Tom Stracener "Strace",
Contract Engineer
MITRE

EvilAdamSmith,
Sr. Security Consultant

Sean Barnum,
Cybersecurity Principal
MITRE

So Many Ways to Slap a YoHo: Hacking Facebook & YoVille

Misclaneous Disclaimers

Its Medicinal!

What is YoVille?

- It's part of the Zynga Family of games that are amazingly popular on Facebook.

YoVille Population: 5 Million Active Players

What is YoVille?

- Special thanks to Chris Peterson, VP of Application Security at Zynga.
- Zynga was aware of the security issues we brought to their attention

- A security fix for the issues we will discuss is in place
- The Facebook Application API can still be abused

Roadmap

1) Introduction

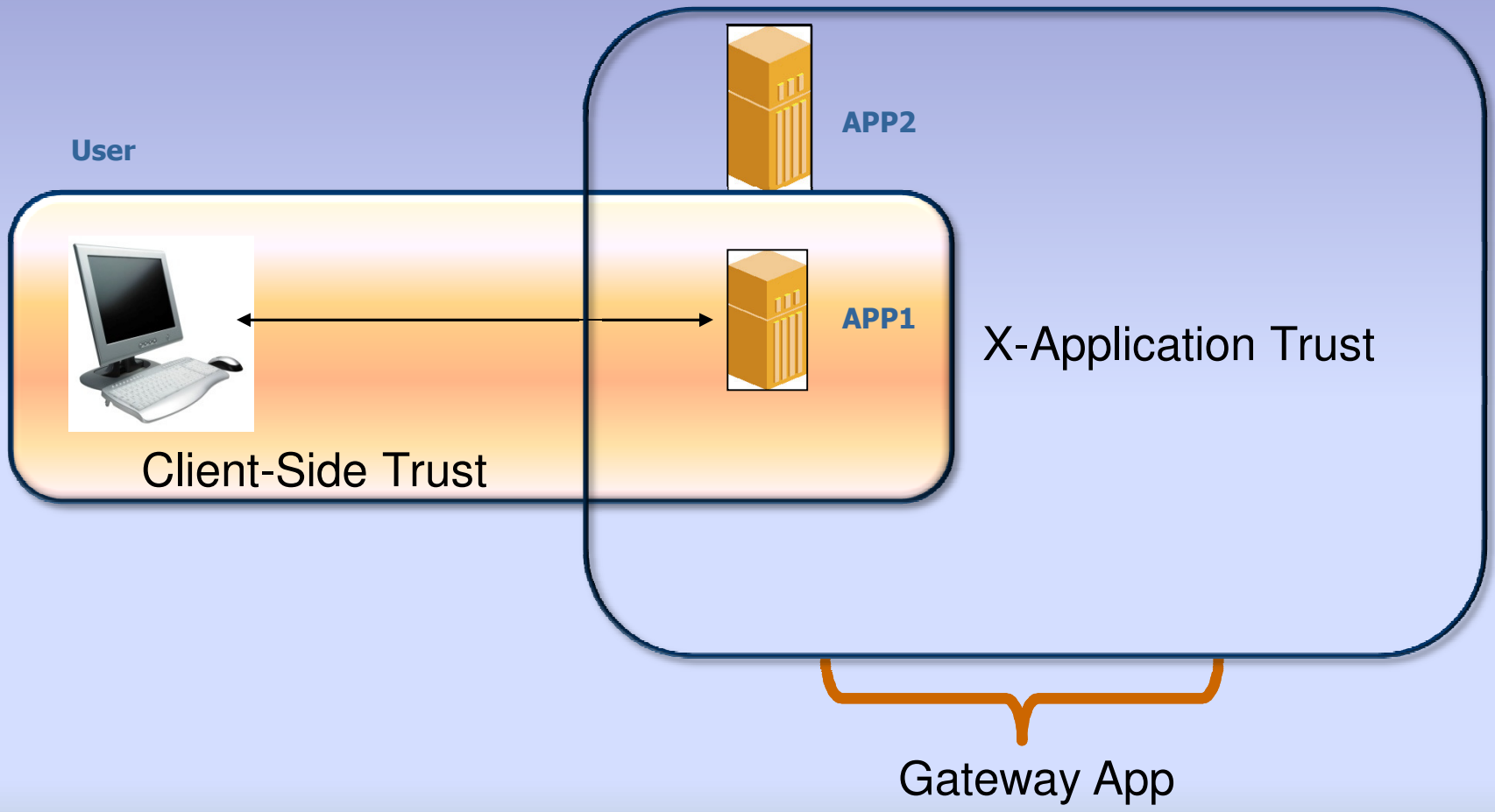
2) Client-side trust attacks within Application APIs

3) Attack Patterns Against Social Network Gaming

4) Impact of the attacks using YoVille as an example

5) How to keep your software off the stage at DEF CON

Client-Side Trust



Attack Characteristics

- ✓ Amplification: Attacker can use one compromised account to attack that users friends via social gaming.
- ✓ Deception: Phishers can create messages to lure users to click on malicious links or buttons, in some cases with the URI masked
- ✓ Easy to Exploit: By using a MITM proxy an attacker can create fake but legitimate looking prizes, gifts, or awards. Manipulating the API is trivial.

Attack Characteristics

- ✓ Trust: Since the attacks often originate from in-game friends or neighbors there is a greater tendency to trust the content as legitimate
- ✓ Stealth: Because the attacks happen at the layer of application logic they are very difficult to detect (i.e. no noisy metacharacters or scripts).
- ✓ Urgency: Users are trained to quickly click and claim items their friends discover before the item expires or is used up.

Attack Patterns for Client-Side Trust

1) Application API Manipulation via Man-in-the-Middle

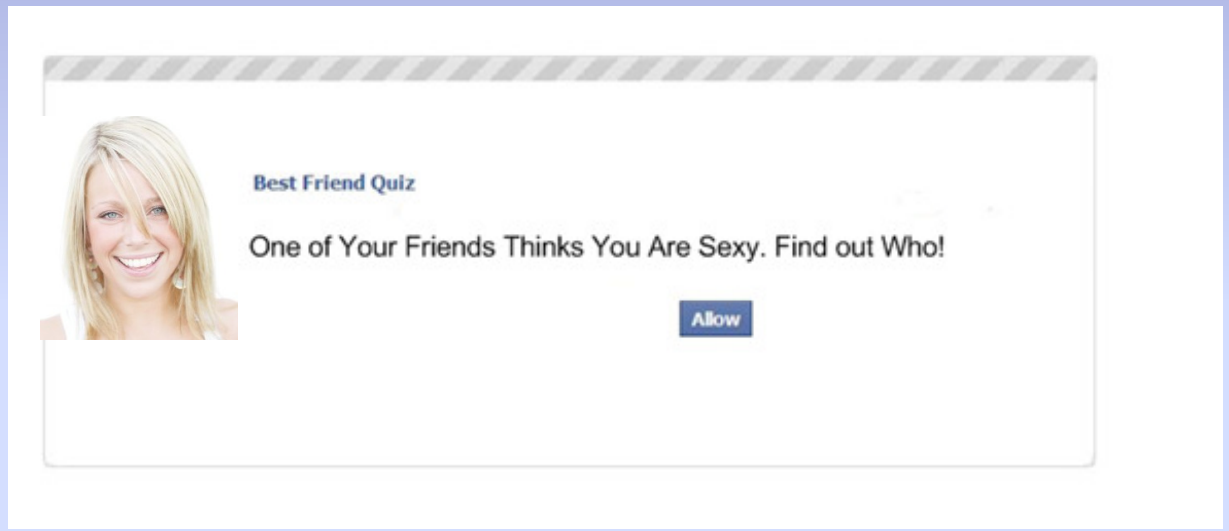
2) Application API Content Spoofing via API Manipulation

3) Transaction or Event Tampering via API Manipulation

4) Transaction or Event Replay via API Manipulation

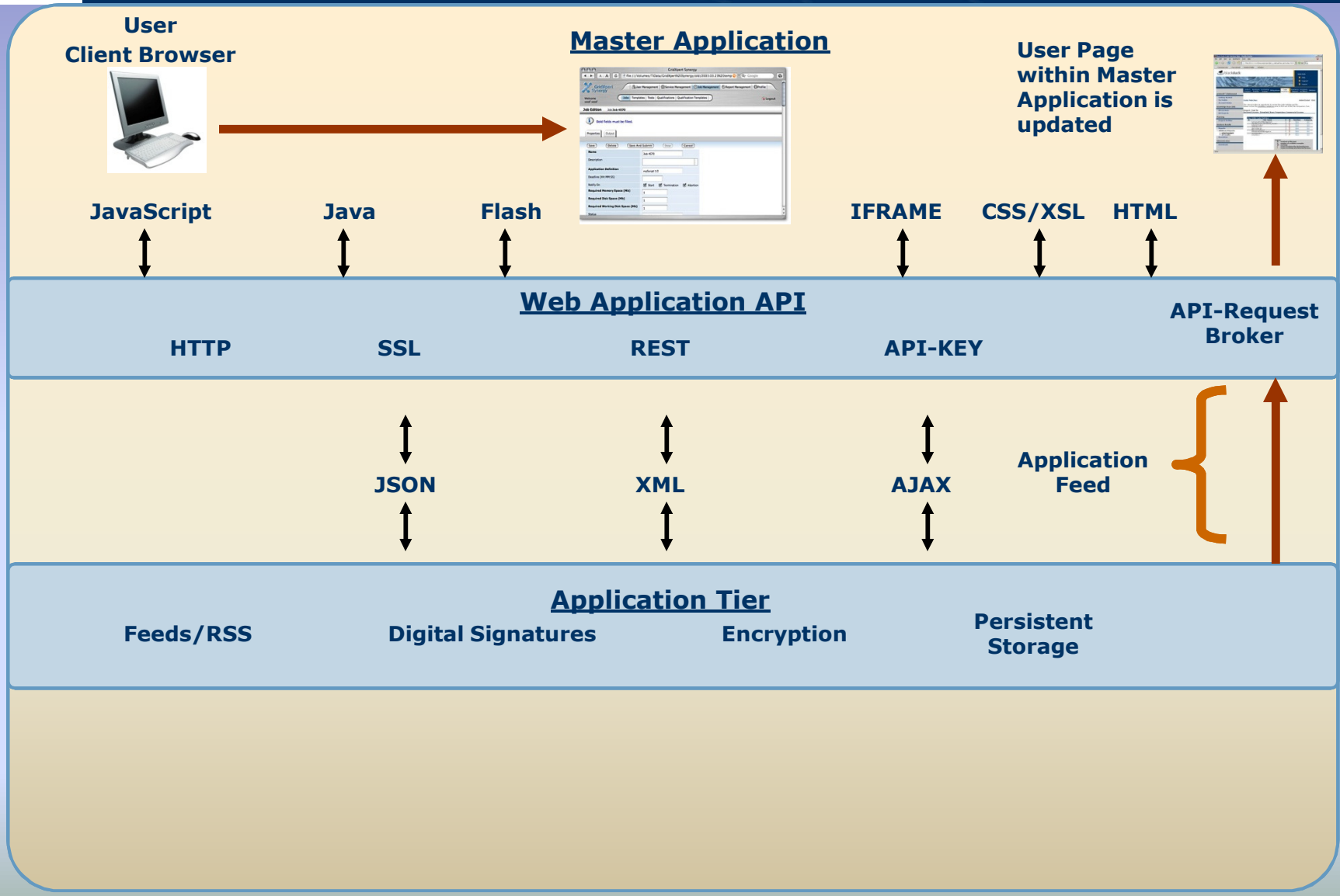
Attacks can prey on users interests or vanity

The best kind of lies are those we want to be believe…

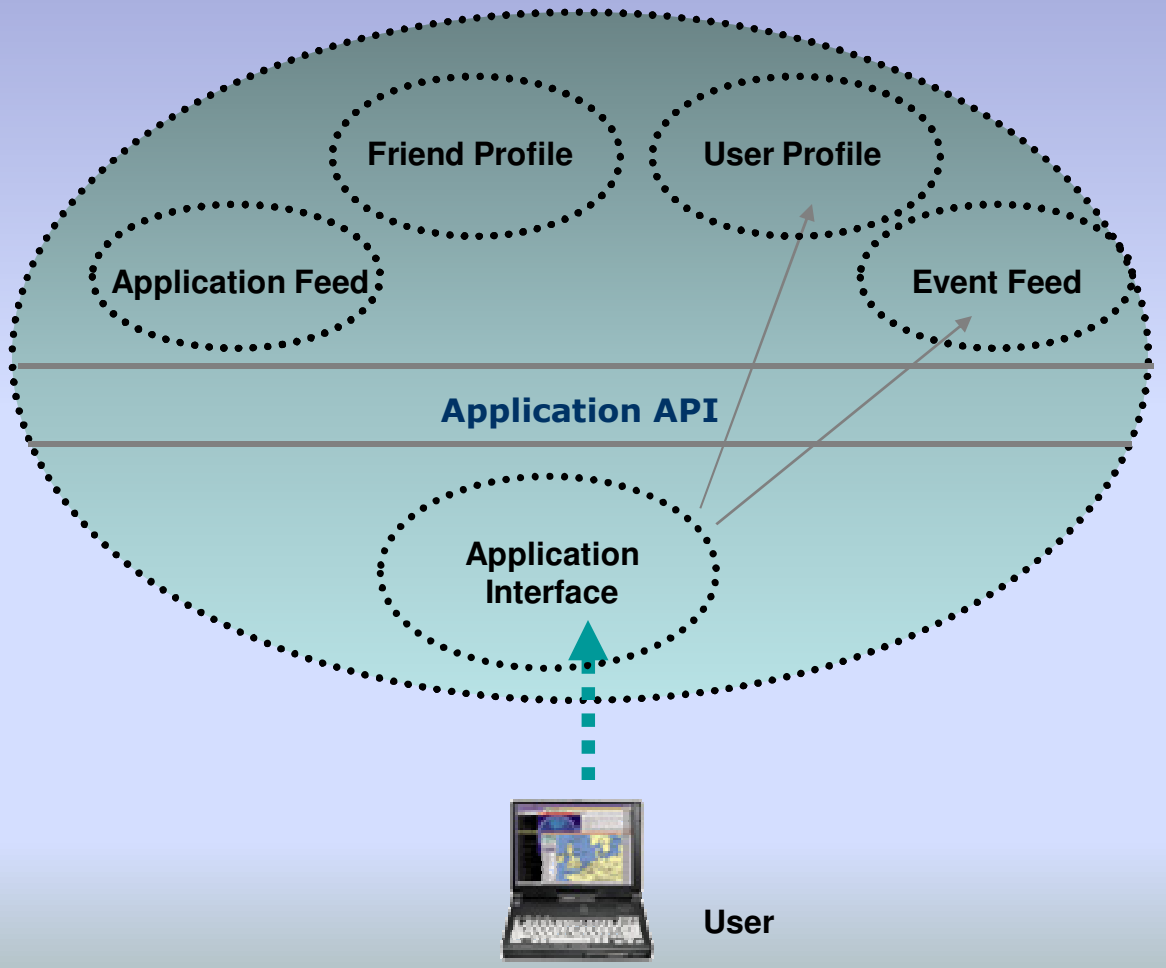


Clicking Allow takes you to a Adobe PDF exploit

Anatomy of a web 2.0 Application Framework

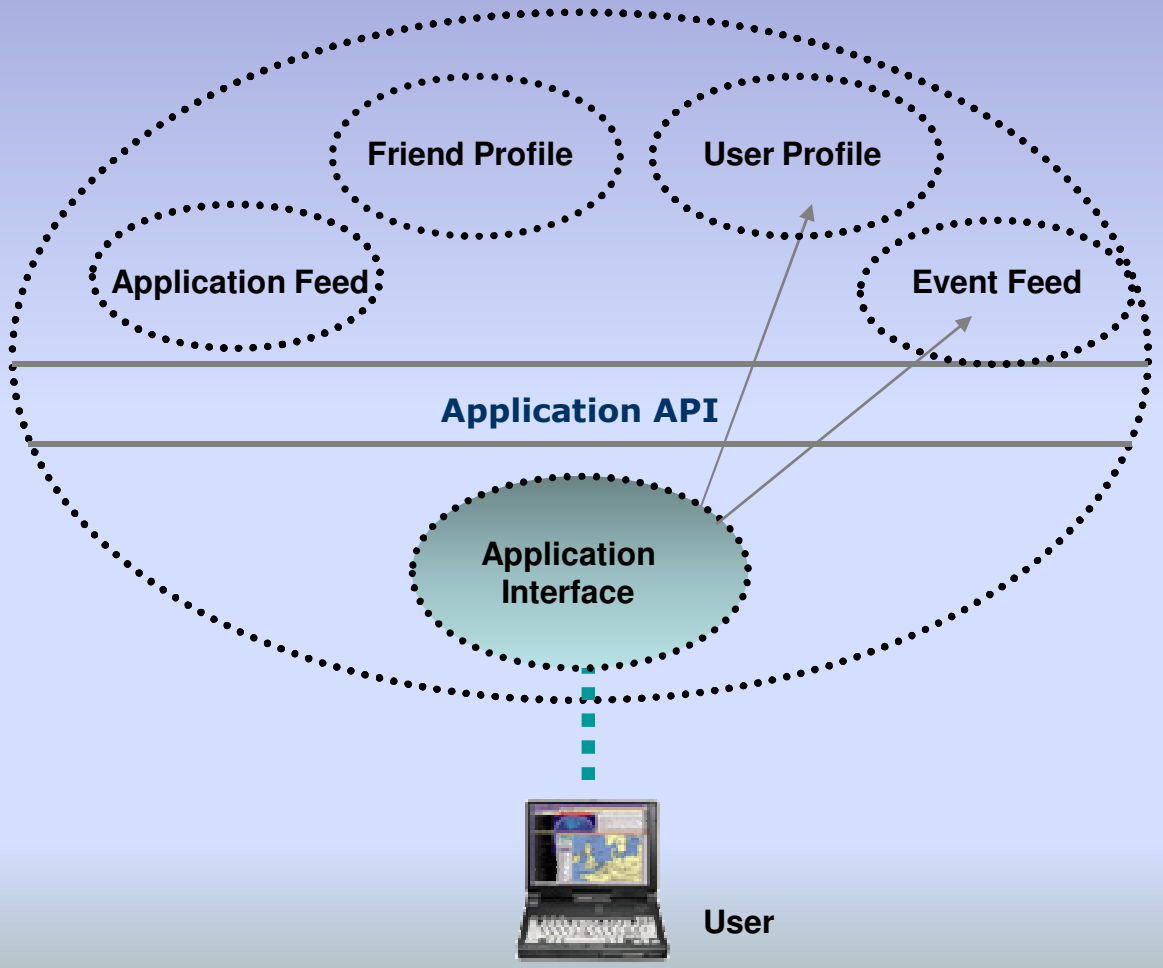


Application Framework & API



Application Framework & API

- IFRAME
- Flash
- Applet
- ActiveX



Application API Content Spoofing

An attacker is able to modify message content or make API calls to create arbitrary content within cross-application Messages

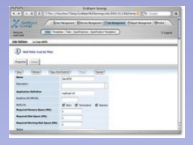
- **Root Cause:** Failure to protect data from modification (i.e. failure to ensure data integrity).
- **Impact:** Attacker can create deceptive content that enables social engineering attacks, phishing, or user harassment

Content Spoofing Example

Content can be spoofed by modifying messages or creating new messages via direct query

Attack Execution Flow: Spoofing

1. Direct API Call



Message can be a 'wall update' or a 'gift', for example

Application Acknowledgement 2.

Feed published to Gateway App via Feed 4.

5. Gift/Message Sent

Gift or Message is Delivered to Target

Cont.

Client

App API Method

Gateway App

App: GUI

Feed

GW: User News Feed

GW: Messages\Inbox

GW: Notification\Alerts

Attack Patterns

5) Application API Navigation Remapping

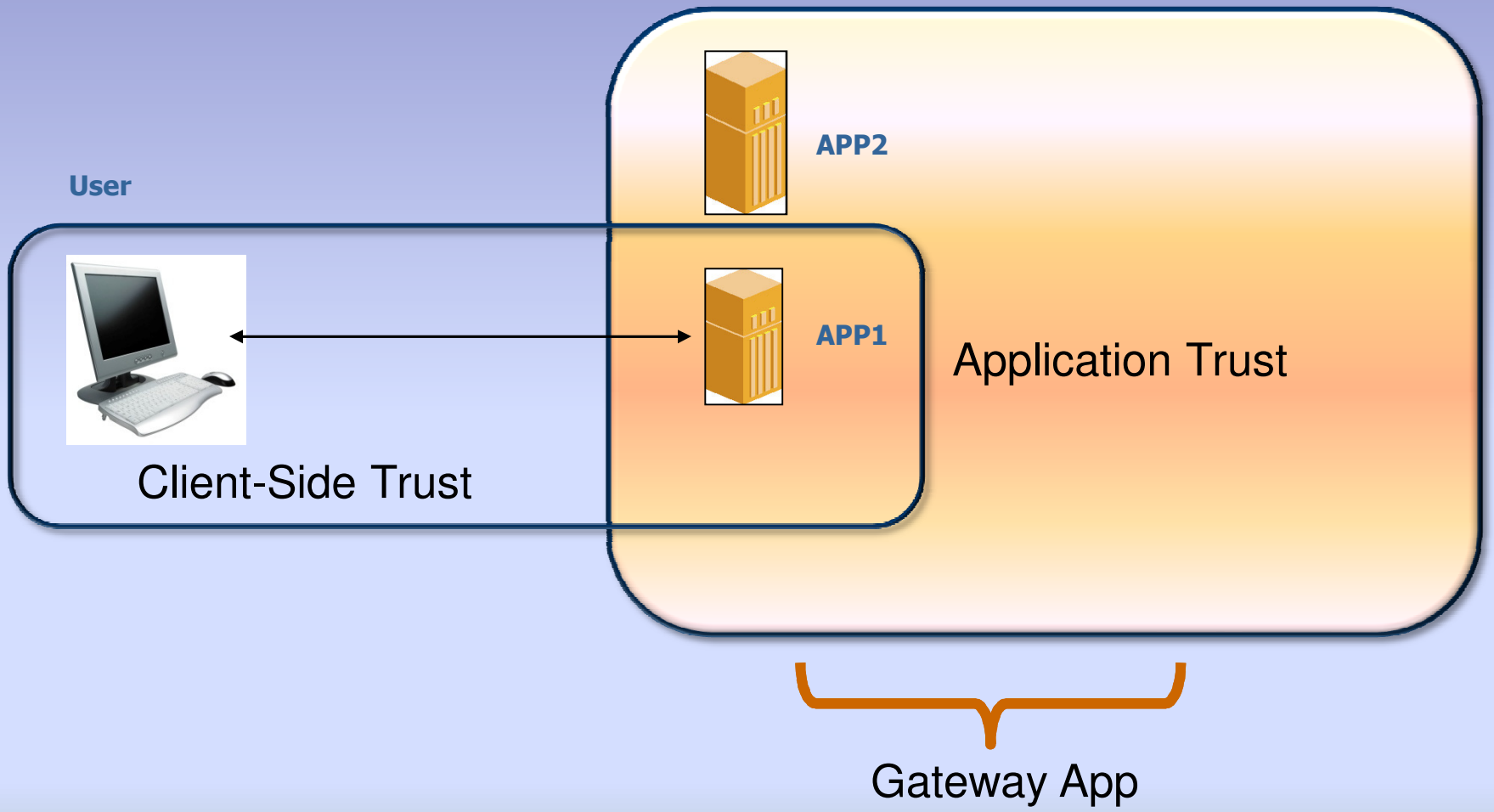
6) Application API Button Hijacking

7) Harvesting Usernames via API Event Monitoring

8) Exploit Injection via Application API Message

9) Malware Propagation via Application API Message

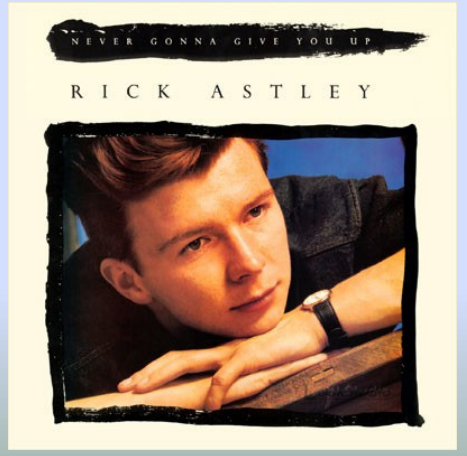
Application Trust Boundaries



Application API Navigation Remapping

When web application links that should point back to the application or its content are rewritten to trick users into following a malicious link.

- **Root Cause:** Failure to protect data from modification (i.e. failure to ensure data integrity).
- **Impact:** Potential compromise of user's machine and/or accounts via direct exploitation of browser or plugin flaws. Potential for spoofing, phishing, & authorization of malicious applications



API Request: Feed Processing

```
POST http://www.facebook.com/fbml/ajax/prompt_feed.php?__a=1 HTTP/1.1
Accept: */*
Accept-Language: en-us
Referer: http://www.facebook.com/connect/prompt_feed.php?locale=en_US
x-svn-rev: 253302
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.
2152; .NET CLR 3.5.30729; MS-RTC LM 8) Paros/3.2.13
Host: www.facebook.com
Content-length: 1861
Proxy-Connection: Keep-Alive
Pragma: no-cache
Cookie: datr=1254403372-89260de69f7f9ed40e6fde5f39e27abf2e1179ff524653c7166ae; lo=o33GkiXzEpSdBKh-I-Nd2g; lxe=strace%40gmail.com; lxs=2; c_user=
1409174187; lxr=1; sct=1274314001; sid=1; xs=8f7ea76b44fb16a3fb41794bee1182d2; presence=DJ275933229G32H1L1409174187MF275933228563WMblcMsn
dPBbloMbvtMctMsbPBtA_7bQBfAnullBuctMsA0QBblADacA8V275933229Z406BlcPBcvrADrA0.9BtsP275932874QQQ; force_hcfb=1
```

```
feed_info[template_id]=60341837091&feed_info[templatized]=0&feed_info[template_data][name]=Consider%20This%20B1TCH!&feed_info[template_data][description
]=&feed_info[template_data][href]=http%3A%2F%2Fapps.facebook.com%2Fyoville%2Findex.php%3Fpoe%3D94%26ifpid%3D138104352%26if%3D12%26d%3D%26s
k%3D4d8cae0f5bea9e0a9b9d477d6526fae3%2524%2524cgF5O.ST55bNY5%252AUCOK%252CStS8LpqyrpMxzaygV6US%26src%3Dfeed%26aff%3Difeed%26crt%3
D12&&feed_info[template_data][creative]=n0_c0_m0_a0&feed_info[template_data][caption]=%7B*actor*%7D%20recieved%20a%20BURNING%20CROSS%20from%
20someone%20to%20Welcome%20You%20to%20the%20neighborhood.%20DONT%20F@CK%20With%20TomDude%20AGAIN%20OR%20YOUR%20ACCOUNT%
20WILL%20BE%20PWNED%20AND%20YOU%20WILL%20BECOME%20THE%20BIGGEST%20FAN%20OF%20GOAT%20SEX%20ON%20FACEBOOK&feed_info[te
mplate_data][media][0][type]=image&feed_info[template_data][media][0][src]=http%3A%2F%2Fwww.splcenter.org%2Fimages%2Fimglib%2FK%2Fir_107_crossburnin
g_200x200.jpg&feed_info[template_data][media][0][href]=http%3A%2F%2Fapps.facebook.com%2Fyoville%2Findex.php%3Fpoe%3D94%26ifpid%3D138104352%26if
%3D12%26d%3D%26sk%3D%23sk%23%26src%3Dfeed%26aff%3Difeed%26crt%3D12&feed_info[action_links][0][text]=Claim%20Mystery%20Keys&feed_info[action_
links][0][href]=http%3A%2F%2Fapps.facebook.com%2Fyoville%2Findex.php%3Fpoe%3D94%26ifpid%3D138104352%26if%3D12%26d%3D%26sk%3D4d8cae0f5bea
9e0a9b9d477d6526fae3%2524%2524cgF5O.ST55bNY5%252AUCOK%252CStS8LpqyrpMxzaygV6US%26src%3Dfeed%26aff%3Difeed%26crt%3D12&feed_info[app_
has_no_session]=false&feed_info[body_general]&feedform_type=63&preview=false&feed_target_type=self_feed&app_id=21526880407&size=2&extern=1&privacy_da
ta[value]=80&privacy_data[friends]=0&&&&privacy_data[list_anon]=0&&privacy_data[list_x_anon]=0&&user_message=&nctr[_ia]=1&__d=1&post_form_id=79815067f5a
2adcd8164e7cbb2d33d6a&fb_dtsg=uXhu7&post_form_id_source=AsyncRequest
```

MITM Proxy view

Link (Navigation) Tampering

- &feed_info[template_data][name]=
  - Title of message,
  - clickable=Yes
- &feed_info[template_data][href]=
  - URL for message title
  - URI masked=Yes
- &feed_info[template_data][caption]=
  - Content of message
  - Clickable=No
- &feed_info[template_data][media][0][src]=
  - Location of Image
  - URI masked=Yes
  - Clickable=No
- &feed_info[template_data][media][0][href]=
  - link for image within message
  - clickable=Yes
  - URI masked=Yes
- &feed_info[action_link][0][text]=
  - Content of action text
  - URI masked=Yes
  - i.e. “Claim Mystery Keys”
- &feed_info[action_link][0][href]=
  - Content of message
  - Clickable=No
- &feed_info[template_data][media][0][src]=
  - Hyperlink for Message Image
  - URI masked=Yes

Link Tampering

Tom Stracener

Ass of Fire!

Lost and lonely hearts are Burning up in YoVille!

February 19 at 4:10pm via YoVille · Comment · Like · Collect the Ass of Fire

Link Tampering

Actor

[media][src]=
[media][0][href]=

&Feed_info[template_data][name]=

[template_data][href]

feed_info[template_data][caption]=

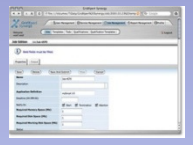
February 19 at 4:10pm via YoVille · Comment · Like

[action_link][0][text]

action_link][0][href]

Attack Execution Flow

1. Application Event



Game Application accessed via Gateway application

Application Event Message 2.

Game Application generates a structured API request to update Gateway App.

Attacker Modifies Link Destinations 3.

Event published to Gateway App via Feed 4.

Attack Patterns

5) Application API Navigation Remapping

6) Application API Button Hijacking

7) Harvesting Usernames via API Event Monitoring

8) Exploit Injection via Application API Message

9) Malware Propagation via Application API Message

Application API Button Hijacking
CAPEC: 388

You'll have to come see the talk. ;-)

Attack Patterns

5) Application API Navigation Remapping

6) Application API Button Hijacking

7) Harvesting Usernames via API Event Monitoring

8) Exploit Injection via Application API Message

9) Malware Propagation via Application API Message

Malware Propagation via Application API Message
CAPEC: 391

You'll have to come see the talk. ;-)

How to Keep Your Software off the Stage at DEF CON

To build secure software you MUST understand how it will be attacked

A broad understanding of the attackers perspective resides in the heads of a relatively small group of people - most of them are here this weekend

The only way to scale this knowledge is to capture and share it in a structured and standardized way

CAPEC

http://capec.mitre.org

CWE

http://cwe.mitre.org

Attack Patterns for Social Gaming

Application API Manipulation via Man-in-the-Middle	**CAPEC-383**
Application API Content Spoofing via API Manipulation	**CAPEC-384**
Transaction or Event Tampering via API Manipulation	**CAPEC-385**
Transaction or Event Replay via API Manipulation	**CAPEC-386**
Application API Navigation Remapping	**CAPEC-387**
Application API Button Hijacking	**CAPEC-388**
Harvesting Usernames via API Event Monitoring	**CAPEC-389**
Exploit Injection via Application API Message	**CAPEC-390**
Malware Propagation via Application API Message	**CAPEC-391**

Prescriptive Guidance

In other words: How do I avoid this $H17?

You'll have to come see the talk. ;-)