

Web 2.0 and Beyond

Technology challenges, risks and rewards

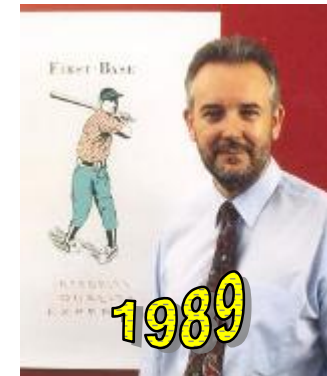


Peter Wood
Chief Executive Officer
First • Base Technologies LLP



Who am I ?

- Worked in computers & electronics since 1969
- Founded First Base Technologies in 1989
(one of the first ethical hacking firms)
- Primary roles:
 - Network penetration tester
 - Social engineer
 - Conference speaker
 - TV and radio security 'expert'
 - Security author
 - Active member of BCS, IISP and ISACA
 - Member of CEP Management Team





Scope

- Where is your security perimeter when many endpoints are mobile handheld devices?
- How do you enable good governance whilst taking advantage of the cloud?
- What are the legal, confidentiality and availability issues in the cloud and in Web 2.0?
- What happens when your interaction with customers is immediate and intimate through Web 2.0?





Web 2.0 and Beyond

Technologies and expectations



'Generation Y' technologies

- Blogs and Wikis
- Social networking
- Instant Messaging
- Web conferencing
- VoIP
- P2P
- IPTV



flickr™

facebook

BitTorrent



bebo

plaxo



webex

skype™

LinkedIn

twitter



Generation Z or I ?

- Generation I (*according to Bill Gates, 1999*)
 - The Internet Generation - "Digital Natives"
 - The first generation to grow up with the Internet
 - Lifelong use of communications and media technologies:
 - Web
 - Instant messaging
 - Text messaging
 - MP3 players
 - Mobile phones
 - YouTube
- 
- A photograph of three women sitting on a couch. The woman on the left is looking at a mobile phone. The woman in the middle is looking at a laptop. The woman on the right is reading a newspaper.
- No longer limited to the home computer, the Internet is now increasingly carried in their pockets on mobile devices



The Value Of Corporate Secrets

- Secrets comprise 62% of the value of firms' information portfolios and are twice as valuable as custodial data.
- Enterprises devote 40% of their security budgets to compliance and 40% to securing secrets.
- Firms focus on preventing accidents, but theft is where the money is. Employee theft of sensitive information is 10 times costlier on a per-incident basis than any single incident caused by accidents.
- The more valuable a firm's information, the more incidents it will have. High-value enterprises had four times as many security incidents as low-value firms.
- CISOs do not know how effective their security controls actually are. Nearly every company rated its security controls to be equally effective - even though the number and cost of incidents varied widely.

The Value Of Corporate Secrets, Forrester March 2010



Security vs the Digital Native

“... although data breaches and accidental losses of sensitive information get most of the headlines, intentional theft of corporate data causes 10 times more financial loss.”

The Value Of Corporate Secrets, Forrester March 2010

“I wonder how the culture of corporate secrecy relates to the evolving world of digital natives. A digital native is used to having a lot of control over data: see how Apple caved in to selling music without copy protection. The digital natives I know are as likely to have ripped movies as DVDs.

On the other hand, companies that cater to digital natives, like Apple, are notorious for their corporate secrecy. It will be interesting to see how this plays out.”

<http://www.cryptosmith.com/archives/983>



Web 2.0 and Beyond

Information Leakage





Information leakage

- Exposure of
 - Corporate hierarchy (social engineering)
 - E-mail addresses (spam, social engineering, malware)
 - Phone numbers (sales calls, social engineering)
 - Technical infrastructure (hacker footprinting)
 - Business plans (industrial espionage)
 - Sensitive information (legal, contractual penalties)

... and identity theft: personal and business



Bruce Schneier's view

- People have always talked about work to their friends
- Historically, organizations generally didn't care very much. The conversations were intimate and ephemeral, so the risk was small.
- What has changed is the nature of how we interact with our friends
- We talk about our lives on our blogs, on social networking sites such as Facebook and Twitter, and on message boards pertaining to the work we're doing
- What was once intimate and ephemeral is now available to the whole world, indexed by Google, and archived for posterity
- A good open-source intelligence gatherer can learn a lot about what a company is doing by monitoring its employees' online activities



Social networking from a hacker's perspective

- “It's the easiest way to passively gain intelligence on the largest groups of society and nearly every walk of life”

Robert Hansen, aka RSnake, founder of SecTheory LLC

- Social networking sites by nature aren't secure
- They typically don't authenticate new members - you can't always be sure that your online friend is who she says she is - and attackers can easily exploit and capitalize on the “trusted” culture within the social network
- Users often don't deploy the security and privacy options that some of these sites offer, either

Kelly Jackson Higgins, DarkReading



LinkedIn from a hacker's perspective

- Hamiel and Moyer demonstrated that you don't even have to have a social networking profile to be targeted
- They were able to easily impersonate Marcus Ranum (with his permission) on LinkedIn
- Ranum didn't have an account, so they lifted Ranum's photo off the Internet and gathered information on him online and built a convincing phony Ranum profile.



The Marcus Experiment



Marcus was concerned about SocNets. He agreed to help us out.



The Marcus Experiment

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





Please burgle my house

A survey of >2,000 social media users in UK:

- 38% posted status updates detailing their holiday plans
- 33% posted that they are away for the weekend

Legal & General's Digital Criminal Report

"We were saying, 'This has been the best vacation we ever had'," Claudette McCubbin said about her recent vacation to Florida.

Unfortunately, all the relaxation was lost when they arrived back to Knoxville Wednesday. The family room and bedrooms in the West Knoxville house were all trashed. Thousands of dollars in electronics were missing.

Claudette posted messages stating when the family was leaving and how much fun they were having when they arrived in Florida. "I wanted to share with our friends everything that we were doing. We know a lot of people. We have a really good support group. Who would've thought that one of them [a thief] saw that or maybe a friend of a friend. That was a huge mistake," Claudette said.



WBIR.com
02/04/2010

© First Base Technologies 2010



Twitter from a hacker's perspective

- Twitter introduces a whole other element to social networking security - physical security ... leading to burglary, stalking, etc.
- "I never talk about where I am, who I'm with, where I'm going, or any other specific details, but that doesn't stop anyone else who knows that same information from doing that behind my back - maliciously or not."

Robert Hansen, aka RSnake, founder of SecTheory LLC



PLEASE ROB ME



Raising awareness about over-sharing

Check out our [guest blog post](#) on the CDT website.

Recent Empty Homes

7 new opportunities



@acejam left home and checked in **about a minute ago**:

I'm at LogMeIn (500 Unicorn Park, Woburn). <http://4sq.com/aA8EJE>



@pagetx left home and checked in **about a minute ago**:

I'm at Hilton Austin Hotel (500 E 4th St, Neches St, Austin).

<http://4sq.com/5lmzhQ>



Web 2.0 and Beyond

SocNet Hacking

WTF is this about?

- ▶ SocNets as attack platform
 - ▶ Millions of users^H^H^H^Htargets
 - ▶ Business model: Ads, user-generated content
- ▶ Vuln Mashups 2.0
 - ▶ Promiscuous and pervasive trust
 - ▶ SocEng + vulns = attacker ROI
- ▶ App threats (OpenSocial, FB)
 - ▶ Attacking clients with apps
 - ▶ Attacking apps with apps
 - ▶ SocNet as lightweight Botnet





Cross-site scripting and cross-site request forgery attacks

- XSS: malicious code is injected into vulnerable web applications and users who view those pages can get hacked
- CSRF: an attacker tricks the victim's browser into making a request as the logged-in user
- A CSRF attack could jump and spread across multiple social networking sites that the user is logged on to - spreading the attack from one social network to another

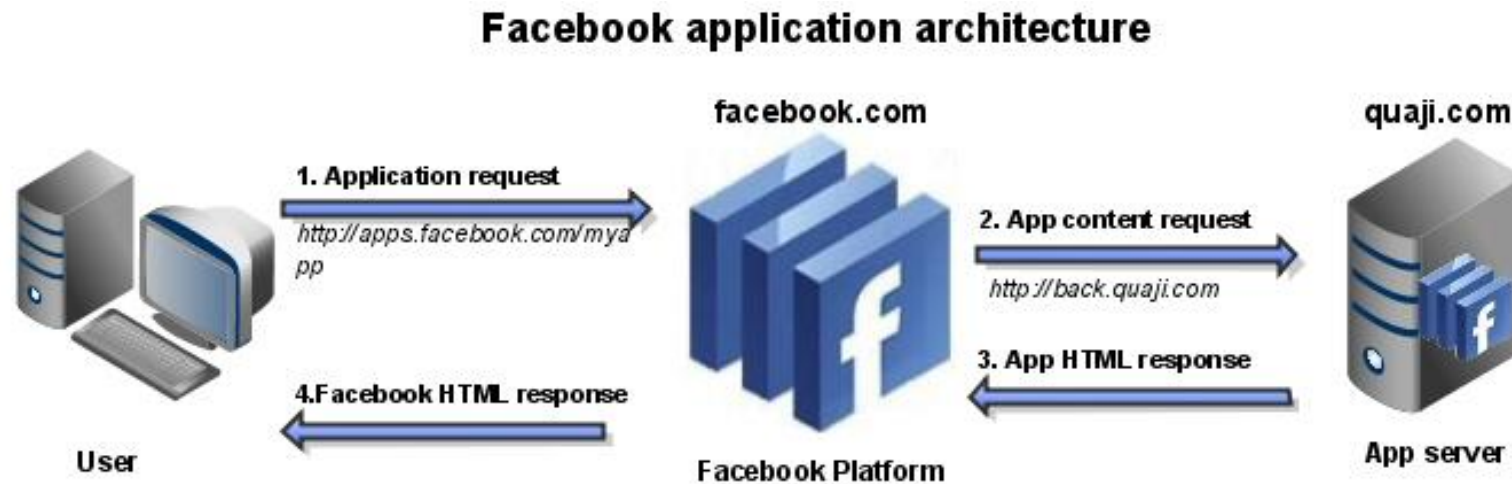
HD Moore, director of security research for BreakingPoint Systems



Cross-site request forgery attacks

A Facebook application has a “front” address in the apps.facebook.com domain. The user accesses this address, then Facebook itself contacts the app server for the content through its real address

<http://blog.quaji.com/2009/08/facebook-csrf-attack-full-disclosure.html>



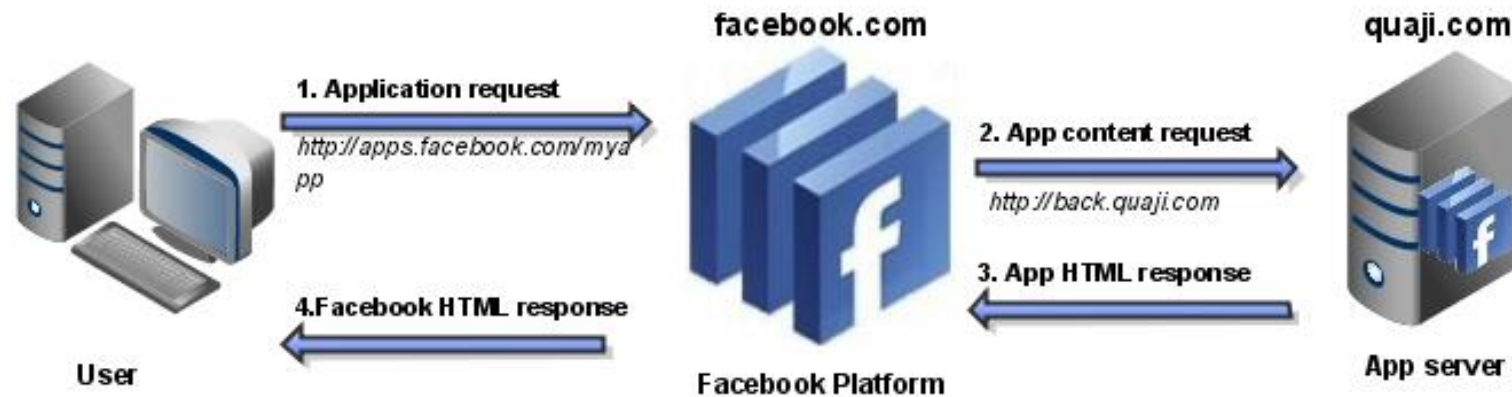


Cross-site request forgery attacks

Facebook has a module called Automatic Authentication (which sounds like trouble just by its name...) This mechanism allows the app to receive some of the user's info automatically, without the user's consent. These details include full name, profile picture, and friends list.

<http://blog.quaji.com/2009/08/facebook-csrf-attack-full-disclosure.html>

Facebook application architecture





Cross-site request forgery attacks

A simple redirect from one page to another in the same application fools Facebook because the second request originates from a Facebook URL (the first request). Therefore, the second request activates Automatic Authentication and personal info is sent.

The simplest way to exploit this is by luring the innocent user to a page on our website (say by sending a link in the mail). In this page we can cause the user's browser to access any URL (using a hidden IFRAME for example). Specifically we'll send the user to: <http://apps.facebook.com/hacker-app/step1.php>.

This will cause the browser to then go to [step2.php](#) and we get the info.

<http://blog.quaji.com/2009/08/facebook-csrf-attack-full-disclosure.html>

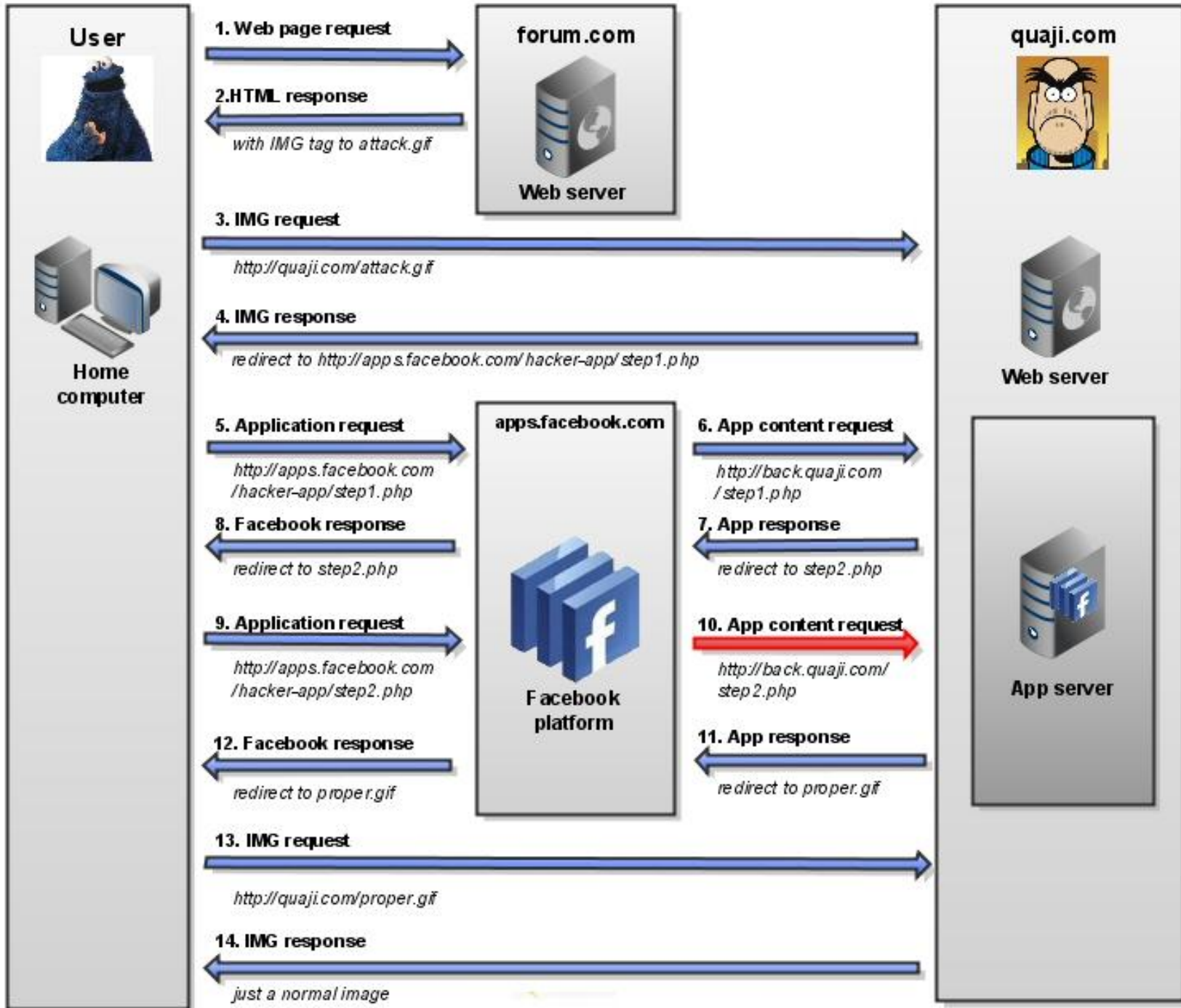


Cross-site request forgery attacks

We can craft the entire thing in an IMG tag. An IMG tag also causes the browser to go the specified address looking for image data. And if the the browser recieves a redirect response, it relentlessly goes through it looking for those pixels.

The huge difference between the two approches is that many blogs/forum sites allow user comments to contain IMG tags, and therefore the attack can be launched without having the user visit our website. Instead, merely viewing a "treated" forum thread will cause the attack to take place.

<http://blog.quaji.com/2009/08/facebook-csrf-attack-full-disclosure.html>





Web 2.0 and Beyond

Web 2.0 Malware



Malware

- Malware opportunities through
 - Fake links & apps in SocNet sites
 - Infection via IM channels (and SpIM)
 - Infection via peer-to-peer (P2P)
 - E-mail
 - Flash and movie files
 - Spyware installed silently by P2P client software



Malware on LinkedIn

Malware Targets LinkedIn Users



Malware Targets LinkedIn Users

by [Andy](#) on January 9th, 2009 in [Security Alert](#).

The business-oriented social networking site, [LinkedIn](#), has had a recent bout with malware, as you may have seen by all of the [buzz this week](#) in the news headlines. As most of you who use them know, social networking sites, while having many advantages to users, have long been targeted by socially engineered scams - meaning you need to take care when roaming around on these types of sites.

In terms of the issues seen lately on LinkedIn - profiles on the site were created to act as a staging point for the distribution of 'FakeAlert' software. This malware serves typical scareware messages claiming that your machine is infected and that you should install the rogue anti-malware application that the warning message is peddling. Despite the FTC's recent efforts in tackling the scourge of rogueware, the fact that these applications continue to proliferate proves they still provide a significant return of investment for malware authors.

January 2009
www.lavasoft.com



Malware on Facebook

- Users don't always realize that third-party widgets for Facebook, for example, aren't written by Facebook
- Some collect more information than necessary or safe
- Others have been written specifically to install adware or generate revenue
- "Secret Crush" on Facebook spread spyware
- Victims received an invitation to find out who has a secret "crush" on them, lured them into installing the Secret Crush app, which spread spyware via an iFrame
- The attack became worm-like when it required the victim to invite at least five friends before learning who their "crush" was

Kelly Jackson Higgins, DarkReading



Malware on IM

SECURITY CENTER: SPYWARE HORROR STORIES

Malware's IM hideaway

Published 9/28/07 by: **Eivind**

I used to use **Windows Live Messenger** a lot, talking to all of my friends. Then I suddenly get this message, "Wow! Is this you on this picture?????" from one of the girls in class. Of course, curious as I am, I clicked on the text.

Got your own spyware horror story?

Share it with us!

Then this window pops up asking, "Do you want to run "****.jpg (.exe)" from unsigned user..." I just clicked "OK" without thinking (uh-oh!), so I ended up installing some weird program, still hoping I could see if it was me in the picture. Then suddenly, McAfee went crazy, finding tons of Trojans. The last thing I saw was the virus sending "Wow is this you..." messages to all of my logged-on friends on the messenger. Then my computer went black.



Malware in Flash

Next-Generation Flash Vulnerability



July 22nd, 2009

Tags: Endpoint Protection (AntiVirus), Emerging Threats, Malicious Code, Security, Vulnerabilities & Exploits, Security Response



Recently we came into possession of an Adobe Acrobat PDF file that upon opening drops and executes a malicious binary. It was quite clear that this PDF was exploiting some vulnerability in order to drop its payload. And, during the analysis it soon became apparent that this vulnerability was not one we had seen in the wild before. What was even more surprising was that this vulnerability affects Adobe Flash—not Adobe Reader as we initially suspected.

An issue in Adobe Flash is more serious. Most vulnerabilities are confined to one technology; for example, a vulnerability may affect a particular browser or a particular operating system, but it is rare for a vulnerability to span multiple platforms and products. This is not the case with Flash. Flash exists in all popular browsers and is also available in PDF documents. It is also largely operating system independent; therefore, the threat posed by this issue is not to be taken lightly. Flash has become an integral part of the modern browsing experience—becoming so ubiquitous that most users don't even notice it.


Thomas Ptacek of Matasano Security summed up just how serious Flash vulnerabilities are: "*Why do you care about Flash exploits? Because in the field, any one of them wins a commanding majority of browser installs for an attacker.*" (The full blog post is here: [This New Vulnerability: Dowd's Inhuman Flash Exploit.](#)) The large user base of Flash presents attackers with a huge target audience and will certainly be too much for them to resist.





Malware in P2P

- One month of data from Limewire
- 68% of archives and executables contained malware

LimeWire 5.5.8

 **Download Now** (23.06MB)
Tested spyware free ⓘ

CNET editors' rating:  **Average user rating:** 
out of 10005 votes

Product Ranking: #1 in P2P & File-Sharing Software

CNET edit

Reviewed by: Seth Rosenblatt on February 12, 2009

From its start as a post-Napster clone to its leading role as the quintessential Gnutella client, LimeWire is the highest-profile P2P application. Version 5 re-envisioned LimeWire for a Web 2.0 world, with an emphasis on sharing with friends, square buttons with rounded corners, and overall a cleaner interface.

Name	Files	Responses
Trojan.VB-100	19841	774216
Worm.Alcan.D	5978	140428
Worm.VB-16	334	5329
Worm.P2P.Poom.A	372	5120
Worm.SomeFool.P	83	2196
Trojan.Downloader.Istbar-176	331	818
Worm.VB-26	190	557
Trojan.JS.Startpage.C	212	447
Worm.Wupeer.A	159	182
Worm.P2P.Selmo.A	65	66

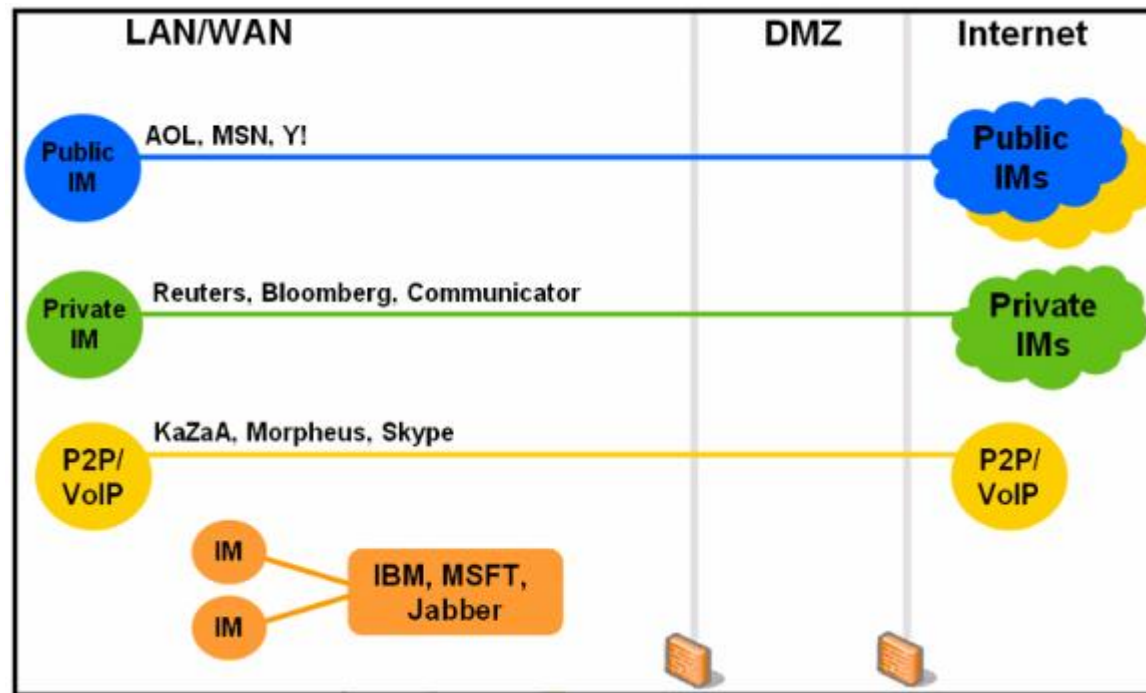
Table 2: Summary of top malware found in Limewire.

A study of malware in peer-to-peer networks
6th ACM SIGCOMM conference on Internet measurement
<http://portal.acm.org/citation.cfm?id=1177080.1177124>



Drilling Holes

- P2P on desktops and laptops connect directly to the Internet
- Designed to bypass firewalls by port crawling & tunnelling



Integrated Management and Security for IM in the Enterprise, Facetime



Web 2.0 and Beyond

Cloud Computing: Define



Cloud Categories

- **Infrastructure** (IaaS) includes storage, servers and networking components
- **Platform** (PaaS) is a set of software and product development tools for creating applications on the provider's platform over the Internet
- **Software** (SaaS) is a specific application accessed interacts with the user through a front-end portal
- **Cloud software** is off-the-shelf software that can be used to create an internal cloud or in some cases can be used to customize infrastructure services to mold a custom cloud solution

Is that right? Depends who you ask!

Infrastructure Services

Storage

- Amazon S3
- Zetta
- CTERA Portal
- Mosso Cloud Files
- Nirvanix

Cloud Brokers

- RightScale
- enStratus
- Kaavo
- Elastra
- CloudKick
- CloudSwitch

Compute

- Amazon EC2
- Serve Path GoGrid
- Elastra
- Mosso Cloud Servers
- Joyent Accelerators
- AppNexus
- Flexiscale
- ElasticHosts
- Hosting.com CloudNine
- Terremark
- GridLayer
- ITRICITY
- LayeredTech

Services Management

- Scalr
- CohesiveFT
- Ylastic
- Dynect
- CloudFoundry
- NewRelic
- Cloud42

Cloud Software

Data

- 10Gen MongoDB
- Oracle Coherence
- Gemstone Gemfire
- Apache CouchDb
- Apache HBase
- Hypertable
- TerraCotta
- Tokyo Cabinet
- Cassandra
- memcached
- Infinispan

Appliances

- PingIdentity
- Simplified
- rPath
- Vordel

Compute

- Globus Toolkit
- Xeround
- Beowulf
- Sun Grid Engine
- Hadoop
- OpenCloud
- Gigaspace
- DataSynapse
- Xeround

File Storage

- EMC Atmos
- ParaScale
- Zmamba
- CTERA

Cloud Management

- 3Tera App Logic
- OpenNebula
- Open.ControlTier
- Enomaly Enomalism
- Altor Networks
- VMware vSphere
- OnPathTech
- CohesiveFT VPN Cubed
- Hyperic
- Eucalyptus
- Reductive Lbs Puppet
- OpenQRM
- Appistry
- VMWare VCloud Express

CLOUD TAXONOMY

Platform Services

General Purpose

- Force.com
- Etelos
- LongJump
- AppJet
- Rollbase
- Bungee Labs Connect
- Google App Engine
- Engine Yard
- Caspio
- Qrimp
- MS Azure Services Platform
- Mosso Cloud Sites

Business Intelligence

- Aster DB
- Quantivo
- Cloud9 Analytics
- Blink Logic
- K2 Analytics
- LogiXML
- Oco
- Panorama
- PivotLink
- Clario Analytics
- ColdLight Neuron
- Infobright
- Vertica

Integration

- Amazon SQS
- MuleSource Mule OnDemand
- Boomi
- SnapLogic
- OpSource Connect
- Cast Iron
- Microsoft BizTalk Services
- gnip
- SnapLogic SaaS Solution Packs
- Appian Anywhere
- HubSpan
- Informatica On-Demand

Development & Testing

- Keynote Systems
- Mercury
- SOASTA
- SkyTap
- Aptana
- LoadStorm
- Collabnet
- Dynamicsoft

Database

- Google BigTable
- Amazon SimpleDB
- FathomDB
- Microsoft SDS

Software Services

Billing

- Aria Systems
- eVapt
- OpSource
- Redi2
- Zuora

Financials

- Concur
- Xero
- Workday
- Beam4d

Legal

- DirectLaw
- Advologix
- Fios
- Sertifi

Sales

- Xactly
- LucidEra
- StreetSmarts
- Success Metrics

Desktop Productivity

- Zoho
- IBM Lotus Live
- Google Apps
- HyperOffice
- Microsoft Live
- ClusterSeven

Human Resources

- Taleo
- Workday
- iCIMS

Content Management

- Clickability
- SpringCM
- CrownPoint

Backup & Recovery

- JungleDisk
- Mozy
- Zmamba Cloud Backup
- OpenRSM
- Syncplicity

CRM

- NetSuite
- Parature
- Responsys
- Rightnow
- Salesforce.com
- LiveOps
- MSDynamics
- Oracle On Demand

Document Management

- NetDocuments
- Questys
- DocLanding
- Aconex
- Xythos
- Knowledge TreeLive
- SpringCM

Collaboration

- Box.net
- DropBox

Social Networks

- Ning
- Zemby
- Amitive



Web 2.0 and Beyond

Cloud Computing (In)security



Corporate cloud use

- Your data is ... *where*?
- Which country?
- Who has access?
- Have staff been vetted?
- How well is it segregated from other users?
- Is it encrypted? Who holds the keys?
- How is it backed up (encrypted? where is it?)
- How is it transmitted (encrypted? authenticated?)
- Have the providers been tested by a reputable third party?
- Non-critical systems don't imply non-sensitive data!





Amrit Williams Blog

Observations of a Digitally Enlightened Mind

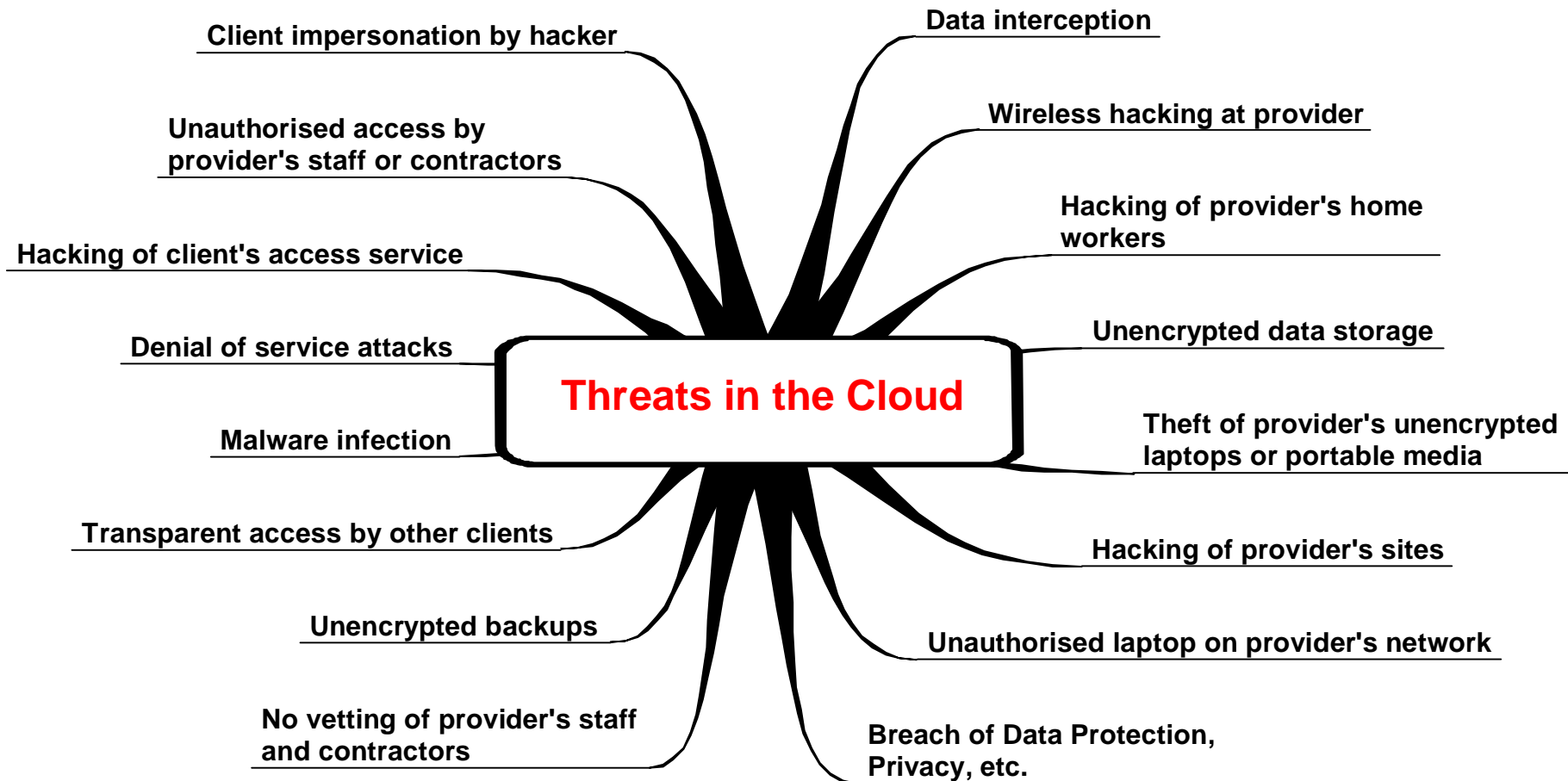
- When we allow services to be delivered by a third party, we lose all control over how they secure and maintain the health of their environments - and you simply can't enforce what you can't control.
- The 'experts' will tell you otherwise, convince you that their model is 100 per cent secure and that you have nothing to fear. Then again, those experts don't lose their jobs if you fail.

Amrit Williams is CTO at BigFix and was previously a research director in the Information Security and Risk Research Practice at Gartner, Inc.

<http://techbuddha.wordpress.com/>



Just a little brainstorm





Cloud Security Alliance

Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Reaching the point where computing functions as a utility has great potential, promising innovations we cannot yet imagine.

Customers are both excited and nervous at the prospects of Cloud Computing. They are excited by the opportunities to reduce capital costs. They are excited for a chance to divest themselves of infrastructure management, and focus on core competencies. Most of all, they are excited by the agility offered by the on-demand provisioning of computing and the ability to align information technology with business strategies and needs more readily. **However, customers are also very concerned about the risks of Cloud Computing if not properly secured, and the loss of direct control over systems for which they are nonetheless accountable.**

Top Threats to Cloud Computing V1.0, March 2010



1: Abuse and Nefarious Use of Cloud Computing

- Cloud Computing providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited
- IaaS offerings have hosted the Zeus botnet, InfoStealer trojan horses, and downloads for Microsoft Office and Adobe PDF exploits. Additionally, botnets have used IaaS servers for command and control functions. Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklisted.
- Future areas of concern include password and key cracking, DDOS, launching dynamic attack points, hosting malicious data, botnet command and control, building rainbow tables, and CAPTCHA solving farms.

Top Threats to Cloud Computing V1.0, March 2010



2: Insecure Interfaces and APIs

- While most providers strive to ensure security is well integrated into their service models, it is critical for consumers of those services to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services. Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.
- Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.



3: Malicious Insiders

- As organizations adopt cloud services, the human element takes on an even more profound importance. It is critical therefore that consumers of cloud services understand what providers are doing to detect and defend against the malicious insider threat.
- The convergence of IT services and customers under a single management domain, combined with a general lack of transparency into provider process and procedure amplifies this threat. For example, a provider may not reveal how it grants employees access to physical and virtual assets, how it monitors these employees, or how it analyzes and reports on policy compliance.



4: Shared Technology Issues

- Attacks have surfaced in recent years that target the shared technology inside Cloud Computing environments. Disk partitions, CPU caches, GPUs, and other shared elements were never designed for strong compartmentalization. As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.
- Hypervisors have exhibited flaws that have enabled guest operating systems to gain inappropriate levels of control or influence on the underlying platform.
- Joanna Rutkowska's Red and Blue Pill exploits
- Kortchinsky's CloudBurst presentations (BlackHat)



#5: Data Loss or Leakage

- The threat of data compromise increases in the cloud, due to the number of and interactions between risks and challenges which are either unique to cloud, or more dangerous because of the architectural or operational characteristics of the cloud environment
 - Insufficient authentication, authorization, and audit (AAA) controls
 - Inconsistent use of encryption and software keys
 - Operational failures
 - Persistence and remanence challenges
 - Disposal challenges
 - Risk of association
 - Jurisdiction and political issues
 - Data center reliability
 - Disaster recovery



#6: Account or Service Hijacking

- Account or service hijacking is not new. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities still achieve results. Credentials and passwords are often reused, which amplifies the impact of such attacks.
- Cloud solutions add a new threat to the landscape. If an attacker gains access to your credentials, they can eavesdrop on your activities and transactions, manipulate data, return falsified information, and redirect your clients to illegitimate sites. Your account or service instances may become a new base for the attacker. From here, they may leverage the power of your reputation to launch subsequent attacks.



#7: Unknown Risk Profile

- When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging? How are your data and related logs stored and who has access to them? What information if any will the vendor disclose in the event of a security incident?
- Often such questions are not clearly answered or are overlooked, leaving customers with an unknown risk profile that may include serious threats.



Cloud providers shrug off liability for security

Tags: [Data Breach](#), [Cloud](#), [Liability](#)

Tom Espiner ZDNet UK

Published: 12 Feb 2010 13:30 GMT



Email



Trackback



Clip Link



Print



Post a comment

Businesses signing up for standard cloud services should not expect the provider to accept liability for data breaches and other security incidents, Microsoft and others have said.

At a Cloud Law Summit in London on Wednesday, Microsoft's head of legal, Dervish Tayyip, said the company would not provide financial guarantees against data-protection issues on cloud contracts.

"We're not an insurance company," Tayyip told ZDNet UK. "What is important is that customers understand the [cloud] offerings are standardised — they are what they are. If the offering does not meet customer needs, maybe the cloud is not a realistic offering."



Web 2.0 and Beyond

What about my original scope?



Question #1

Where is your security perimeter when many endpoints are mobile handheld devices?

- Wrong question!
- Remember the value of secrets
- Identify sensitive data
- Protect sensitive data
- Monitor sensitive data
- How can your staff help?





Question #2

How do you enable good governance whilst taking advantage of the cloud?

- By following best practice!
- Remember the value of secrets
- Contracts conform to ISO 27000
- Thorough audit of suppliers
- Thorough testing of services
- Continual monitoring and tests





Question #3

What are the legal, confidentiality and availability issues in the cloud and in Web 2.0?

- The cloud is outsourcing – don't repeat your mistakes
- In Web 2.0 we cannot treat people as obstacles to security - they have to be part of the solution
- Remember the value of secrets





Question #4

What happens when your interaction with customers is immediate and intimate through Web 2.0?

- You'd better learn the new business model
- You'll need your staff to help you, not hinder
- Loyalty will be critical
- Start to think like a Digital Native





Need more information?

Peter Wood

Chief Executive Officer
First • Base Technologies LLP

peter@firstbase.co.uk

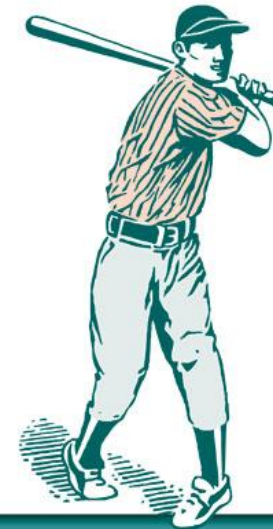
<http://firstbase.co.uk>

<http://white-hats.co.uk>

<http://peterwood.com>

<http://fpws.blogspot.com>

twitter: peterwoodx



FIRST • BASE
technologies