SMARTPHONES, APPLICATIONS & SECURITY

HITB KL 2010
INTRODUCTION
PAUL SEBASTIAN ZIEGLER
THINGS I DO

REVERSE CODE ENGINEER

WHITEHAT HACKER

DEVELOPER

AUTHOR
Cross-Site Scripting

Paul Sebastian Ziegler


Dieses TecFeed ist bemüht, das zu ändern. In einfachen Schritten führt der Autor Sie in das komplexe Thema ein. Sie werden lernen, was Cross-Site Scripting ist und wie man mit seiner Hilfe Webanwendungen angreifen kann. Nach der Lektüre dieses TecFeeds werden Sie in der Lage sein, Schwachstellen zu erkennen und zu beheben.
BERLIN

CURRENTLY

TOKYO

MOSTLY
Passport Scanner at Narita Airport

Unpatched Windows XP SP1
ANYTHING ELSE?
ASK!
“PHONE HACKING” - 1970
“PHONE HACKING” - 1970

USING THIS!
“PHONE HACKING” - 1970

USING THIS! TO HACK THIS!
“PHONE Hacking” - 2010
“PHONE HACKING” - 2010

ATTACKING THIS!
“PHONE HACKING” - 2010

ATTACKING THIS!

TO HACK THIS!
MALWARE.
ON A MOBILE PHONE.
SO WHAT?
THE USUAL SUSPECTS
EAVESDROPPING
THE OLD WAY
THE OLD WAY
THE OLD WAY
THE OLD WAY
THE OLD WAY
THE OLD WAY

PROXIMITY
RESULT
RESULT
THE NEW WAY
THE NEW WAY
THE NEW WAY
NO PROXIMITY

NO ADVANCED HARDWARE
SNIFFING TEXT MESSAGES
GATHERING PHONE BOOK ENTRIES
COLLECTING CALL AND BROWSER HISTORY
WHAT DO WE KNOW?
WHAT DO WE KNOW?
WHAT DO WE KNOW?
WHAT DO WE KNOW?
WHAT DO WE KNOW?

Friend  Friend  Friend
--  --  --

Coworker  Coworker  Coworker
---  ---  ---

DATA

Target

---
WHAT DO WE KNOW?

DATA

CONVERSATIONS
WHAT DO WE KNOW?

CONVERSATIONS

DATA

EMAILS
WHAT DO WE KNOW?

DATA

CONVERSATIONS

EMAILS

SMS
CRAZIER TARGETS
ALTERING MESSAGES
ON THE FLY
IF ("HACKER INC" IN SMS.TEXT) { %S/SELL/BUY/G };
IF ("HACKER INC" IN SMS.TEXT) { %S/SELL/BUY/G };

OMG! **SELL** AS MUCH HACKER INC STOCK AS POSSIBLE! WILL EXPLAIN L8TR!

OMG! **BUY** AS MUCH HACKER INC STOCK AS POSSIBLE! WILL EXPLAIN L8TR!
THE SAME WORKS FOR INCOMING DATA
THE SAME WORKS FOR INCOMING DATA

EMAILS
WEB PAGES
IMAGES
RSS FEEDS
MMS
REQUESTS INFORMATION FROM SECURE SOURCE
REQUESTS INFORMATION FROM SECURE SOURCE

RECEIVES REAL DATA
REQUESTS INFORMATION FROM SECURE SOURCE

RECEIVES REAL DATA

SEES FAKE DATA
REQUESTS INFORMATION FROM SECURE SOURCE

RECEIVES REAL DATA

SEES FAKE DATA

IS TRICKED INTO ACTION THE ATTACKER DESIRES
REQUESTS INFORMATION FROM SECURE SOURCE

RECEIVES REAL DATA

SEES FAKE DATA

IS TRICKED INTO ACTION THE ATTACKER DESIRES

AUTHENTICATING AGAINST FAKE SERVER
REQUESTS INFORMATION FROM SECURE SOURCE

RECEIVES REAL DATA

SEES FAKE DATA

IS TRICKED INTO ACTION THE ATTACKER DESIRES

AUTHENTICATING AGAINST FAKE SERVER

REVEALING CONFIDENTIAL INFORMATION
PARTS OF A SMARTPHONE
PARTS OF A SMARTPHONE
PARTS OF A SMARTPHONE
PARTS OF A SMARTPHONE
PARTS OF A SMARTPHONE
PRIME TARGET
<table>
<thead>
<tr>
<th>Feature</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendars</td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>+</td>
</tr>
<tr>
<td>Data Storage</td>
<td>+</td>
</tr>
<tr>
<td>Constant Uplink</td>
<td>+</td>
</tr>
<tr>
<td>MarcoPolo 2.0</td>
<td>=</td>
</tr>
<tr>
<td>Microphone</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---</td>
</tr>
<tr>
<td>Data Storage</td>
<td>+</td>
</tr>
<tr>
<td>Constant Uplink</td>
<td>+</td>
</tr>
<tr>
<td><strong>Bug 2.0</strong></td>
<td>=</td>
</tr>
<tr>
<td>Speaker</td>
<td>Data Storage</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>Constant Uplink</td>
</tr>
<tr>
<td></td>
<td>Scary 2.0</td>
</tr>
</tbody>
</table>
AND THAT’S WITHOUT THE DATA STORED BY APPS
THINGS PEOPLE STORE IN APPS
THINGS PEOPLE STORE IN APPS

Banking Information & Financial Information

![Banking Information & Financial Information on an app](Image)
THINGS PEOPLE STORE IN APPS

HEALTH INFORMATION
THINGS PEOPLE STORE IN APPS

PICTURES
HOMES -> ADDRESSES

CREDIT CARDS -> NUMBERS

THEMSELVES

THEIR FAMILY
THINGS PEOPLE STORE IN APPS

FAVORITE RESTAURANTS
SO WHAT?
Hi, this is Target’s Name! I am calling about my account at Bank’s Name. Please make a 2800$ transfer to some shady account. Of course! Send me the confirmation email! The account number is 1234-5678-9123-4567. Answer my secret question? What’s my eye color? Why, green of course!
SOCIAL ENGINEERING HEAVEN

Anything any company / bank / institution could ever possibly ask an attacker to confirm the identity will be in one of the mails, pictures, apps or can be picked up through the microphone.
NOVEMBER 2009
THE RICK ROLLING WORM

SPREAD TO JAILBROKEN IPHONES USING THE SSH DEFAULT PASSWORD. INSTALLED A WALLPAPER FEATURING RICK ASTLEY.
JANUARY 2010

FAKE E-BANKING APPS

SUBMITTED TO THE ANDROID MARKETPLACE. NOT MADE BY THE ACTUAL BANKS. REMOVED BY GOOGLE.
JANUARY 2010
FAKE E-BANKING APPS

SUBMITTED TO THE ANDROID MARKETPLACE. NOT MADE BY THE ACTUAL BANKS.
REMOVED BY GOOGLE.

MANY SIMILAR APPS SINCE.
JUNE 2010
TWILIGHT BOTNET POC

DEMONSTRATED BY JON OBERHEIDE AT SUMMERCON. LEGIT LOOKING APP FETCHES NEW EXPLOIT CODE FROM ATTACKER LONG AFTER IT HAS BEEN DOWNLOADED BY MANY.
DETAILED LOOK
FAKE E-BANKING APPS
Fake App -> Teh Fake App

Teh Bank
SECURITY = VALID CERTIFICATE
SECURITY = ANIMATED GIF
Teh Fake App

ANDROID MARKETPLACE
Teh Fake App

ANDROID MARKETPLACE
Teh Hacker

Teh Fake App

Teh Bank

Android Marketplace

Target

Target

Target
YEAH.
IT’S THAT SIMPLE.
HE JAILBREAKS ME,
HE JAILBREAKS ME NOT
YES.
NON JAILBROKEN PHONES HAVE BEEN HACKED.
VINCENZO IOZZO & PHILLIPP WEINMANN
(AIDED BY HALVAR FLAKE)

PWN2OWN 2010 @ CANSECWEST
EXPLOITED BROWSER VULNERABILITY

VINCENTO IOZZO & PHILLIPP WEINMANN
(AIDED BY HALVAR FLAKE)

PWN2OWN 2010 @ CANSECWEST
EXPLOITED BROWSER VULNERABILITY

CONVINCED PHONE TO UPLOAD THE SMS DATABASE

VINCENZO IOZZO & PHILLIPP WEINMANN
(AIDED BY HALVAR FLAKE)

PWN2OWN 2010 @ CANSECWEST
EXPLOITED BROWSER VULNERABILITY

CONVINCED PHONE TO UPLOAD THE SMS DATABASE

VINCENTZIO IOZZO & PHILLIPP WEINMANN
(AIDED BY HALVAR FLAKE)

PWN2OWN 2010 @ CANSECWEST

STILL INSIDE THE IPHONE'S SANDBOX
SO WITHOUT THE SANDBOX?
WITHOUT THE SANDBOX

PRIME TARGET
RUNNING AS ROOT
NO FIREWALL
NO AV SOFTWARE
ALL IPHONE MALWARE SO FAR WAS TARGETED AT JAILBROKEN PHONES.
ALL IPHONE MALWARE SO FAR WAS TARGETED AT JAILBROKEN PHONES.

MOSTLY TARGETING THE SSH LOGIN
ALL IPHONE MALWARE SO FAR WAS TARGETED AT JAILBROKEN PHONES.

MOSTLY TARGETING THE SSH LOGIN APPS DOWNLOADED FROM CYDIA & CO HAVE NO VALIDATION AND UNLIMITED ACCESS.
THUS FROM A SECURITY STANDPOINT
THIS:
HEY! LET'S INSTALL THE LATEST [PIRATED] VERSION OF THIS APP FROM THE CYDIA STORE ONTO OUR IPHONES!
EQUALS THIS:
HEY! LET’S CLICK ON THIS RANDOM EXE FILE I FOUND ON TPB WITHOUT RUNNING AN ANTI-VIRUS SCAN ON MY UNPATCHED WINDOWS 95 BOX!
ANDROID’S SANDBOX
“ROOTING” YOUR PHONE
IN A NUTSHELL
IN A NUTSHELL

THE SANDBOX AND CODE-SIGNING FEATURES ARE THE ONLY REAL LINE OF DEFENSE ON ANY CURRENT MODERN SMARTPHONE.
This
PHYSICAL ACCESS (AGAIN)
BASIC ASSUMPTION
BASIC ASSUMPTION

IF SOMEONE HAS PHYSICAL ACCESS TO
YOUR GEAR (PHONE, SERVER, HOME, BOX,
KEYBOARD, REFRIGERATOR), YOU’RE SCREWED.
BUT I ONLY LEFT MY PHONE FOR 2 MINUTES!
2 MINUTES YOU SAY?
QUESTION:
HOW LONG DOES IT TAKE YOU TO TYPE THIS:

JAILBREAKME.COM
Launching Safari and Typing

16 seconds
JAILBREAKING

37 SECONDS
RESPRINGING

19 SECONDS
48 SECONDS
48 SECONDS TO INSTALL ANYTHING YOU WANT FROM CYDIA.
THAT’S THE **FANCY** VERSION.
2 MINUTE DEMONSTRATION
BUT I HAVE A PASSCODE!
GREAT!
IS IT IN THIS LIST?

☐ Your / Your Spouse's / Your Child's Birthday

☐ Last 4 digits of phone number

☐ 1337

☐ 1234

☐ 3141

☐ 0000

☐ 9876
IS IT IN THIS LIST?

- Your / Your spouse's / Your child's birthday
- Last 4 digits of phone number
- 1337
- 1234
- 3141
- 0000
- 9876

~50%
BUT I USE ANDROID’S SWIPE UNLOCK!
ONE SMALL PROBLEM
ONE SMALL PROBLEM
YES, SOMEONE DID A STUDY

SMUDGE ATTACKS ON SMARTPHONE TOUCH SCREENS

ADAM J. AVIV, KATHERINE GIBSON, EVAN MOSSOP, MATT BLAZE, AND JONATHAN M. SMITH

DEPARTMENT OF COMPUTER AND INFORMATION SCIENCE - UNIVERSITY OF PENNSYLVANIA
PARTIAL RETRIEVAL

96%
IN A NUTSHELL
PASSCODE / SWIPE SYSTEMS IN THE HANDS OF NORMAL USERS

(C) DAVID MONNIAUX
NOW FOR THE “WORRYING” PART

TAKING THINGS MULTI-PLATFORM
MULTI WHAT?
MALWARE RUNNING ON SEVERAL PLATFORMS
MALWARE RUNNING ON SEVERAL PLATFORMS

MALWARE CARRYING PAYLOADS FOR SEVERAL PLATFORMS
IMPLICATIONS
CORPORATE NETWORK

FIREWALLS,
ACCESS CONTROLS,
GUARDS,
DOGS,
CROCODILES

VULNERABLE SERVICE
EMPLOYEE'S PC

CORPORATE NETWORK

VULNERABLE SERVICE
EMPLOYEE’S PC

EMPLOYEE’S PHONE

CORPORATE NETWORK

Hacker

Target

VULNERABLE SERVICE
EMPLOYEE'S PC

EMPLOYEE'S PHONE

CORPORATE NETWORK

VULNERABLE SERVICE
DEMONSTRATION
SUMMARY
ARE WE SCREWED?
YES (YAY)
QUESTIONS?
THANK YOU FOR LISTENING.