* [IEEE.org](http://www.ieee.org" \t "_blank)
* |
* [IEEE](http://ieeexplore.ieee.org" \t "_blank) *[Xplore](http://ieeexplore.ieee.org" \t "_blank)* [Digital Library](http://ieeexplore.ieee.org" \t "_blank)
* |
* [IEEE Standards](http://standards.ieee.org" \t "_blank)
* |
* [IEEE Spectrum](http://spectrum.ieee.org/)
* |
* [More Sites](http://www.ieee.org/sitemap" \t "_blank)

[EEE Spectrum logo](http://spectrum.ieee.org/)

Follow on:

* [Engineering Topics](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [Special Reports](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [Blogs](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [Multimedia](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [The Magazine](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [Professional Resources](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* [Search](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* **Sections**
  + [Cover Story](http://spectrum.ieee.org/magazine)
  + [Departments](http://spectrum.ieee.org/magazine)
  + [Features](http://spectrum.ieee.org/magazine)
  + [News](http://spectrum.ieee.org/magazine)
  + [Opinion](http://spectrum.ieee.org/magazine)
  + [View The Issue](http://spectrum.ieee.org/magazine)
  + [Browse Archives](http://spectrum.ieee.org/magazine/archive)

[Subscribe](http://spectrum.ieee.org/static/readerservices)

* + **September 2014**

[](http://spectrum.ieee.org/magazine)

* + **Cover Story**

**[How to Catch Brain Waves in a Net](http://spectrum.ieee.org/biomedical/bionics/how-to-catch-brain-waves-in-a-net)**

[A mesh of electrodes draped over the cortex could be the future of brain-machine interfaces  
21 Aug](http://spectrum.ieee.org/biomedical/bionics/how-to-catch-brain-waves-in-a-net)

* Feature
* [Computing](http://spectrum.ieee.org/computing)
* [Software](http://spectrum.ieee.org/computing/software)

**Fresh Phish**

**How a recently discovered flaw in the Internet's Domain Name System makes it easy for scammers to lure you to fake Web sites**

By David Schneider

Posted 1 Oct 2008 | 4:00 GMT

* [Share](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* |
* [Email](http://spectrum.ieee.org/computing/software/fresh-phish/0" \o "Email" \t "_blank)
* |
* [Print](http://spectrum.ieee.org/computing/software/fresh-phish/0)

**When you direct** your browser to www.google.com, you take it for granted that the Web page that appears will indeed come from Google and not from some shadowy Internet scammer pretending to be Google. But your faith is misplaced. It turns out to be easy for a malicious computer hacker to trick your browser into steering you anywhere he wants and then to pilfer sensitive information, like your user name, password, and credit card number.

Dan Kaminsky, of the Seattle-based computer-security firm IOActive, stumbled onto the problem in February while examining the functioning of the Domain Name System, or DNS, the database that computers use to find their way around the Internet. At the time, it was still just a theoretical vulnerability; he had not actually observed anyone taking advantage of it. But he knew that clever criminals would eventually uncover the flaw, at which point all kinds of damage could be done. ”I realized the scope of this pretty quickly,” he recalls.

He then alerted other security experts and the makers of network equipment and worked with them behind the scenes to get software patches written. The various vendors released their new code in a coordinated move on 8 July. At that point the existence of the threat became common knowledge, at least among computer types, but the details of how the flaw could be exploited were still shrouded in mystery. To give network administrators time to install the new software, Kaminsky had planned to wait 30 days before publicly describing the vulnerability. But things soon spiraled out of his control.

By looking at the patch, others guessed what Kaminsky had found, and soon some had posted their ideas on the Internet. The cat slipped fully out of the bag when a blogger at the computer-security firm Matasano Security confirmed some of these speculations. The blog post was taken down quickly, but not quickly enough to prevent it from being copied and widely disseminated.

Within days, code to exploit the newfound weakness in the DNS had been posted on the Web site of the ”computer academic underground” (<http://www.caughq.org>)--precisely the kind of thing Kaminsky had hoped to forestall.

Whereas some network administrators may initially have been reluctant to patch their systems, fearing that the upgrade itself might cause problems, most of them now seem to have made the change. No definitive tally is available, but Kaminsky has created a tool on his personal Web site (<http://www.doxpara.com>) that allows visitors to check whether the server they are using has been patched. He reports that as of 9 July, about 85 percent of the name servers being tested were vulnerable. But by 6 August, the proportion had dropped to 30 percent.

But even those who have taken the appropriate steps are not exactly breathing easy. The patch is not a perfect countermeasure, as Kaminsky has emphasized on his blog: ”This is just a stopgap--we're still in trouble with DNS, just less.”

**If you follow** computing at all, you know that security experts routinely uncover software glitches and vulnerabilities and then issue software patches and upgrades. What Kaminsky has found, however, is much bigger and much scarier.

To understand why, you need to know the basics of how the DNS works. The Domain Name System is essentially the Internet's phone book. It's a huge database containing the 32â¿¿bit numeric codes that identify every single site on the Internet. These are known as Internet Protocol addresses, or IP addresses for short. Amazingly, this database is distributed over some 12 million computers worldwide, known as DNS name servers.

When you type ”www.google.com” into your browser, it must translate that human-readable text into an IP address before it can access the site. To do so, your computer sends a request to a name server upstream, probably one maintained by your Internet service provider.

Then, if your ISP's name server has the IP address for the requested site stored--or ”cached”--it returns this information to your computer pronto. If not, it goes through what may be an elaborate process querying other name servers to find the address.

Kaminsky has discovered a way for a hacker to insert a false IP address into the cache of a name server. The hacker could, for example, change the name server's entry for ”www.paypal.com,” thus blocking access to PayPal, or worse, duping people into going to a site that mimics PayPal's. From there, it would be relatively simple to harvest user names, passwords, and other valuable data.

Such an attack would work much like the many ”phishing” scams now plaguing the Internet, but in this case the victims wouldn't need to click on a link in a shady e-mail message. They could type the correct name, ”www.paypal.com,” directly into a browser and still get sent to the wrong place. (The real PayPal would upgrade the security of the connection from http to https, but the victim may easily fail to notice when this doesn't happen on the scammer's simulated site.)

The attacker could also use this tactic to redirect e-mail. By replacing the IP address of, say, a corporate mail server with the IP address of a mail server that he controlled, he could inspect incoming correspondence before passing it on to the targeted company's mail server. Even more troubling, he could add his own malicious code to e-mail attachments, which from the recipient's point of view might appear to come from known and trusted sources.

Security experts had long been aware of two general ways that a hacker could carry out such a ”cache poisoning” attack on a name server. But both had been rendered ineffective years ago with changes to DNS software. Kaminsky, however, has found a way for a hacker to circumvent these fixes--and to combine the two exploits in a way that makes an attack especially potent.

**The first kind** of [attack](http://spectrum.ieee.org/images/oct08/images/phish02.pdf)causes the targeted name server to query a second name server, one that the bad guy controls. That turns out to be incredibly easy to do, even if the name server to be poisoned is behind a corporate firewall or otherwise protected from outside access.

Suppose this hypothetical villain creates a Web page that contains a description of Mother Teresa--perhaps an eBay ad for a copy of her definitive biography. Unbeknownst to you, the page includes an embedded image that is hosted on a machine in the hacker's evil domain, BadGuysAreUs.com. So when you access that eBay page seeking to purchase a book about Mother Teresa, your browser sends out a DNS query to look up the IP address of BadGuysAreUs.com.

Assuming the hacker doesn't try this too often, the address won't be in your name server's cache, so it will issue a series of queries to other name servers. Eventually, your name server will be referred to the bad guy's name server, which responds by supplying the requested IP address. Now here's where it gets ugly: the Domain Name System allows the answer to include additional information. The bad guy's name server could thus be programmed to send a false IP address for any other site--such as Citibank (<http://www.citibank.com>)--along with the requested IP address. The fake address would then take the place of the bank's real IP address in your name server's cache, where it would act to redirect traffic from anyone trying to use that server to reach www.citibank.com.

The ability to tack on additional information in a DNS response was considered a valuable feature when the Internet was first set up--it was designed to provide the IP addresses of name servers referenced in the main part of the response. At that time, which predates the Web by many years, nobody thought much about the possibility of scammers using this mechanism to take advantage of folks purchasing things through an Internet auction or doing their banking online.

To counter such mischief, DNS software was changed about a decade ago to do what is called bailiwick checking. With that, any extra information added to a DNS response is ignored if it pertains to a domain that is different from the one that was asked about in the first place. So your name server would disregard an IP address said to be for www.citibank.com if the original query was about BadGuysAreUs.com.

The second way an attacker can poison a name server's cache relies on the fact that the conversation your computer has with the name server upstream--or the conversation between two name servers involved in answering your query--is fundamentally insecure. One computer sends out a request to another and then waits for an answer from it. But the answer could, in fact, come from any machine, anywhere.

Well, almost--a few systems work differently. Anyone accessing sites in Sweden's .se domain, for example, can use a secure extension to DNS called DNSSEC (for Domain Name System Security Extensions) to carry out DNS lookups. But DNSSEC hasn't really caught on, in part because it is cumbersome for name-server administrators to manage. That attitude now seems due for an adjustment. ”There certainly was a spike in interest in DNSSEC” after Kaminsky made his discovery known, says Cricket Liu, a DNS expert at Infoblox, a Santa Clara, Calif., provider of DNS hardware and software.

Still, most communication between name servers continues to take place over an insecure channel. The receiver does check the origin of an answer using a numeric tag attached to the request. But this query ID number wasn't designed with security in mind; it was intended originally just to match up outgoing requests with incoming answers. Early on, DNS software assigned those numbers sequentially, which made it easy for an attacker to guess them. Since about 1997, DNS software has been configured to assign those ID numbers randomly to make such attacks harder. But the ID number has only 16 bits, which translates to 65 536 possible values--few enough to give an attacker a reasonable chance of guessing right if he can try thousands of times.

And that, it turns out, is easy. All a hacker needs to do is send a request to the name server asking it to look up an IP address it doesn't have cached. Then he immediately bombards the server with answers, each containing a different query ID number. Many of the fake replies will beat the real answer back to the name server seeking the address. One of them, the attacker hopes, will contain the correct query ID. More sophisticated versions of this second type of attack don't have such long odds: one scheme, for example, takes advantage of the fact that nominally ”random” query IDs can to some extent be predicted.

Up until now, guess-the-query-ID attacks hadn't been considered much of a menace, because the hacker would very likely fail on the first attempt, and the name server would then store the correct IP address in its cache, typically for a day or so. Thus, if the first such attack failed, the hacker would have to wait a day or more to try again. If he had to attempt this hundreds of times before achieving success, it could take years to poison the name server's cache.

Kaminsky's insight reveals [how an attacker could sidestep that problem](http://spectrum.ieee.org/images/oct08/images/phish03.pdf). Imagine that a hacker asked your ISP's name server to look up a nonexistent address within the paypal.com domain--for instance, aaa.paypal.com. This nonsensical name would, of course, not be cached in your ISP's name server, so it would pass the request up the line, eventually asking the real PayPal's name server for the corresponding IP address. While all that was going on, the attacker would send your ISP's name server a lot of spoofed answers with different ID numbers.

Because the hacker has a head start in the race, many of his simulated DNS responses will beat the real one back to your name server. If, for example, 100 fake answers arrive before the real one, the attacker's chances of having one of his bogus responses accepted improve, from 1 in 65 536 to a more worrisome 1 in 655. Even if all 100 spoofed answers fail to get the ID number right, there's nothing preventing him from repeating this attack as many times as he wants, asking about different nonexistent addresses each time: aab.paypal.com, aac.paypal.com, and so forth. Eventually--typically in about 10 seconds by Kaminsky's estimation--a false answer will be accepted.

What's so scary about someone giving your name server an IP address for, say, pdq.paypal.com? Nothing, of course. But remember that the attacker can add some devastating additional information to his spoofed DNS response--namely, a false IP address for www.paypal.com. Such fakery will pass the bailiwick checks because the extra information is for the same domain as the bogus name that was being looked up in the first place. So the bad address will go into the cache, taking the place of the previous entry for www.paypal.com if one had been stored there.

The 8 July patch makes such an attack much more difficult--though not impossible. It works by randomly varying not just the query ID but also the port number in use, which you can think of as being like the suite number on a postal address. To defeat this defense, a hacker must guess both the 16-bit query ID and the 16-bit port number--32 bits in all--requiring, on average, some 4 billion spoofed replies to be received. Such a colossal amount of traffic would be hard to conceal from network administrators.

**Security** professionals are taking Kaminsky's attack scenario very seriously, and hackers appear to be testing the waters.

Computer-security expert Steven M. Bellovin, a professor of computer science at Columbia University, in New York City, says, ”I've seen reports that it's started to happen in the wild.” But he believes that DNS cache poisoning will ultimately affect few people--in contrast to what can happen with certain computer viruses and worms--given that system administrators are now taking appropriate steps. He nevertheless cautions, ”It's one of the more serious problems we've seen, because it's going after the infrastructure. The hard-core bad guys are starting to wake up.”

**To Probe Further**

Paul Vixie’s pioneering report ”DNS and BIND Security Issues,” which warned that the Domain Name System was vulnerable to attack, appeared in *Proceedings of the Fifth USENIX UNIX Security Symposium* , Salt Lake City, June 1995.

A full description of how the Domain Name System works is available in *DNS and BIND* , Fifth Edition, by Cricket Liu and Paul Albitz, O’Reilly, 2006.

**Learn More**

[DNS](http://spectrum.ieee.org/tag/DNS) [DNS](http://spectrum.ieee.org/tag/DNS) [DNSSEC](http://spectrum.ieee.org/tag/DNSSEC) [DNSSEC](http://spectrum.ieee.org/tag/DNSSEC) [Dan Kaminsky](http://spectrum.ieee.org/tag/Dan+Kaminsky) [Dan Kaminsky](http://spectrum.ieee.org/tag/Dan+Kaminsky) [IOActive](http://spectrum.ieee.org/tag/IOActive) [IOActive](http://spectrum.ieee.org/tag/IOActive) [Internet security](http://spectrum.ieee.org/tag/Internet+security) [Internet security](http://spectrum.ieee.org/tag/Internet+security) [bailiwick checking](http://spectrum.ieee.org/tag/bailiwick+checking) [bailiwick checking](http://spectrum.ieee.org/tag/bailiwick+checking) [cache poisoning](http://spectrum.ieee.org/tag/cache+poisoning) [cache poisoning](http://spectrum.ieee.org/tag/cache+poisoning) [computer hack](http://spectrum.ieee.org/tag/computer+hack) [computer hack](http://spectrum.ieee.org/tag/computer+hack) [domain-name system](http://spectrum.ieee.org/tag/domain-name+system) [domain-name system](http://spectrum.ieee.org/tag/domain-name+system) [port randomization](http://spectrum.ieee.org/tag/port+randomization) [port randomization](http://spectrum.ieee.org/tag/port+randomization)

* [Share](http://spectrum.ieee.org/computing/software/fresh-phish/0)
* |
* [Email](http://spectrum.ieee.org/computing/software/fresh-phish/0" \o "Email" \t "_blank)
* |
* [Print](http://spectrum.ieee.org/computing/software/fresh-phish/0)

**Comments**

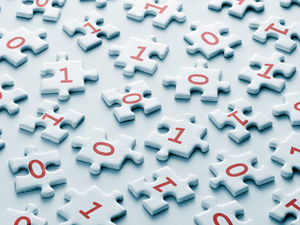
[Comment Policy](http://spectrum.ieee.org/static/comment-policy)

**Related Stories**

[[](http://spectrum.ieee.org/computing/software/skypes-real-time-translator-learns-how-to-speak-from-social-media)Computing](http://spectrum.ieee.org/computing/software/skypes-real-time-translator-learns-how-to-speak-from-social-media)

**[Skype’s Real-Time Translator Learns How to Speak From Social Media](http://spectrum.ieee.org/computing/software/skypes-real-time-translator-learns-how-to-speak-from-social-media)**

[The quirky cant of Twitter and Facebook helped Microsoft build the tools for its real-time translator22 Aug](http://spectrum.ieee.org/computing/software/skypes-real-time-translator-learns-how-to-speak-from-social-media)

[[](http://spectrum.ieee.org/tech-talk/computing/software/cybersecurity-center-mathematical-obfuscation)Computing](http://spectrum.ieee.org/tech-talk/computing/software/cybersecurity-center-mathematical-obfuscation)

**[Mathematical Obfuscation Against Hackers Is Focus of New Cybersecurity Center](http://spectrum.ieee.org/tech-talk/computing/software/cybersecurity-center-mathematical-obfuscation)**

[Researchers hope obfuscation methods will protect software from hackers14 Aug](http://spectrum.ieee.org/tech-talk/computing/software/cybersecurity-center-mathematical-obfuscation)

[[](http://spectrum.ieee.org/tech-talk/computing/software/google-searches-predict-politics-stock-market)Computing](http://spectrum.ieee.org/tech-talk/computing/software/google-searches-predict-politics-stock-market)

**[Google Searches About Politics Predict the Stock Market](http://spectrum.ieee.org/tech-talk/computing/software/google-searches-predict-politics-stock-market)**

[But the connection is weakening30 Jul](http://spectrum.ieee.org/tech-talk/computing/software/google-searches-predict-politics-stock-market)

[[](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-metric-moves-to-the-real-world)Computing](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-metric-moves-to-the-real-world)

**[A Fictional Compression Metric Moves Into the Real World](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-metric-moves-to-the-real-world)**

[The Weissman Score, a compression algorithm metric created for HBO's Silicon Valley, is making its way into the real world28 Jul](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-metric-moves-to-the-real-world)

[[](http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race)Computing](http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race)

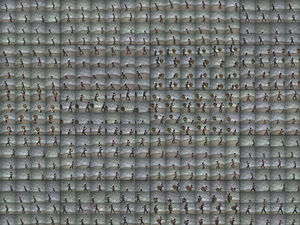
**[Browser Fingerprinting and the Online-Tracking Arms Race](http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race)**

[Web advertisers are stealthily monitoring our browsing habits—even when we tell them not to25 Jul](http://spectrum.ieee.org/computing/software/browser-fingerprinting-and-the-onlinetracking-arms-race)

[[](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-algorithm)Computing](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-algorithm)

**[A Made-For-TV Compression Algorithm](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-algorithm)**

[Stanford’s Tsachy Weissman and Vinith Misra created a fictional, but plausible, compression algorithm for HBO’s Silicon Valley comedy series25 Jul](http://spectrum.ieee.org/view-from-the-valley/computing/software/a-madefortv-compression-algorithm)

[[](http://spectrum.ieee.org/tech-talk/computing/software/camerafilled-dome-recreates-full-3d-motion-scenes)Computing](http://spectrum.ieee.org/tech-talk/computing/software/camerafilled-dome-recreates-full-3d-motion-scenes)

**[Camera-Filled Dome Recreates Full 3-D Motion Scenes](http://spectrum.ieee.org/tech-talk/computing/software/camerafilled-dome-recreates-full-3d-motion-scenes)**

[The same technique could theoretically recreate scenes captured by hundreds of spectator cameras23 Jul](http://spectrum.ieee.org/tech-talk/computing/software/camerafilled-dome-recreates-full-3d-motion-scenes)

[[](http://spectrum.ieee.org/computing/software/top-10-programming-languages)Computing](http://spectrum.ieee.org/computing/software/top-10-programming-languages)

**[Top 10 Programming Languages](http://spectrum.ieee.org/computing/software/top-10-programming-languages)**

[Spectrum’s 2014 Ranking19 Jul](http://spectrum.ieee.org/computing/software/top-10-programming-languages)

[[](http://spectrum.ieee.org/tech-talk/computing/software/motion-capture-technology-goes-into-the-wild-for-dawn-of-the-planet-of-the-apes)Computing](http://spectrum.ieee.org/tech-talk/computing/software/motion-capture-technology-goes-into-the-wild-for-dawn-of-the-planet-of-the-apes)

**[Motion Capture Technology Goes Into the Wild for Dawn of the Planet of the Apes](http://spectrum.ieee.org/tech-talk/computing/software/motion-capture-technology-goes-into-the-wild-for-dawn-of-the-planet-of-the-apes)**

[Weta Digital takes motion capture systems out of the movie studio and into the woods10 Jul](http://spectrum.ieee.org/tech-talk/computing/software/motion-capture-technology-goes-into-the-wild-for-dawn-of-the-planet-of-the-apes)

[[](http://spectrum.ieee.org/static/interactive-the-top-programming-languages)Computing](http://spectrum.ieee.org/static/interactive-the-top-programming-languages)

**[Interactive: The Top Programming Languages](http://spectrum.ieee.org/static/interactive-the-top-programming-languages)**

[IEEE Spectrum’s 2014 Ranking3 Jul](http://spectrum.ieee.org/static/interactive-the-top-programming-languages)

[[](http://spectrum.ieee.org/podcast/computing/software/combing-sensors-and-rewards-for-good-behavior-with-nudge-engines)Computing](http://spectrum.ieee.org/podcast/computing/software/combing-sensors-and-rewards-for-good-behavior-with-nudge-engines)

**[Combing Sensors and Rewards for Good Behavior with “Nudge Engines”](http://spectrum.ieee.org/podcast/computing/software/combing-sensors-and-rewards-for-good-behavior-with-nudge-engines)**

[Balaji Prabhakar’s technology can produce less-crowded streets and healthier employees17 Jun](http://spectrum.ieee.org/podcast/computing/software/combing-sensors-and-rewards-for-good-behavior-with-nudge-engines)

[[](http://spectrum.ieee.org/tech-talk/computing/software/skype-will-translate-multilingual-conversations-by-next-year)Computing](http://spectrum.ieee.org/tech-talk/computing/software/skype-will-translate-multilingual-conversations-by-next-year)

**[Skype Will Translate Multilingual Conversations by Next Year](http://spectrum.ieee.org/tech-talk/computing/software/skype-will-translate-multilingual-conversations-by-next-year)**

[Skype Translator is trying to connect people across the globe, regardless of language barriers28 May](http://spectrum.ieee.org/tech-talk/computing/software/skype-will-translate-multilingual-conversations-by-next-year)

[[](http://spectrum.ieee.org/computing/software/digital-actors-go-beyond-the-uncanny-valley)Computing](http://spectrum.ieee.org/computing/software/digital-actors-go-beyond-the-uncanny-valley)

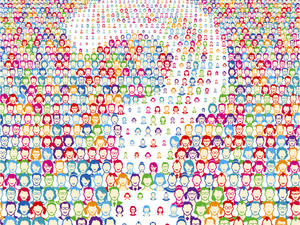
**[Digital Actors Go Beyond the Uncanny Valley](http://spectrum.ieee.org/computing/software/digital-actors-go-beyond-the-uncanny-valley)**

[Computer-generated humans in movies and video games are paving the way for new forms of entertainment27 May](http://spectrum.ieee.org/computing/software/digital-actors-go-beyond-the-uncanny-valley)

[[](http://spectrum.ieee.org/tech-talk/computing/software/the-golden-age-of-basic)Computing](http://spectrum.ieee.org/tech-talk/computing/software/the-golden-age-of-basic)

**[The Golden Age of Basic](http://spectrum.ieee.org/tech-talk/computing/software/the-golden-age-of-basic)**

[In the 1980s, Basic shaped a generation of young programmers1 May](http://spectrum.ieee.org/tech-talk/computing/software/the-golden-age-of-basic)

[[](http://spectrum.ieee.org/tech-talk/computing/software/fbis-facial-recognition-database-will-include-noncriminal)Computing](http://spectrum.ieee.org/tech-talk/computing/software/fbis-facial-recognition-database-will-include-noncriminal)

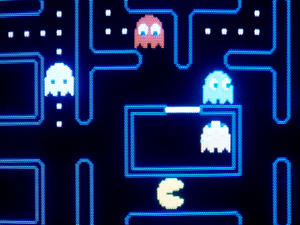
**[FBI's Facial Recognition Database Will Include Non-Criminals](http://spectrum.ieee.org/tech-talk/computing/software/fbis-facial-recognition-database-will-include-noncriminal)**

[The FBI's new database of face images will allow law enforcement to search for suspect matches among ordinary citizens16 Apr](http://spectrum.ieee.org/tech-talk/computing/software/fbis-facial-recognition-database-will-include-noncriminal)

[[](http://spectrum.ieee.org/tech-talk/computing/software/face-aging-software-can-show-your-childs-future)Computing](http://spectrum.ieee.org/tech-talk/computing/software/face-aging-software-can-show-your-childs-future)

**[Face Aging Software Can Show Your Child's Future](http://spectrum.ieee.org/tech-talk/computing/software/face-aging-software-can-show-your-childs-future)**

[A baby's face can be accurately aged through adulthood with the first automated aging software10 Apr](http://spectrum.ieee.org/tech-talk/computing/software/face-aging-software-can-show-your-childs-future)

[[](http://spectrum.ieee.org/tech-talk/computing/software/computers-learn-and-teach-each-other-by-playing-pacman)Computing](http://spectrum.ieee.org/tech-talk/computing/software/computers-learn-and-teach-each-other-by-playing-pacman)

**[Computers Learn and Teach Each Other by Playing Pac-Man](http://spectrum.ieee.org/tech-talk/computing/software/computers-learn-and-teach-each-other-by-playing-pacman)**

[Knowing when to give advice is the key to success3 Apr](http://spectrum.ieee.org/tech-talk/computing/software/computers-learn-and-teach-each-other-by-playing-pacman)

[[](http://spectrum.ieee.org/tech-talk/computing/software/computer-can-spot-fake-expressions-of-pain-)Computing](http://spectrum.ieee.org/tech-talk/computing/software/computer-can-spot-fake-expressions-of-pain-)

**[New Computer Vision System: "Nope. She's Faking It"](http://spectrum.ieee.org/tech-talk/computing/software/computer-can-spot-fake-expressions-of-pain-)**

[Computers are better than humans at spotting fake expressions of pain20 Mar](http://spectrum.ieee.org/tech-talk/computing/software/computer-can-spot-fake-expressions-of-pain-)

[[](http://spectrum.ieee.org/podcast/computing/software/identifying-the-recipe-for-literary-success)Computing](http://spectrum.ieee.org/podcast/computing/software/identifying-the-recipe-for-literary-success)

**[Identifying the Recipe for Literary Success](http://spectrum.ieee.org/podcast/computing/software/identifying-the-recipe-for-literary-success)**

[Computer analysis can predict a book’s appeal7 Mar](http://spectrum.ieee.org/podcast/computing/software/identifying-the-recipe-for-literary-success)

[EEE Spectrum logo](http://spectrum.ieee.org/)

**Topics**

* [Aerospace](http://spectrum.ieee.org/aerospace)
* [At Work](http://spectrum.ieee.org/at-work)
* [Biomedical](http://spectrum.ieee.org/biomedical)
* [Computing](http://spectrum.ieee.org/computing)
* [Energy](http://spectrum.ieee.org/energy)
* [Gadgets](http://spectrum.ieee.org/gadgets)
* [Geek Life](http://spectrum.ieee.org/geek-life)
* [Robotics](http://spectrum.ieee.org/robotics)
* [Semiconductors](http://spectrum.ieee.org/semiconductors)
* [Telecom](http://spectrum.ieee.org/telecom)

**Connect**

* [Facebook](http://www.facebook.com/IEEE.Spectrum" \t "_blank)
* [Twitter](http://twitter.com/" \l "%21/IEEESpectrum" \t "_blank)
* [LinkedIn](http://www.linkedin.com/groups/IEEE-Spectrum-1982451?home=&gid=1982451&trk=anet_ug_hm" \t "_blank)
* [Google+](https://plus.google.com/105079317383160047042/posts" \t "_blank)
* [RSS](http://spectrum.ieee.org/static/rss" \t "_blank)

**IEEE Spectrum**

* [Contact Us](http://spectrum.ieee.org/static/contactus)
* [About](http://spectrum.ieee.org/static/aboutus)
* [Newsletters](http://spectrum.ieee.org/static/newsletters)
* [Mobile Site](http://m.spectrum.ieee.org/)

**IEEE Partners**

* [Advertising & Media Center](http://advertise.ieee.org)
* [IEEE Job Site](http://careers.ieee.org/)
* [Buyer’s Guide](http://spectrumsuppliermarketplace.com/)

**The Magazine**

* [agazine cover image](http://spectrum.ieee.org/magazine)
* [Subscribe Now](http://spectrum.ieee.org/static/readerservices)
* [Digital Download](http://www.qmags.com/subscribers)
* © Copyright 2014 IEEE Spectrum
* [Terms & Conditions](http://www.ieee.org/site_terms_conditions.html?WT.mc_id=hpf_terms) | [Privacy & Security](http://www.ieee.org/privacy) | [Nondiscrimination Policy](http://www.ieee.org/nondiscrimination)

[EEE logo](http://www.ieee.org)

* [About IEEE](http://www.ieee.org/about/index.html)
* [Conferences & Events](http://www.ieee.org/conferences_events/index.html)
* [Education & Careers](http://www.ieee.org/education_careers/index.html)
* [Membership & Services](http://www.ieee.org/membership_services/index.html)
* [Publications and Standards](http://www.ieee.org/publications_standards/index.html)
* [Societies & Communities](http://www.ieee.org/societies_communities/index.html)