

# [Gadgets, tech and links by Alex Moskalyuk](#)

---

## Archive for the 'DefCon' Category

[« Previous Entries](#)

### [DefCon Chronicles: another AP article](#)

Sunday, August 6th, 2006

**Associates Press** [reports from DefCon](#):

About 6,000 computer aficionados gathered at the annual three-day event in Las Vegas, which concluded Sunday. More than 500 contestants will have competed in capture the flag and 16 other Defcon games, considered a legal talent show for hackers — a way to show corporations, consumers and government agencies how vulnerable their networks are, without the risk of criminal prosecution or financial liabilities.

Posted in [DefCon](#) | [No Comments »](#)

### [DefCon Chronicles: creating an anonymous identity](#)

Sunday, August 6th, 2006

Can you be completely anonymous? Not while browsing the Internet, we know what [Tor](#) is for, but in real life. **Johan Hybinette** discussed this topic this morning at DefCon, pointing out various loopholes here and there that would allow one to gain complete anonymity.

First off, **social security number**. There's no real way to get a fake one, except for manufacturing a fake card, but the government has a Web site, where one could verify social security numbers by last name. You have to be a US employer to gain access to the Web site. Faking one is close to impossible, since the number could be easily verified, and therefore an attacker would have to steal one. Stealing one is easier than one would think. Are you used to calling the bank and being asked for your social security number last four digits?

Last four digits couldn't be too much, could it? After all, there's 5 digits that the attacker still has to guess, and the possibilities range from 000-00 to 999-99. Not quite. The first three digits of the social security number are determined by the place that issues you the Social Security card. If you're a native American, that's the local Social Security administration at the time of birth. If you're naturalized, it's whatever office you used to get your original SSN.



What follows is the group #. The group # is those two digits following the SSN office number, and the information is available from Social Security Administration. Basically, the numbers range 00 to 99, and Social Security Administration is publishing a bulletin where it says, which group number it's on right now. If you can estimate the victim's age, you almost have the group number figured out, or at least guessed within a very close proximity. Get someone with access to SSA social security number verification site, and you can easily run a check of your best bets.

After that comes **the passport**. It's extremely hard to gain a valid US passport, unless you're an American, and therefore few people attempt it. However, if an attacker steals the identity of a valid SSN holder, getting a

passport becomes a bit easier. Therefore, if you're an American and you don't have a passport, **get it**. Even if you don't plan to travel, there's a possibility that someone might abuse your identity just to get a passport. Beyond US passports, there's a possibility of getting some other countries into helping you to create your fake identity.

Are you Jewish? Apply for Israeli citizenship. Are you Irish? You can apply for Irish citizenship and get a perfectly valid passport from Ireland? Have tons of cash? Argentina, Bahamas and some other country would be happy to issue you a passport of their own that they revoke frequently? Have some money but not a lot, and don't intend to travel? Get a passport of Soviet Union, British Honduras, or another country that doesn't exist anymore. Those passports are not good for travel, since the personnel is trained to spot them, but you can get a perfectly good bank account with those.

**US birth certificates** - hard to obtain, hard to use. Most of the attackers don't try them. Some states, however, will renew a birth certificate if you claim it lost and provide a valid social security card and a driver's license.

So what about **driver's license**? Those are reasonably easy to get if you're within the United States and don't have any qualms about visiting your local DMV. However, after standing in line, being yelled at, and being exposed to people with pretty bad body odour condition, you can only get a license for yourself, so what's the point of doing that?

There're are always [novelty driving license sites](#), if you do not intend to ever use the driving license in front of the government official such as cop, who can check the numbers against the database, those will work. However, frequently attackers would go against terminally ill or very old people, offering them some cash for turning over all the personal details (driver's license, SSN, passport #, certificate of birth) and paying them not to submit the certificate of death. When the person goes away, living the very last days off attacker's generous financial donation, an entire identity is up for grabs and becomes an extremely hot black market commodity.



**Fake Id Sites**

Hybinette's talk was both informative and disturbing, and some loopholes in the US legislature, such as the possibility of coming back to the country on an Irish passport (which is extremely easy to get as long as one of your ancestors can claim a drop of Irish blood) will be shut down.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: Suru - man in the middle proxy](#)

Sunday, August 6th, 2006

**SensePost** presented [Suru](#), a man in the middle proxy for testing Web applications for potential vulnerabilities. It allows you to sit in the middle of HTTP GET and POST request, modify the requests with regular expressions (to insert some single quotes, perhaps) as well as attach a [fuzzing](#) tool to the Web service requests. It also does some reconnaissance as you browse the site:

As you browse Suru automatically detects when a new directory is used (e.g. when the user surfed to `http://abc_corp/abc/` the directory `/abc/` is automatically searched). This means that, as the analyst is surfing the application Suru will learn more and more about the application and perform more in-depth discovery of the site.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: disrupting companies with Yahoo! Finance message boards](#)

Sunday, August 6th, 2006

[Broward Horne](#) is telling a story of disrupting [SalesLogix](#) back in the days of the dot-com boom by posting some pretty good satire on Yahoo! Finance message boards for SalesLogix. The talk is titled *Meme Hacking – Subverting The Ideosphere* and talks about propagating information and manipulating opinions on the Internet. Not a whole lot of technical tips, mostly psychological.

Posted in [Yahoo!](#), [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: fuzzing](#)

Sunday, August 6th, 2006

[Fuzzing](#) seems to be the word of the day at [DefCon](#). It's a technique of evaluating the application by attaching a source of random data to it. The Wikipedia link points to the paper [Fuzz Testing of Application Reliability](#). Want to do some fuzz testing? Just point a generator of random data at your application's input.

Posted in [DefCon](#) | [1 Comment »](#)

## [DefCon Chronicles: a day in the life of a botnet](#)

Sunday, August 6th, 2006

**Rick Wesson** of [Support Intelligence, LLC](#) conducted extensive research of existing botnets. He spends his days looking up active botnets on the Web and penetrating those for research. Occasionally he would call the victims to tell them their identities have been compromised, and people would get mad, and he'd find himself on the receiving end of threats and frustrations, when he told the person their social security number and credit card information.

Chevron is one of the companies mentioned. Chevron's corp network was compromised to send out large amounts of spam. Indeed, why would you bother with pesky home desktops, if you can compromise a large corp network hooked up to a T1.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: why DefCon is unique](#)

Sunday, August 6th, 2006

DefCon is probably the only conference where

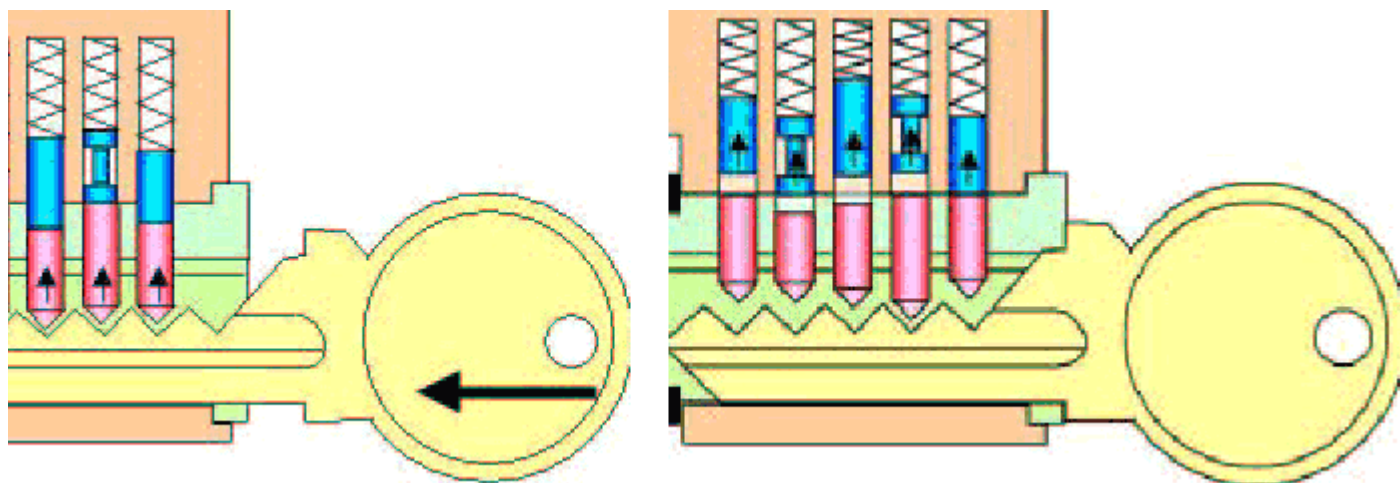
1. the organizers keep reporting on dealing with hotel management, and whether or not the conference will be kicked out (fyi, Riviera is quite happy with DefCon attendees so far)
2. the early 10 am speaker brings helpings of beer to his talk just to help people who are hungover

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: open any lock under 5 seconds](#)

Saturday, August 5th, 2006

**Marc Weber Tobias** and **Matt Fiddler** are talking about bump-opening most of the locks out there in the United States. The full paper [is available at security.org](#). They also conducted a research with USPS and Mailboxes, etc. While USPS quickly worked with the researchers and agreed that the issue was there, MailBoxes, etc. keeps denying there's a problem. A PDF with detailed technical analysis [is also available](#). The presentation promised:



Case examples and demonstrations detailing a major security flaw and vulnerability in locks used by the federal government and a private sector corporation that affect millions of users will be presented.

and it certainly delivered that. Live in an apartment complex? you can make a **bump key** out of your key that will open any apartment. Rent a mail box? Gain access to anything that uses the same type of key. And if you're bothered too much with creating your own bump keys, just [buy some off eBay](#).

Posted in [DefCon](#) | [1 Comment »](#)

## [DefCon Chronicles: hacking retail kiosks](#)

Saturday, August 5th, 2006

**Peleus Uhley** of [@Stake](#), and therefore, of Symantec, talked a little bit about [kiosk security](#) and the ways to hack the retail kiosks. For the kiosks that are Windows-based and are running Internet Explorer connecting to custom sites it's amazing how many shortcuts there are to open up various dialog boxes that allow you to navigate somewhere else on the Net. There's also the Print dialog that allows the user to select printing to file, and then navigating to the Network shares dialog box, which is really nifty for exploring the retailer's network.

[PublicWebStations](#) is one of the site pointed out in presentation, an open Linux-based kiosk environment.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: untraceable voice communication channels](#)

Saturday, August 5th, 2006

**Michael Hampton** [reports from the first talk at DefCon on Saturday](#) on [mysterious phone stations](#):

The presentation detailed how third parties could be used unwittingly to create a virtually untraceable communications channel between two parties in order to foil traffic analysis attempts by hostile intelligence agencies. It seems to have worked.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: plausible deniability toolkit](#)

Saturday, August 5th, 2006

[Plausible Deniability ToolKit](#) “is not a set of tools to download, but a set of ideas and philosophies to adapt to protect your privacy in an ever-increasingly scary world of eroding personal rights”.

It was introduced at DefCon by hackers, who were advising others on dealing with potential prosecution. The plausible deniability toolkit provides the tools for managing your PC in a plausible manner, so that when you claim later on in court that you **always** delete your work files, it's true; and it's not a one-time action you took after being indicted.

The authors recommend you visit the page only with [Tor](#) enabled, as the visit might be used later on as the evidence against you. The slides are available [here](#).

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: some stuff you can get](#)

Saturday, August 5th, 2006

Some neat stuff you can get in the vendor row.



Posted in [DefCon](#) | [2 Comments »](#)

## [DefCon Chronicles: wall of shame](#)

Saturday, August 5th, 2006

DefCon Wall of Sheep presents a real time view of usernames and passwords sent in the clear over DefCon WiFi in Riviera Hotel. The conference booklet warns about using any password-protected sites that ask for the password in the clear, and the Wall of Sheep just accentuates that warning. They do mask the second half of the password, though, to protect the innocent.



Dan's research. The banks that display a login-password module in plain on every page are the worst. The banks that ask for username in plain and then redirecting to SSLed page for the password entry are wising up.

[Kaminsky](#)'s advice? As soon as user starts typing in the username for login, generate an IFRAME with HTTPS page loading in it. That SSLed page should ask for the password, not the plain text HTTP one.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: faking 802.11 frames](#)

Saturday, August 5th, 2006

**Damon McCoy** and **Anmol Sheth** wrote [Zulu](#), "a light weight 802.11 wireless frame generation tool to enable fast and easy debugging and probing of 802.11 networks". It's available for download [here](#).

The logo for Zulu, featuring the word "ZULU" in a stylized, multi-colored font. The letters are blue and purple, with a gradient effect.

The tool has numerous application beyond malicious, such as testing wireless device drivers. 20+ command line options, works on Linux. Good defaults, doesn't require you to memorize the command line syntax before you start using it.

Posted in [DefCon](#) | [2 Comments »](#)

## [DefCon Chronicles: MatriXay DB security scanner](#)

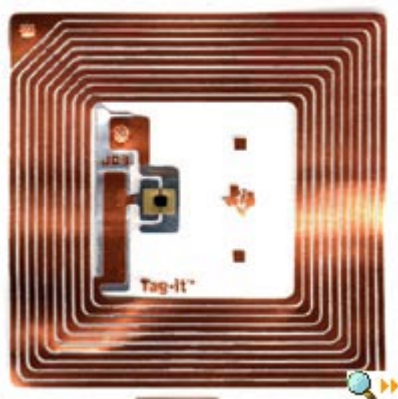
Saturday, August 5th, 2006

**DB AppSecurity** announced [MatriXay](#), a nifty tool for SQL injection attacks on existing Web databases that also runs through default passwords trying to break into the backend DB. Support for MSSQL, Access, MySQL, Oracle, DB2, Sybase, bruteforce password generation (if you have the CPU cycles).

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: RFID spoofing](#)

Friday, August 4th, 2006



**Melanie Rieback** (whose academic advisor is Andrew Tanenbaum, yeah, [that Andrew Tanenbaum](#)) presented *A Hacker's Guide to RFID Spoofing and Jamming*. Looking through her work, there's also an interesting paper [Is your car infected with a computer virus?](#)

She mentioned RFID tracking of products, boxes, animals and even humans with [the VeriChip product](#), which is apparently advocated by some exclusive clubs out there (no more standing in VIP line). A quote by Applied Digital CEO, where the company says they're not putting encryption into their RFID tags, since it could only be read by proprietary scanners generated a few laughs.

While the tags themselves are pretty simplistic, there's a potential for abuse. Reading somebody else's tags, replicating and manipulating them, generating false positives, running equipment to capture valid RFID tags and to generate the corresponding fake ones (perfect man in the middle attack).

[RFID Guardian](#) is the project Melanie's working on, and the video is available at the bottom of the page.

Why doesn't RFID standard support basic authentication mechanism between the RFID tag and the reader? The standard went into the market, and if the companies agreed to add the authentication bits to it, that would mean

making the entire product lines obsolete.

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: database of intentions revisited](#)

Friday, August 4th, 2006

I see that the press picked up on the presentation by **Greg Conti**, a computer science professor at the United States Military Academy. The basic premise was collecting the Internet cache data, showing it to the user, and then asking the user to filter out the information that should not be shared with the public. Most people will filter out personal information, personal locations, SSNs or credit card numbers. Greg Conti showed that normally it's anywhere between 10% and 31% that we ourselves decide we wouldn't like to share.

Now let's remember that search engines out there get **all** that information, and a portal with wide variety of services (he used an example of Google, but I guess one could come up with numerous other ones) would contain even more information, such as friends' e-mail addresses, phone numbers, and interesting places we look up on the map.

Overall, the presentation didn't strike me as anything special (maybe I spent too much time inside the Internet industry). It's the same argument we've heard before, and solution usually is that if you're paranoid, try to disclose as little information about yourself as possible. It also rings a bell, if you recall **John Battelle's** [Database of intentions](#):

The Database of Intentions is simply this: The aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result. It lives in many places, but three or four places in particular hold a massive amount of this data (ie MSN, Google, and Yahoo). This information represents, in aggregate form, a place holder for the intentions of humankind - a massive database of desires, needs, wants, and likes that can be discovered, subpoenaed, archived, tracked, and exploited to all sorts of ends. Such a beast has never before existed in the history of culture, but is almost guaranteed to grow exponentially from this day forward. This artifact can tell us extraordinary things about who we are and what we want as a culture. And it has the potential to be abused in equally extraordinary fashion.

Now [to quote Conti's presentation](#):

"I was shocked, and I think other people will be shocked, to learn the information they've been handing over," Conti said in an interview ahead of his presentation. "What we're doing is implicitly trusting a handful of companies with a tremendous amount of our personal information."

Posted in [DefCon](#) | [No Comments »](#)

## [DefCon Chronicles: it's all about the forensics](#)

Friday, August 4th, 2006



Two forensics-related presentations were excellent: informative, humorous and engaging. First, **Johnny Long** amused the audience with the tales from the forensics world, displaying probably hundreds of various devices containing USB in them. Watches, ducks, fake sushu, iPod Shuffle, you name it - everything had a USB port in it and therefore should be picked up from the crime scene as evidence.

Then **Amber Schroader** and **Tyler Cohen** in the next presentation went through Johnny's "personal" items, trying to draw a verdict on his criminal



activities. They showcased a variety of nifty tools from [Paraben](#), which allows an investigator to go knee-deep into people's mobile devices in order to fetch the useful data. The tool also automatically tries to recognize common file types and match those against common signatures, so saving critical information into an **.mp3** file just hoping that it will be ignored by the investigator won't work anymore.

It's iPods everywhere, in both presentations, and for a moment you think you're at MacWorld, but the reason is simple - USB-powered devices with large storage are capable of storing much more than someone's Britney Spears tunes. First off, you can run things like [Damn Small Linux](#) directly off an iPod, and second, the device ignores everything that's not music, which makes it pretty useful to carry around with your own library of files that you just never know you might need, like [Metasploit Framework](#).



Another bit of information that I guess everybody is familiar with - encrypted AAC files purchased from Apple iTunes contain the buyer's e-mail address in the clear. It's also the e-mail address associated with the credit card, which might not be your .Mac e-mail address.

Posted in [Gadgets](#), [DefCon](#) | [1 Comment](#) »

## [DefCon Chronicles: recovering your hard drive](#)

Friday, August 4th, 2006

**Scott Moulton** of [Forensic Strategy Services, LLC](#) just got finished with a great presentation on hard drive recovery. Scott runs [the forensics company](#) that has to deal with dead or malfunctioning hard drives a lot, and he had a lot of information on the inner working of hard drive, how new perpendicular hard drives would be pretty easy to recover. He named about a dozen of reasons why hard drives die, and his presentation gave an appreciation for the job of data recovery, and what complexity is involved with it.

For a lot of the hard drives with failing electronics or mechanical parts, the exact same parts need to be purchased and replaced, and therefore Scott is a frequenter of eBay, where he can find all sorts of obscure components and complete replicas of the hard drive models he needs.



The presentation is [available online in Flash format](#).

Posted in [DefCon](#) | [No Comments](#) »

[« Previous Entries](#)

### • **Search:**

## • Categories

- [BitTorrent clients](#) (8)
- [DefCon](#) (25)
- [DIY](#) (5)
- [Entertainment](#) (146)
- [Gadgets](#) (75)
- [General](#) (87)
- [Health](#) (7)
- [Immortality](#) (5)
- [Internet scams](#) (18)
- [LabView for dummies](#) (1)
- [LLC](#) (4)
- [Money](#) (132)
- [Netflix](#) (12)
- [New software releases](#) (48)
- [News](#) (92)
- [Programming](#) (133)
- [Review](#) (25)
- [Robots](#) (1)
- [San Diego](#) (2)
- [Science](#) (12)
- [Silicon Valley](#) (37)
- [Startups](#) (52)
- [Technology](#) (394)
- [Wireless](#) (28)
- [WordPress](#) (15)
- [Yahoo!](#) (38)

## • Recommendations

- [Sonic.net DSL](#) - starting at \$15 a month, great Silicon Valley based support by people who speak English
- [Read my reviews on Judy's Book](#) - mostly restaurants in Mountain View, Palo Alto, Sunnyvale and other Bay Area places.



Subscribe



XML





### Bookmark This Site

[+Del.icio.us](#)

[+Furl It](#)

[+Spurl](#)

[+Tag!RawSugar](#)

[+Simpy This!](#)

[+Shadows Tag!](#)

[+Blink It](#)

[+My Web](#)

[Create Feed Buttons](#)

## • Daily reading

- [Daily Rotation](#)
- [EnGadget](#)
- [ExtremeTech](#)
- [Gizmodo](#)
- [IT Facts](#)
- [MetaFilter](#)
- [Microsoft Blogs](#)
- [NYT Technology](#)
- [Slashdot](#)
- [TechDirt](#)

## • Financial sites

- [All My Rebates](#)
- [Best Cash Cow](#)
- [FreeMoneyFinance](#)
- [GuruFocus](#)
- [Options trading](#)
- [Small business trends](#)
- [What you owe in taxes](#)

## • Interesting sites

- [Free flash games](#)
- [SD Forum Event Calendar](#)

- [ShaveBlog](#)
- [The Stalwart](#)
- [WorkHappy](#)
- [Yoga for Geeks](#)

## • Itroneers

- [Pavel Popov](#)
- [Amit Sharma](#)
- [LinuxPunks](#)

## • Journalist blogs

- [Business 2.0 blog](#)
- [DealFlow @ BusinessWeek](#)
- [Fast Company blog](#)
- [Missing links @ CNET](#)
- [PC World TechLog](#)
- [ZDNet blogs](#)

## • Links

- [Collector Car Buff](#)
- [LiveJournal friends aggregator](#)
- [That was funny](#)
- [WordPress](#)

## • People

- [Joel Spolsky](#)
- [John Battelle](#)
- [Om Malik](#)
- [Sergey Petrenko](#)
- [Mark Cuban](#)
- [Dave Viner](#)
- [Sanaz Ahari](#)
- [Ivan Grynov](#)
- [Carson McComas](#)
- [David Churback](#)
- [Jeffrey Friedl](#)
- [Richard McManus](#)
- [Matt Cutts](#)
- [Niall Kennedy](#)
- [Michael Parekh](#)
- [Henry Blodget](#)
- [Scott Adams](#)
- [Suprcilious](#)
- [Ethan Stock](#)
- [Ken Norton](#)
- [Jim Forbes](#)
- [Jibbering](#)

- [Guy Kawasaki](#)
- [Simon Willison](#)
- [Jeff Barr](#)
- [Bob Walsh](#)
- [Nitin Borwankar](#)
- [Joseph A. di Paolantonio](#)
- [Matt Ingot](#)

## • Programming

- [Pagerank calculator](#)
- [AJAX Tutorials](#)
- [Ruby on Rails tutorials](#)
- [JavaScript tutorials](#)
- [XUL tutorials](#)
- [SitePoint](#)

## • Science news

- [Berkeley](#)
- [MIT](#)
- [PSU Live](#)
- [Science blogs](#)
- [Science Magazine](#)
- [Seed magazine](#)
- [Stanford](#)
- [UCLA](#)
- [UCSF](#)

## • Technology sites

- [ACM Daily News](#)
- [Everything Ajax](#)
- [Everything Firebird](#)
- [Fast Company](#)
- [Hot deals portal](#)
- [Interview questions](#)
- [Nokia 770](#)
- [PlayStation Portable Blog](#)
- [PopGamers](#)
- [Smalley's Research Watch](#)
- [Under the Radar](#)
- [Wall Street Programmer](#)

## • Top referrers

- [google.com](#)
- [it.slashdot.org](#)
- [Plasma HDTV prices](#)
- [search.yahoo.com](#)

## • Ukrainian media

- [ITC](#)
- [Korrespondent](#)
- [UkrPravda](#)

## • Venture capital

- [AVC](#)
- [Bill Burnham](#)
- [Press releases from startups](#)
- [Startup Blog](#)
- [Topix.net startups](#)
- [Venture capital news](#)
- [Venture capital statistics](#)
- [VentureBlog](#)

## • Yahoo!s

- [Jeff Boulter](#)
- [Jeremy Zawodny](#)
- [Chad Dickerson](#)
- [Jeffrey McManus](#)
- [Scott Gatz](#)
- [Andrew Wooldridge](#)
- [Ted Drake](#)
- [JR Conlin](#)
- [Glen Campbell](#)
- [Chris Cowan](#)
- [Amr Awadallah](#)
- [Dave Beckett](#)
- [Bradley Horowitz](#)
- [Ben Margolin](#)

## • Archives

- [DefCon Chronicles: another AP article](#)
- [DefCon Chronicles: creating an anonymous identity](#)
- [DefCon Chronicles: Suru - man in the middle proxy](#)
- [DefCon Chronicles: disrupting companies with Yahoo! Finance message boards](#)
- [Microsoft freebies](#)
- [Las Vegas monorail](#)
- [DefCon Chronicles: fuzzing](#)
- [DefCon Chronicles: a day in the life of a botnet](#)
- [DefCon Chronicles: why DefCon is unique](#)
- [DefCon Chronicles: open any lock under 5 seconds](#)
- [DefCon Chronicles: hacking retail kiosks](#)
- [DefCon Chronicles: untraceable voice communication channels](#)
- [DefCon Chronicles: plausible deniability toolkit](#)
- [DefCon Chronicles: some stuff you can get](#)
- [DefCon Chronicles: wall of shame](#)

- [DefCon Chronicles: Black Ops 2006](#)
- [DefCon Chronicles: faking 802.11 frames](#)
- [DefCon Chronicles: MatriXay DB security scanner](#)
- [DefCon Chronicles: RFID spoofing](#)
- [DefCon Chronicles: database of intentions revisited](#)
- **[My Web 2.0 Links](#)**
  - **[Gadgets, tech and links â Edit Comments â WordPress](#)**  
Tags: [null](#)
  - **[My Yahoo! - Blogs](#)**  
Tags: [null](#)
  - **[Self-medicating Online - World of Psychology](#)**  
Tags: [brain](#), [medicine](#), [mind](#), ..
  - **[Mind Hacks: Mind-reading competition](#)**  
Don't worry, this isn't about telepathy and doesn't...  
Tags: [mind reading](#), [psychology](#), [reading](#)
  - **[Future Boy: This is your brain on Google - Jul. 21, 2006](#)**  
Brain-reading technology is improving rapidly. Last year, So...  
Tags: [brain](#), [science](#)
  - **[Why fast-spinning young stars don't fly apart](#)**  
Young stars are loaded with energy, and they can spin around...  
Tags: [science](#), [space](#)
  - **[Wiki start-up taps open source to lure new users | CNET News...](#)**  
MindTouch, founded by former Microsoft employees, on Tuesday...  
Tags: [startup](#), [wiki](#)
  - **[Emerging Giants](#)**  
Many more companies are using their bases in the developing ...  
Tags: [economics](#), [globalization](#)
  - **[Market grows by 4.3%: CommsUpdate : TeleGeography Research](#)**  
Tags: [italy](#), [itfacts](#), [telecom](#)
  - **[Gyongyi, Zoltan; Garcia-Molina, Hector; Pedersen, Jan: Web C...](#)**  
Document categorization is one of the foundational problems ...  
Tags: [categorization](#), [computer science](#), [database](#)
  - **[Science & Technology at Scientific American.com: The Geo...](#)**  
If there is a mathematician eagerly waiting for the Large Ha...  
Tags: [geometry](#), [science](#)
  - **[Science & Technology at Scientific American.com: The Fis...](#)**  
Few wildlife spectacles in North America compare to the sigh...  
Tags: [forest](#), [river](#), [science](#)
  - **[Science & Technology at Scientific American.com: The Exp...](#)**  
Tags: [expert](#), [mind](#), [sciam](#), ..
  - **[Ask the Experts: Environment: If carbon dioxide makes up suc...](#)**  
The Earth's surface absorbs visible radiation from the sun, ...  
Tags: [science](#)
  - **[Transcript - Transcript of interview with Werner Vogels, CTO...](#)**  
When you talk about service-oriented architecture, a lot of ...  
Tags: [amazon](#), [servers](#), [service-oriented](#), ..
  - **[Technology Review: Emerging Technologies and their Impact](#)**  
Tags: [online](#), [storage](#)
  - **[Index of /ebookz/Teach Yourself series](#)**  
Tags: [books](#), [ebooks](#), [programming](#)
  - **[O'Reilly Radar > Levels of the Game: The Hierarchy o...](#)**  
Tags: [application](#), [desktop application](#), [hierarchy](#), ..
  - **[MyWeb2 Bookmarklets](#)**  
Tags: [null](#)

- [tagschema](#)  
database tech for tag-based apps  
Tags: [database](#), [programming](#), [schema](#), ..

Powered by [Yahoo! Search](#)

## • Saved stuff

- [Coffee table for sale](#)
- [Compound interest calculator](#)
- [Cool Firefox extensions](#)
- [Credit card payment schedule](#)
- [CVS commands](#)
- [Digital cameras under \\$500](#)
- [grep tutorial](#)
- [How to remove cigarette smell from the apartment](#)
- [Magazines](#)
- [Plasma and LCD TV prices](#)
- [Regular expression helpers](#)
- [Romantic dinners in SF Bay Area](#)
- [Web Services with PHP](#)