Certs for the Masses

The Case for a Community-Oriented Certificate Authority

Author: ©2004 Adam Butler <adam@donkeyrequiem.com>

Secure authentication and encryption methodologies want to be free.

Okay, I admit it. Compared with all the other OSS anthropomorphisms floating around, that one's a bit of a mouthful. Nevertheless, the need for strong and reliable data security is as old as data itself.

While the Internet community has championed the "information wants to be free" cause for as long as I can remember, this concept has always been tempered with a profound respect for personal privacy. Consistently, the heroes of the open source movement trumpet the emancipation of innumerable ones and zeroes across the globe while contemporaneously applauding the individual's right to keep his or her ones and zeroes private and secure.

Savvy computer users recognised this need from the very beginning not because they had anything in particular to hide; rather, they merely realised that private data wasn't safe from prying eyes unless specific steps were taken to ensure that safety.

Long before buggy WEP-encrypted WLAN access points dotted the landscape—hell, even before the 1990s Internet retailing explosion—countless individuals sent countless petabytes of God-knows-what to God-knows-who without realising that every bit of their communications could be (and often were) intercepted by others.

Over time, folks wised up. For the sysadmins among us, ask yourself: When was the last time you accessed one of your boxes in an open, untrusted environment, using telnet rather than SSH?

And even Joe User caught on, eventually learning to check his browser for that nifty lock/key icon before submitting his online purchase. Sure, he probably still has little or no idea what is meant by terms like "Secure Sockets Layer" or "128-bit encryption," but at least he knows to check first before spiriting his credit card information off into the ether as clear text.

I doubt anyone would seriously discount the role of PKI, SSL, et al, in strengthening consumer confidence in secure web transactions and thereby laying the groundwork that allowed companies like Amazon and eBay to succeed—but the Public Key Infrastructure allows for so much more than mere virtual mercantilism.

For the most part, the Internet community exploits only a tiny fraction of what this valuable technology has to offer—and with gross privacy violations occurring at disturbingly increasing frequencies,[1] it would seem that now more than ever, the importance of publicly available cryptography tools and techniques cannot be understated.

It's time to take the next steps in securing our personal data and that of our users. For that, we're going to need a Certificate Authority.

ENTER CACERT

Until recently, the thought of approaching a CA for not one but *numerous* X.509 certificates might have tied your stomach in knots, caused you to break out in hives, and may have even prompted you to murder your entire family. Because unless Daddy's trust fund left you so much dough that you're routinely torching $100 bills just to light your Havanas, you're probably turned off a bit by the realisation that the best price any CA offers is still going to require you take out a second mortgage on the house.

But Dylan quotes so often lend themselves to the OSS movement, and now is no exception: Times are indeed a-changin'.

Late last year, CAcert, a nonprofit, OSS-based Certificate Authority quietly stepped forward with a proposal that was as simple as it was groundbreaking: the Australian-borne organisation would offer signed, 128-bit X.509 certificates for personal and server-side use…for free.

Like so many open source mavericks before them, a small group of committed individuals simply took a long, hard look at a particular industry—in this case, the buying and selling of X.509 certificates—and realised they could do a better job. In almost no time at all, CAcert was providing gratis what industry leaders Thawte and VeriSign were routinely hawking for hundreds or even thousands of dollars apiece.[2]

Today, CAcert offers signed, 128-bit X.509(v3) certificates for SSL, Wireless Auth, S/MIME, VPN, and other authentication/encryption schemes. And whether you're in the market for a personal or server-side solution, you can leave your cache of Spanish doubloons at home—CAcert's expenses are still covered by donations and advertising, not exorbitant (and unnecessary) annual fees.

And that's not all. The venerable CA already offers a highly thought-out "Web of Trust" assurance scheme,[3] gently lifted from the highly thought-out WOT scheme offered by Thawte,[4] which was in turn borrowed from the highly thought-out WOT scheme developed by Phil Zimmerman and the folks at PGP.[5] The WOT program allows CAcert's more than 5000 members to notarise/sign/assure (depending on whose terminology you prefer) one another in pursuit of "Trust Points."

As a user increases his or her number of trust points with CAcert, advanced features are unlocked and become available for use. One such feature allows users to submit their PGP/GPG key to be signed by the CAcert master key, a novel integration of multiple PKI technologies.

Another feature, expected to be in place by the time you read this, will be the availability of so-called "code signing" certificates—similar in concept to those used in Microsoft's Authenticode initiative,[6] but minus the evil. CAcert sees this as a chance to give back to its fellow open source compatriots, empowering developers on various OSS projects with the means to digitally sign their work without having to rely on certs from expensive, corporate CAs who could care less about the OSS community.

SUPPORTING THE OSS INFRASTRUCTURE

Undoubtedly the most important role of a Community-Oriented Certificate Authority is to provide an affordable alternative to commercial certificate authorities, thus enabling thousands of smaller web presences to abandon their current hackneyed PKI implementations and fall under the umbrella of a true CA, rather than relying on self-generated certificates in which users are (rightfully) leery of placing their trust.

As the situation currently stands, webmasters who wish to employ some type of Public Key Infrastructure—SSL, for example—usually feel that they must choose between (1) paying hundreds of dollars each year for a "trusted" certificate signed by some big name CA, or (2) grabbing a current copy of the SSL libraries and generating their own self-signed, "untrusted" cert for $0. Unsurprisingly, many of these webmasters opt for the second choice—necessitating that each of their (apparently *quite* trusting) users download and install their sites' home-brewed root certificates, always assuming/trusting that Webmaster X **really is** Webmaster X, even if no one has ever confirmed this in any form or fashion.

With CAcert, a new option unfolds. Rather than fool around with generating a homebrew SSL cert, a webmaster unwilling to pony up for commercial certificate services can instead obtain one signed by CAcert. And unlike the self-signed certificate, CAcert "vouches for" its certificate and reveals to site visitors (via trust points) how well known/trusted the webmaster is by the CA, giving visitors to the site straightforward, independent verification that Bob's Porn Palace is indeed operated by Bob.

Additionally, as more webmasters abandon self-signed certificates for flexible, widely-available CAcert products, they free themselves of having to publish site-specific root certificates, revocation lists, and the like. Users simply install CAcert's root certificate—which isn't that much to ask, considering that CAcert (as an independent CA) employs the same methods of member verification as its for-profit competitors—and voila, they'll be able to work with not just that one site, but all other sites that fall under CAcert's umbrella.

Thus a CAcert solution requires less work on the part of the webmaster and it's safer for the users—the latter point having the added advantage of potentially driving more traffic to certain sites, as users who didn't trust the homebrew PKI solution might be more inclined to accept the CAcert trust model instead.

So CAcert is rocking and rolling along, expanding on traditional PKI and offering gads of cool new options for encryption, authentication, digital signing, and the like—and all without robbing its users blind. What's the catch?

Well, there's no catch—just head over to www.cacert.org and check it out for yourself. But there are a few small flies in the ointment.

Fortunately, hackers are well known for jumping into the thick of things and coming to the aid of worthwhile projects…the perfect audience for a subtle call to action. ;)

ROOT CERTIFICATE INCLUSION IN BROWSERS

Obviously a major goal for CAcert is to have its root certificate included with all of the popular web browsers, so visitors to secure sites are neither required to download and install the cert themselves nor be subjected to whatever awkward error messages their browser of choice decides to toss at them.

With something like 300 billion people using Windows in southern Florida alone, it's no shock that Internet Explorer is by far the leader when it comes to browser market share. Anecdotal evidence (and common sense) seems to suggest that back during the Browser Wars, commercial certificate authorities probably greased the wheels with a healthy chunk of change to ensure that their root certificates would be included in both Navigator/Communicator and IE—ah, the hidden costs of "strategic partnerships!"

These days, each browser has dramatically different requirements in terms of root certificate inclusion.

In true Microsoft style, Redmond adopted a new metric for determining whether a CA's root certificate is to be included with its browser/operating-system/kitchen-sink product: in order for a CA's root certificate to be accepted—I swear I'm not making this up—said certificate authorities must pay a WebTrust-licensed member of the American Institute of Certified Public Accountants ***up to $250,000*** for an initial evaluation/inspection, plus additional *tens of thousands of dollars* in fees for periodic "follow-ups."[7]

The makers of the Opera web browser did not respond to email queries regarding their inclusion policies/requirements, however a Bermuda-based CA representative stated in the netscape.public.mozilla.crypto newsgroup that "as of [his] last contact in 2003, Opera wanted cash to add a CA [root certificate]. *They currently do not appear to have a standards policy.*"[8,9] Nice to see somebody's got their priorities straight, eh?

Rather than getting into all the other browsers and browser-like programs under the sun, let's jump a bit and discuss open source's favorite son: Mozilla.

GETTING IN GOOD WITH THE LIZARD

The Open Source advocates among us look forward to a time when software is finally wrenched free from the clutches of its faceless captors—massively proprietary organisations whose interests in innovation seldom reach beyond their own shortsighted marketing strategies, leaving less profitable technologies to stagnate.

And while collaborative software initiatives flourish across the globe, services designed to support and expand the underlying OSS infrastructure continue to face significant challenges. These barriers sometimes arise from corporations leveraging their de facto monopolies against newcomers, but often there's no evil empire to blame. Frequently, bumps in the road are merely the result of various open source advocates and developers disagreeing about one thing or another.

After Netscape disappeared, leaving no one behind to make "executive decisions" about critical things such as root certificate inclusions, the Mozilla Foundation embraced a policy of maintaining the status quo,

keeping all existing root certificates installed without really considering what would happen when/if any new CAs came knocking.[10]

(This installed base remained the same even after existing certificate authorities erroneously issued multiple Authenticode certificates labeled "Microsoft Corporation" to a couple of crafty social engineers,[11] arguably demonstrating once and for all that money can't buy you love ***or*** security.)

Trying to go through all the proper channels, developers submitted a "feature enhancment" request to Bugzilla, asking that the CAcert root certificate be included in Mozilla."[12] (This inventive maneuver would pop up in Konqueror's feature request system, also.)[13]

About six months after the Bugzilla request was submitted, an announcement was made inidcating that the CAcert root certificate would be part of the soon-to-be-released Mozilla 1.6.[14]

The announcement momentarily vaulted CAcert's otherwise innocuous request into the public eye—and with all the sudden new exposure came increased scrutiny. While most people were either in favor of the decision or indifferent, some of the more security-minded Mozilla developers voiced concerns.

Despite its nonprofit status, CAcert was criticized for its failure to retain the services of prohibitively expensive third-party auditing firms. As a volunteer-led community certificate authority providing free services to thousands of users, CAcert was in no position to pay for outside consultants.

CAcert is just another two-bit, fly-by-night operation, claimed some of its detractors. There's no oversight, they charged. The whole operation probably just consists of a cable modem, an old Packard Bell laptop, a pirated copy of PC-DOS 3.0, and four lines of Perl code. Their certificates are all encrypted with ROT13. Their private key is stored for safe keeping on a purple Hello Kitty diskette atop Dad's Van de Graaff Generator. Oh, and they spend their free time issuing certificates to serial killers, zombies, and men who bite the heads off kittens. That's right...*kittens.*[15]

Eventually the discussion spilled out of Bugzilla and was was shepherded over to the netscape.public.mozilla.crypto newsgroup. The original Bugzilla feature enhancement request was subsequently blocked/superseded by a directive that the Mozilla Foundation was to develop a formal Certificate Authority acceptance policy before accepting any new root CAs.[16] Wildly disparate proposals for the new acceptance policy flew in from everywhere—people suggested everything from AICPA/WebTrust certification (insanely expensive) to an "open door policy" that would give everybody and anybody who applied access to the root store (insanely reckless)...and every imaginable gradient in between.

I have tremendous respect for all of the individuals who volunteer their time for the Mozilla Foundation, and I can completely understand the fears voiced by those who preferred the status quo. Furthermore, I am certain everyone best intentions at heart...despite the distinct feeling that the discussion had degraded almost to the point of a filibuster.

In some discussions, it seemed as if two or three people were just yelling "NO!" at the top of their lungs without providing any real basis for their concerns—nevertheless, these passionate appeals were frustratingly successful in their ability to steer the debate off-course. I certainly can't fault the individuals involved for trying, of course. For whatever reason, certain people apparently felt that the Mozilla Project was in imminent danger, and so they defended it to the best of their abilities. I have little doubt that I would have done the same, had the roles been reversed.

Fortunately, there is a happy end to this story. After much debate and gnashing of teeth, the CAcert root certificate once again seems on-track for inclusion in the next Mozilla release. (Fingers crossed.)

LOOKING AHEAD

Though the development of a Community-Oriented Certificate Authority doesn't quite reach Kuhn's definition of a true "paradigm shift," it's a revolution nonetheless. Just as when Network Solutions lost its monopoly on domain registration, things have changed significantly for the better. And there's no looking back.

None of us today would consider paying $35 a year to register a top level domain, and very soon VeriSign's $1200+ pricing for SSL certificates will strike us as equally ridiculous—because when you read this article, even if CAcert's root certificate still somehow remains excluded from the basic Mozilla install, the organization will still be growing and gathering momentum. At this point, there's no sense asking if the group will accomplish one thing or another—anything's possible, and it's all just a matter of time.

Says CAcert founder Duane Groth: "[T]he established players in the certificate industry lobby hard to exclude any further competition from entering the market, which means they are able to keep charging exorbitant rates for certificates....This is all set to change.

"Currently there are hundreds of thousands of web browsers out there with our root certificate installed; companies are deploying intranets with certificates issued from CAcert and installing the root certificate on each client machine on the network.... [M]omentum is building at a grass roots level."

Until CAcert's root certificate is preinstalled in your browser of choice, remember that you can always install it manually by visiting www.cacert.org and clicking the appropriate link. And if you're wondering what you can do to help with the effort, join the CAcert mailing list, make suggestions and donations—contribute how you can, if you can. And see the notes at the end of this article for the URLs where you can vote for CAcert's inclusion in Mozilla and Konqueror.

But most importantly: Visit the site, sign up, grab a certificate or two, and start securing your data. Because regardless of what politics may be going on behind the scenes and what seemingly unattainable goals the organisation may set for itself, whether you can spare some time to help with the project isn't the point. CAcert's mission remains the same: to provide you with alternatives to commercial CAs like VeriSign and Thawte, to help you secure your data, and to do the same for the rest of our Internet Community.

It's a crazy world out there, so keep your data safe and your sessions secure. And let us help.

1"The Regulation of Investigational Powers Act (RIPA)," http://www.homeoffice.gov.uk/crimpol /crimreduc/regulation/index.html. 28 Jul 00. See also "U.K. e-mail snooping bill passed," http://www.cnn.com/2000/TECH/computing/07/28/uk.surveillance.idg/: 28 Jul 2000.

2As of 15 Mar 04, Thawte offered two 128-bit SSL server certificates, priced at $199 and $449 per year, respectively. On that same date, VeriSign offered a host of 128-bit SSL certificate packages ranging from $895 to $1495 per year. (All figures in US$ unless otherwise noted.)

3CAcert, "Assurance Programme," http://www.cacert.org/index.php?id=8 (18 Mar 2004).

4Thawte, "Freemail Web of Trust System," https://www.thawte.com/cgi/personal/wot/contents.exe (15 Apr 2004). See also Thawte, "thawte: web of trust," https://www.thawte.com/wot/index.html (18 Apr 2004).

5William Stallings, "The PGP Web of Trust." Byte, Feb 1995.

6Roger Grimes, "Authenticode," Microsoft TechNet, http://www.microsoft.com/technet/ security/topics/secapps/authcode.mspx (18 Mar 04).

7Microsoft Technet, "Microsoft Root Certificate Program Requirements," http://www.microsoft.com/technet/security/news/rootcert.mspx (18 Mar 04). See also American Institute of Certified Public Accountants, "WebTrust Program for Certification Authorities: Version 1.0," http://ftp.webtrust.org/webtrust_public/tpafile7-8-03fortheweb.doc: 25 Aug 2000.

8Emphasis added.

9Name withheld, "RE: Proposed CA certificate metapolicy," news://netscape.public.mozilla.crypto: 3 Mar 2004. See also "Re: why and how VeriSign, thawte became a trusted CA?" news://comp.security.misc: 15 Mar 2004.

10For a list of all the CA root certificates shipped with Mozilla browsers by default, open your copy of Mozilla or Firefox and select Edit -> Preferences -> Privacy & Security -> Certificates -> Manage Certificates -> Authorities.

11Microsoft Knowledge Base, "How to Recognize Erroneously Issued VeriSign Code-Signing Certificates," http://support.microsoft.com/default.aspx?scid=kb;en-us;293817&sd=tech (18 Mar 04). See also Microsoft Technet, "Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard," http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx (18 Mar 04).

12You too can vote for CAcert root certificate inclusion in the next version of Mozilla. The party's right here: http://bugzilla.mozilla.org/show_bug.cgi?id=215243.

13Encourage the KDE Group to include CAcert's root certificate in the next version of Konqueror. Vote at: http://bugs.kde.org/show_bug.cgi?id=74290.

14Frank Hecker, "Additional Comment #20," http://bugzilla.mozilla.org/show_bug.cgi?id=215243: 4 Feb 04.

15Actually, CAcert is a fully recognized, legally incorporated nonprofit organization with a board of directors, an organizational charter, and a strict set of bylaws that explicitly forbids strategic alliances with zombies or other members of the undead. The CA servers are stored at a secure colocation facility, complete with biometric palm scanners and other cool stuff like that. And nothing is stored or signed in ROT13 format—CAcert has always relied on the far superior Triple-ROT26 algorithm for all cryptography. :)

16"Mozilla.org needs a public policy on root CA certs," http://bugzilla.mozilla.org/show_bug.cgi?id=233453 (14 Mar 04).