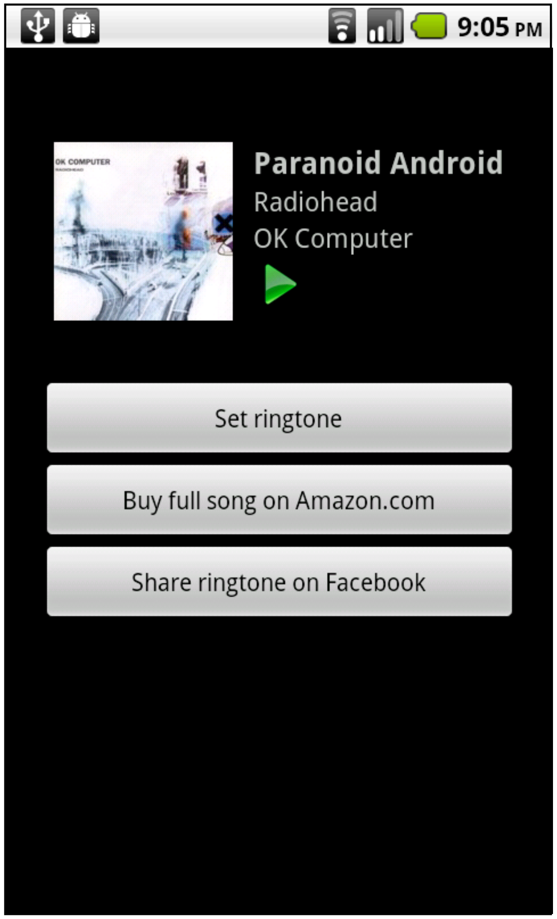


MOBILE ⇒ MOBILE

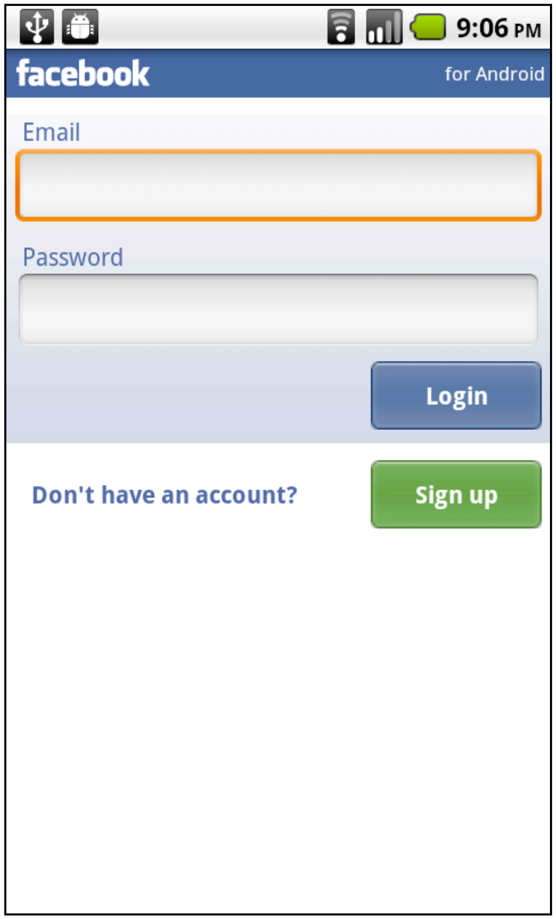
Target	Android	iOS
Mobile app	56%	72%
Password-protected	36%	60%
Payment	10%	34%

M ⇒ M: DIRECT ATTACK

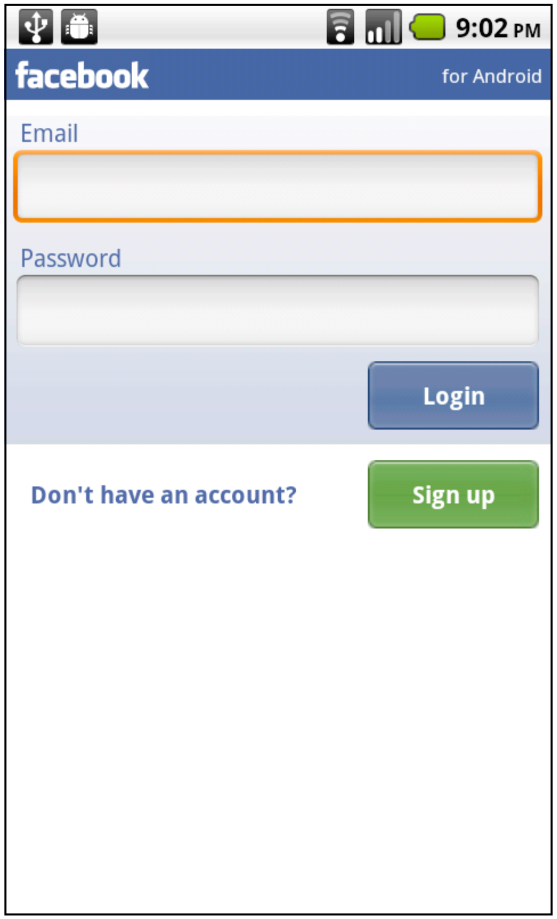
Attack App



Spoof Page



Real Page



M ⇒ M: MITM ATTACK

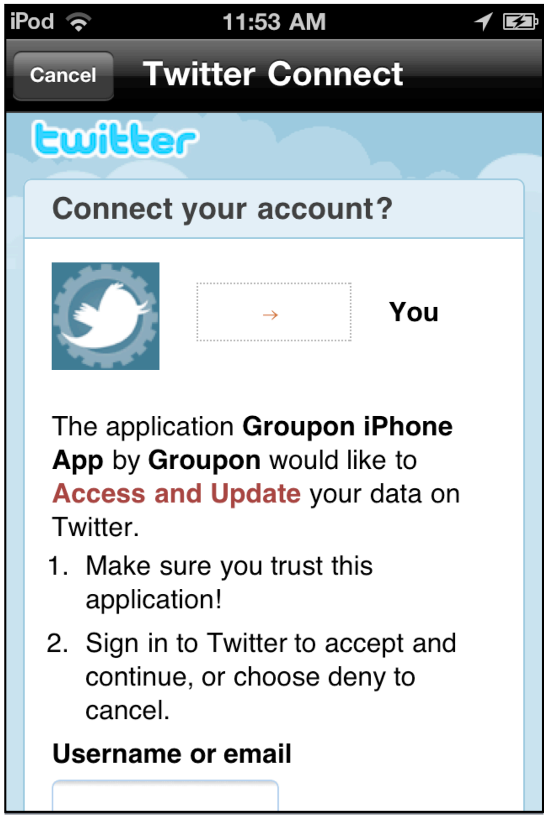
- **Scheme squatting**
  - Register for another app's URI scheme
  - Weak: detectable by user, reviewers
- **Task interception**
  - Poll task list, pop up when target opens
  - Unnoticeable by users

CONTROL TRANSFERS

- Mobile sender ⇒ Mobile target
- Mobile sender ⇒ Web target
- Web sender ⇒ Mobile target
- Web sender ⇒ Web target

MOBILE ⇒ WEB

- **Mechanisms**
  - Links to the browser
  - Embedded web content
- **Reasons**
  - Social sharing
  - Not much payment



Connect your account?

The application **Groupon iPhone App** by **Groupon** would like to **Access and Update** your data on Twitter.

1. Make sure you trust this application!
2. Sign in to Twitter to accept and continue, or choose deny to cancel.

Username or email

MOBILE ⇒ WEB

Browser target

Target	Android	iOS
Web site	30%	18%
Password-protected	3%	4%
Payment	2%	-

Embedded target

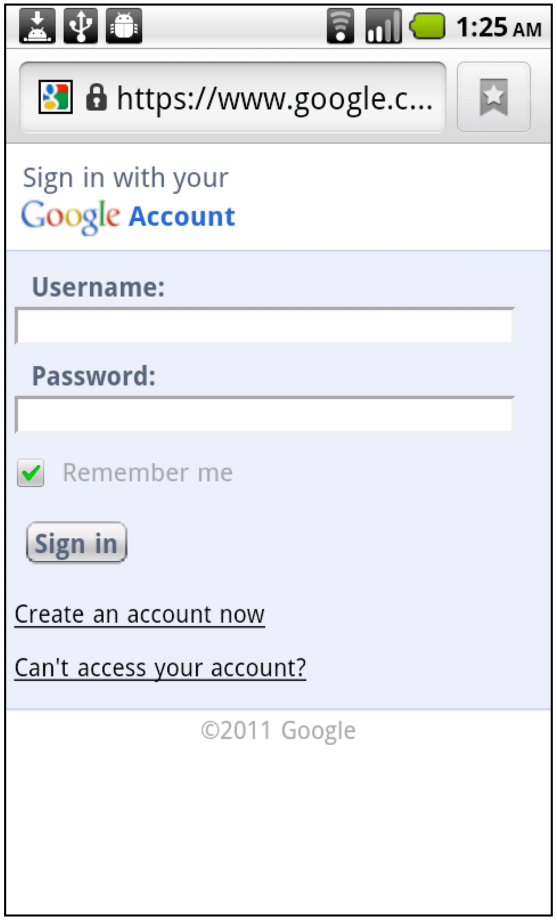
Target	Android	iOS
Web site	16%	42%
Password-protected	8%	38%
Payment	2%	-

M ⇒ W: DIRECT ATTACK

- Link to web browser
    - Send the user to a fake browser
    - Open in real browser, hide/fake URL bar
- Embedded content
    - Eavesdrop on credentials given to embedded content

M ⇒ W: DIRECT ATTACK

Real Browser



1:25 AM

https://www.google.c...

Sign in with your

Google Account

Username:

Password:

☑ Remember me

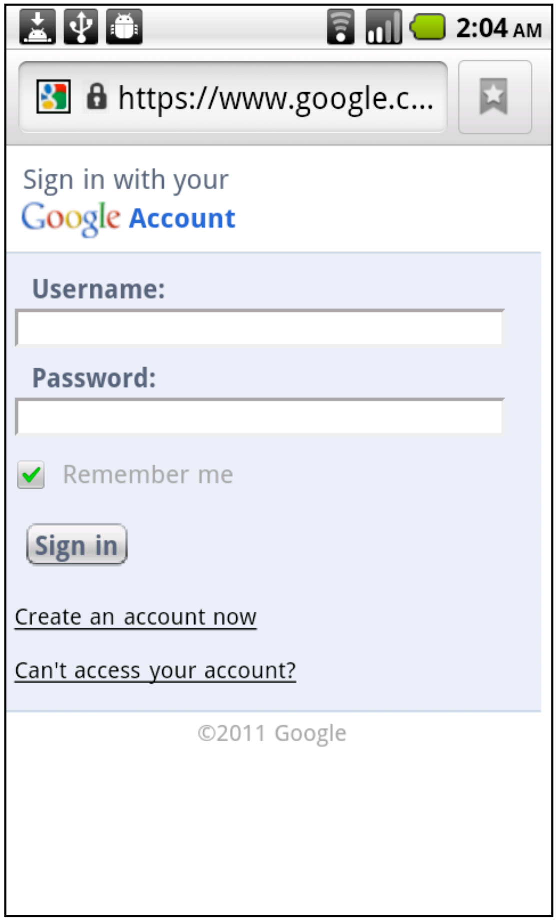
Sign in

Create an account now

Can't access your account?

©2011 Google

Spoof Browser



2:04 AM

https://www.google.c...

Sign in with your

Google Account

Username:

Password:

☑ Remember me

Sign in

Create an account now

Can't access your account?

©2011 Google

M ⇒ W: MITM ATTACK

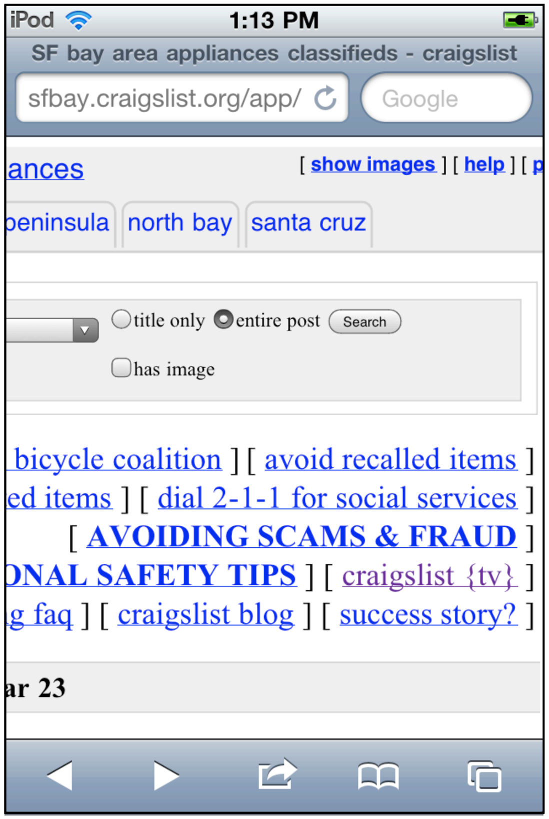
- Attack: alter target of form on HTTP page
- Defense: forms only on HTTPS pages
- Attack: alter links to HTTPS pages

CONTROL TRANSFERS

- Mobile sender ⇒ Mobile target
- Mobile sender ⇒ Web target
- Web sender ⇒ Mobile target
- Web sender ⇒ Web target

WEB ⇒ MOBILE

- **Mechanisms**
  - tel://18005555555
  - market://details?id=123
- **Reasons**
  - mailto, Twitter
  - Install the app version


iPod 1:13 PM

SF bay area appliances classifieds - craigslist

sfbay.craigslist.org/app/

Google

ances [show images] [help] [p

peninsula | north bay | santa cruz

○title only ●entire post Search

□has image

bicycle coalition] [avoid recalled items]
ed items] [dial 2-1-1 for social services]
[AVOIDING SCAMS & FRAUD]
ONAL SAFETY TIPS] [craigslist {tv}]
g faq] [craigslist blog] [success story?]

ar 23

WEB ⇒ MOBILE

Core mobile apps

Target	Android	iOS
Core mobile application	38%	47%
Password-protected	22%	41%
Payment	6%	25%

Any mobile apps

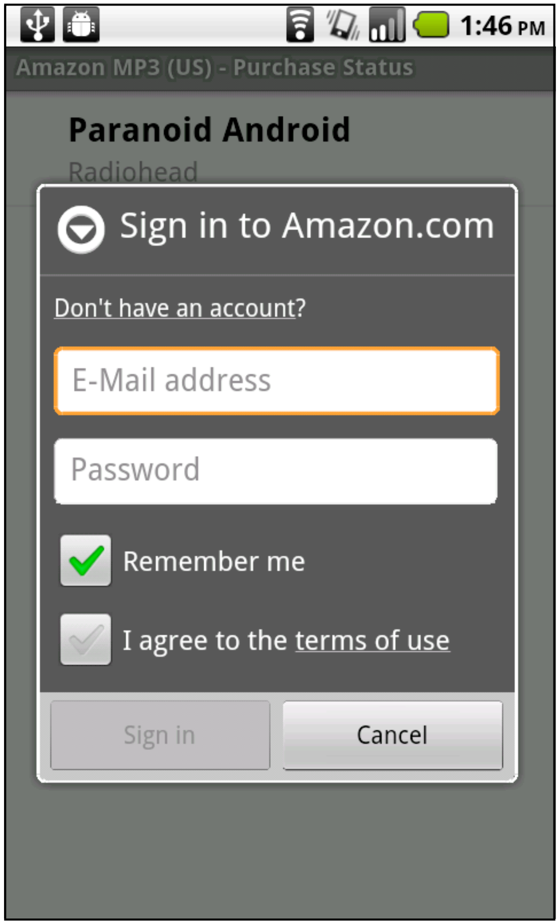
Target	Android	iOS
Any mobile application	49%	48%
Password-protected	38%	42%
Payment	6%	25%

W ⇒ M: DIRECT ATTACK

- Hide the browser chrome and mimic app
  - In Android, only detectable if user hits the “Menu” button
  - Not possible in iOS unless user has “installed” the page

W ⇒ M: DIRECT ATTACK

Real App



Amazon MP3 (US) - Purchase Status

Paranoid Android

Radiohead

Sign in to Amazon.com

Don't have an account?

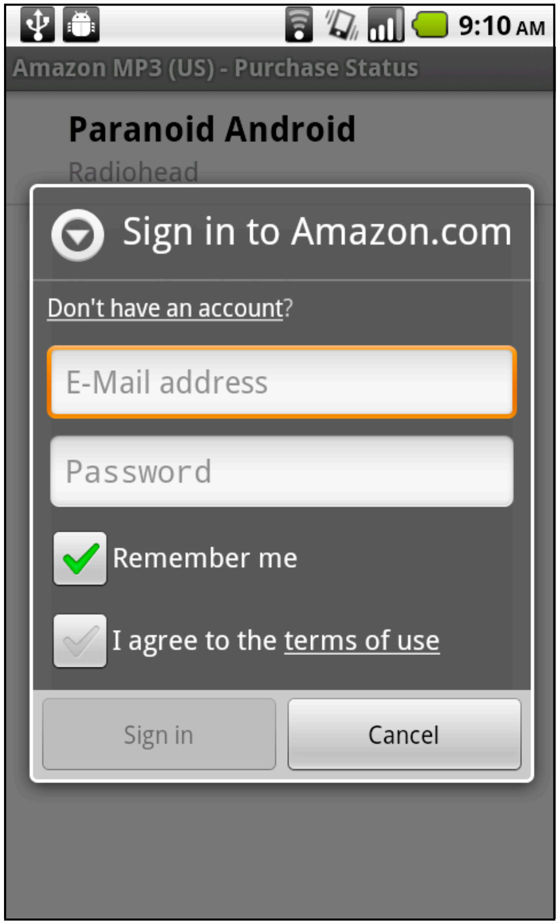
E-Mail address

Password

☑ Remember me

☐ I agree to the terms of use

Spoof App (In Browser)



Amazon MP3 (US) - Purchase Status

Paranoid Android

Radiohead

Sign in to Amazon.com

Don't have an account?

E-Mail address

Password

☑ Remember me

☐ I agree to the terms of use

W ⇒ M: MITM ATTACK

- Scheme squatting
- Task interception

CONTROL TRANSFERS

- Mobile sender ⇒ Mobile target
- Mobile sender ⇒ Web target
- Web sender ⇒ Mobile target
- Web sender ⇒ Web target

WEB ⇒ WEB: DIRECT

- Spoof or hide the URL bar [Niu et al.]
  - Eased how it scrolls
  - Reduced URL loading/rendering time

WEB ⇒ WEB: MITM

- Subvert all HTTP pages so that links to HTTPS are never trustworthy
- User won’t be warned by the URL bar

PREVENTION

- Permanently application identity indicator
  - Embedded web content still a problem
- Trusted password entry mechanism
  - Usability?
  - Adoption?

Questions?

apf@cs.berkeley.edu