Satan Is On My Friends List
Attacking Social Networks
We’re in your Extended Network!

★ Nathan Hamiel
★ Senior Consultant @ Idea InfoSec
★ Associate Professor at UAT
★ Facebook, LinkedIn, MySpace, Twitter

★ Shawn Moyer
★ Hacking for dollars @ FishNet Security
★ BH speaker, multipurpose windbag
★ LinkedIn, Twitter, kinda-sorta Facebook

[ Please pay us to come break your web apps. kthxbye. ]
And so is ....

satan

Male
69 years old
CONNECTICUT
United States

Last
Login: 03/07/2008

View My: Pics | Videos

Contacting satan

satan is in your extended network

satan's Latest Blog Entry [Subscribe to this Blog]

[View All Blog Entries]

satan's Blurbs

About me:

Who I'd like to meet:

satan's Friend Space (Top 7)
No animals, bloggers, journalists or camwhores were harmed during these demonstrations. While actual SocNet sites and users were involved, all payloads were benign and only resulted in wounded pride and possibly high blood pressure.

We are not experts and should not be trusted in any way. Always ask your doctor before changing prescriptions or viewing LiveJournal session captures.

MySpace contains the most feature-complete OpenSocial implementation. Many of the issues discussed here are on their platform.

The rest of you guys suck too, srsly. We mean it.
So, WTF is this about?

★ Our obsession with SocNets, mostly.
  ★ Impromptu threat modeling over ${drinks}$.
  ★ Various (harmless) sorties on SocNet sites.
  ★ SocEng experiments and silliness.

★ But... Are you dropping 0day?
  ★ No, at least we don't think so...
  ★ "Featurebilities". Design flaws. Architecture FAIL.
  ★ They put it there... On purpose! Srsly!
  ★ Still, lots of soft, squishy attack surface.
Roadmap and Nickel Tour

★ SocNets as attack platform
★ Millions of users targets
★ Business model: Ads, user-generated content

★ Vuln Mashups 2.0
★ Promiscuous and pervasive trust
★ SocEng + vulns = attacker ROI

★ Dance, monkey, dance!
★ Demos-of-shame, captures, bugs
★ Things we wish we could un-see
Roadmap and Nickel Tour

★ App threats (OpenSocial, FB)
  ★ Attacking clients with apps
  ★ Attacking apps with apps
  ★ SocNet as lightweight Botnet.

★ CSRF-palooza
  ★ Innocuous functions and escalation
  ★ Broken token + breaking the membrane

★ External content. Bad. Discuss.
  ★ Markup, attributes, blacklisting. Fail.
Don’t Taze Us, Bro...

★ Please don’t hate, Chris.
★ You seem very cool. :)
★ Still, this is a lot of fail, in one handy package.
External Content = Fuxor

★ Link to crap offsite = epic fail
★ IMG tag CSRF
★ CSS Jscript hijacking, click fraud, SocNet as botnet
★ MySpace, Hi5, LiveJournal, many others.

★ Request Conversions (SSRF)
★ POST to GET
★ Sometimes enforced / validated differently based on method
★ Viewstate MAC, params, auth components
★ We don’t need XMLHTTP kung fu for GET-based CSRF
Meet Alice, Bob, and Eva
External content -> CSRF

MySpace add hack
Innocuous Functions

★ Most sites protect functions that appear valuable
  ★ Account changes, messaging, profile admin
  ★ Computationally expensive, overhead
  ★ Tokenized against CSRF (varying entropy... Brutable?)

★ Things that don't appear valuable
  ★ Logging out
  ★ Blocking communication
  ★ Friend adds, apparently
  ★ Lots of other stuff
MySpace DoS (Irritation)
No JavaScript, No Problem

★ There may be other ways ;)

★ <img src="http://domain.com/redirected_image">

★ <meta http-equiv="refresh" content="0;url=http://domain.com/whatever">

★ <iframe src="http://domain.com/whatever"></iframe>
Logic Attacks on SocNets

★ Attacks don't always have to be so straightforward

★ Extremely difficult to identify through automated testing.

★ AdultFriendFinder privilege escalation

★ It’s a SocNet, right? We think so!

★ Allows for the viewing of paid for content
Elite AFF pwnage. Ph33r.
We did you a favor, we promise.
Pwning Kevin Bacon

★ SocNet attacks = SocEng++
  ★ Much of this is about blended threats.
  ★ The social and technical are always linked.

★ This is why this stuff was so fun!
  ★ Generally, we PoC the technical or social.
  ★ Why "weaponize the obvious"? [ @dakami ]
  ★ The combination of the two get ugly FAST.
Profiling and OpSec

★ It's on a public site, you eee-diots!
★ We think ID theft via SocNet is hype
★ You shared it, so ASSUME IT'S PUBLIC
★ If you give your CC to FB, you deserve to fail
Profiling and OpSec

★ It's on a public site, you eee-diot!

★ We think ID theft via SocNet is hype

★ You shared it, so ASSUME IT'S PUBLIC

★ If you give your CC to FB, you deserve to fail
Some SocEng sorties

★ SocEng = low line noise, high hit rate
    ★ Great ROI for a targeted attack.
    ★ Diamond-tipped spearphishing. =)

★ Build a plausible profile
    ★ Public sources, company data
    ★ Get “respectable” # of connections

★ And then what, pray tell?
    ★ We just built friends / connections
    ★ Real attack: mail / msg custom payload
Marcus was concerned about SocNets. He agreed to help us out.
The Marcus Experiment

Profiling was pretty trivial
★ Press releases, bios, articles
★ Took us about 3 hours to build

But, wait... How to build connections?
★ Need quick legitimacy (friends, groups)
★ Meet the linkwhores! =)
The Marcus Experiment
The Marcus Experiment
The Marcus Experiment

The end result

- 50+ connections in less than 24 hours
- CSOs, bigwigs, CISSPs, feds, ISSA ppl, and my personal favorite...

Join my network on LinkedIn
From: Kristin Franceschi
Date: June 15, 2008
To: Marcus J. Ranum
Status: Pending

Kristin Franceschi has indicated you are a Classmate at The Johns Hopkins University:

Whoa! You are there now! Can I be in your network?

[Accept]  [I don't know Kristin]  [Archive]
DoppelGadi!

@GeorgeVHulme It's not something I can talk to yet, but yes, it's there.

RealPlayer bug again. The botmasters will have a busy weekend. http://tinyurl.com/5ijegp about 2 hours ago from web

RealPlayer stack overflow from ZDI. Anyone knows this is different than the heap bug? http://tinyurl.com/65umzpz about 4 hours ago from web

Spam King dead in apparent suicide: http://blogs.zdnet.com/secu... about 5 hours ago from web

First 1M $ phishing fraud hits inboxes: http://tinyurl.com/8lkqgh about 6 hours ago from web
MySpace Apps and OpenSocial

Accessorize with Malware
apps.myspace.com

Your bling just bit you in the ass, douchebag.
User-Installed Nunchaku

★ Who needs vulns?
★ Convenient APIs, 100% arbitrary code
★ OpenSocial: "Write once, own anywhere." (tm)
★ Pick a meme, get installs... Then "go rogue".
★ Your own personal botnet, for a few lines of PHP.

★ SocNet sites DON’T CARE. Period.
★ EULA and separate domain = zero responsibility
★ Arbitrary execution on most sites
★ Little to no validation (vetting process, # friends)
★ Any app can attack another app (same domain)

Let’s Fighting Love
Origin Shmorigin

★ What about same origin?
★★ What are you attacking? Site, or user?
★★ API functions allow you to proxy requests
★★★ Comes from server, not client though ;)
★★ GETs
★★ POSTs

★ Depends on the attacker and goal.
★★ Are you targeting the site itself?
★★ Can still hit many clients via apps
★★ Useful for propagation: installs, messages, adds
★★ We can also CSRF via simple GETs w/o XSS
Pudding and Proof

Nathan

Mood: sneaky
View My: Pics | Videos

Contacting Nathan
- Send Message
- Add to Friends
- IM / Call
- Add to Group
- Forward to Friend
- Add to Favorites
- Block User
- Rank User

CSRfer
Coming Soon

Nathan is in on your network.

Nathan's Latest Blog Entry [Subscribe to this Blog]
[View All Blog Entries]

Nathan's Blurbs
About me:
I am Nathan. I am a security professional and a professor at a University. I spend most of my time pondering problems of the world and trying to work solutions for them. I have been involved with art and music most of my life as well.

Who I'd like to meet:
All of the members of the A-Team.

Are you down with the Hex?
function makeRequest(url) {
  var params = {};
  params[gadgets.io.RequestParameters.METHOD] = gadgets.io.MethodType.GET;
  gadgets.io.makeRequest(url, response, params);
};
OpenSocial POST Request

★ OpenSocial POST method

```javascript
function makeRequest(url, postdata) {
    var params = {
        postdata = gadgets.io.encodeValues(postdata);
        params[gadgets.io.RequestParameters.METHOD] = gadgets.io.MethodType.POST;
        params[gadgets.io.RequestParameters.POST_DATA] = postdata;
        gadgets.io.makeRequest(url, response, params);
    }

    function response(obj) {
        alert(obj.text);
    }

    var data = {
        data1 : "test",
        data2 : 123456
    }
    makeRequest("http://example.com", data);
}
```
More on OpenSocial Requests

★ You can add your own headers

★ Reference for 0.7 OpenSocial

★ http://code.google.com/apis/opensocial/docs/0.7/reference/

★ Relay.proxy smells like fail.

★ MySpace server makes the request for you, even without an app or dev access.

http://api.msappspace.com/proxy/relay.proxy?
opensocial_token=sMAPei0219jvS7VQaBVWaKTsl6cFED5lwyeMNNFEIzQgqBRJbhXM8EugjDvqPIFS8uDTHfGEYGe74uvFMCQ/Uu2mTyxAQaILH3w55n3u8=&opensocial_url=http%3A//www.hexsec.com
Routing Traffic via MySpace

WhatIsMyIP.com

The fastest and easiest way to determine your IP address.

- IP Address
- IP Command Lines
- IP Addresses Explained
- Speed Test
- Automation
- What’s New

Your IP Address Is 204.16.33.73
MySpace Apps Capabilities

If provided it, an app can get:
- Interests
- Heros
- Photo Albums
- Friends / Connections

If you provided it to the app, it's probably offsite:
- Delivers code via the API
- Deliver off-site code / content via iframe
SocNet Apps Jujitsu

★ Attacking social net is trivial.
★ Apps are delivered as:
  ★ External site though iframe
    ★ Functionality on Canvas
    ★ Functionality on Profile
    ★ Functionality on Home
  ★ Contained app grabbing external content
    ★ Functionality in same areas as above
★ Coded by people who shouldn't be writing code
  ★ Trivial to find out who has what apps installed ;)
  ★ Let's look at a couple examples.
Keep It Real

★ Allows for “secret” communication
Keep It Real 0wn3d

★ The ownage
Sexual Positions Poll
★ Kama Sutra poll
Properly Done?

- An self-contained OpenSocial app not an offsite iframe.
- Utilizing signed requests with authtype=SIGNED.
- Request tampering still worked. Why?
Kiss Me App Ownage

api.msappspace.com:80/proxy/relay.proxy?
opensocial_authtype=SIGNED&opensocial_token=Yn7XsoORUtjDaANU0WRKylJula6QvUQYG0VrTU7NSFXXweXSLAomgmuGb1egf5XSDwilli29lim+UduxZUBzFnf9S0QIwFTLNi+34gg91s=&opensocial_url=http%3A//kiss-dynamic-lb.myspacegamingapps.com/hugme/sendmessage%3Fnetwork%3Dmyspace%26to_user_id%3DREMOVED%26type%3DKISS%26from_user_id%3DREMOVED%26from_user_name%3Dcstm_REMOVED%26from_user_profile%3Dhttp%3A//a680.ac-images.myspacecdn.com/images01/110/REMOVED.jpg%26nocache%3D1217872981976
Cajoley Caja, Batman!

★ Caja is meant to create "safe" JavaScript in OpenSocial

★ Tries to un-suckify .js, removing:

★ eval()

★ top.location

★ And many others...

★ Demonstrates the way this problem is typically approached anyway.

★ Seems irrelevant if it’s opt-in.
DoSer Function?

★ Stupid test MySpace app
★ 7 seconds after viewing, it logs you out
★ Logs anyone out that views your page for 7 seconds
★ Logs you out after viewing for 7 seconds ;)
★ Demonstrates content on canvas, profile, and home
Surfs Up!

★ Meet CSRFer
- Demonstrates 3 different ways to do CSRF on MySpace
- Image tags, iframes, and meta tags, oh my!
- Demonstrates content on canvas, profile, and home
Are we hosed? Plz advise.

★ Kill external content
★ Drastically reduce API functionality
★ Threat model your stuff, people
★ Props to late adopters. =)
★ No opt in security models
★ Developers, Developers, Developers
★ Profile lifetime bit (member since / training wheels)
★ Email verification for corporate socnets
★ Create a profile, before someone else does ;)