certs for the masses

A Community-Oriented Certificate Authority

by Adam Butler

Adam Butler is a board member and marketing/PR director for CAcert, Inc. This past April, as part of his "PKI Roadshow," he traveled throughout the European Union to meet with CAcert users and other PKI enthusiasts. Look for Adam and the rest of the CAcert crew at this year's USENIX conference in Boston or email him direct at

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 recognized this need from the very beginning, not because they had anything in particular to hide; rather, they merely realized 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 realizing 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 cleartext.

I doubt anyone would seriously dismiss 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 overstated.

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 certificate authority (CA) for not one but numerous X.509 certificates might have tied your stomach in knots, caused you to break out in hives, and 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

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

bills just to light your Havanas, you're probably turned off a bit by the realization that the best price any CA offers is still going to require that you take out a second mortgage on the house.

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-born organization 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 realized 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 a 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 5,000 members to notarize/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 not care less about the OSS community.

Supporting the OSS Infrastructure

Undoubtedly, the most important role of a community-oriented CA is to provide an affordable alternative to commercial certificate authorities. This enables 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

2. As of March 15, 2004, Thawte offered two 128-bit SSL server solutions, priced at $199 and $449 per year. 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).

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

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

5. William Stallings, "The PGP Web of Trust," *Byte* (February 1995).

6. Roger Grimes, "Authenticode," Microsoft TechNet, *http://www.microsoft.com/technet/security/topics/secapps/authcode.mspx* (March 18, 2004).

A CAcert solution requires less work on the part of the webmaster, and it's safer for the users.

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 one of VeriSign's products 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 from 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, voilà, 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 has 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 gobs 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 *http://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 Cert 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 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 Georgia 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, the various browsers have 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/OS/kitchen-sink product: In order for a CA's root certificate to be accepted – I swear I'm not making this up – Redmond said CA 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 on a periodic "follow-up" basis .[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 did not appear to have a standards policy*."[8] Nice to see somebody's got their priorities straight, eh?[9]

Rather than getting into all the other browsers under the sun, e.g., Safari, Konqueror, Lynx, and whatever crappy little program came with my Palm Pilot, let's jump ahead a bit and discuss open source's favorite son: Mozilla/Firefox.

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 organizations 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.

Earlier, I mentioned the Mozilla Foundation and its (apparently) nonexistent root certificate inclusion policy.

After Netscape disappeared, leaving no one to make "executive decisions" about boring stuff like root certificates and the like, the Mozilla Foundation apparently embraced a policy of maintaining the status quo, keeping all the old faves (like VeriSign and S-Trust) installed without really considering what would happen when/if any new CAs came knocking.[10]

This installed base remained the same even after VeriSign 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 enhancement" request to Bugzilla, asking that the CAcert root certificate be included with Mozilla.[12] (This inventive maneuver would later pop up again in Konqueror's feature request system.)[13]

Six months after the Bugzilla feature enhancement request was submitted, an announcement was made indicating that the CAcert root certificate would be included as part of Mozilla 1.6.[14]

And then the whole world started crying.

7. Microsoft TechNet, "Microsoft Root Certificate Program Requirements," *http://www.microsoft.com/technet/security/news/rootcert.mspx* (March 18, 2004). 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* (August 25, 2000).

8. Emphasis added.

9. Name withheld, "RE: Proposed CA Certificate Metapolicy," *news://netscape.public.mozilla.crypto* (March 3, 2004). See also "Re: Why and How VeriSign, Thawte Became a Trusted CA?" *news://comp.security.misc* (March 15, 2004).

10. For 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.

11. Microsoft Knowledge Base, "How to Recognize Erroneously Issued VeriSign Code-Signing Certificates," *http://support.microsoft.com/default.aspx?scid=kb;enus;293817&sd=tech* (March 18, 2004). See also Microsoft Technet, "Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard," *http://www.microsoft.com/technet/security/bulletin/MS01-017.mspx* (March 18, 2004).

12. You 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*.

13. Encourage 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*.

14. Frank Hecker, "Additional Comment #20," *http://bugzilla.mozilla.org/show_bug.cgi?id=215243* (Feb. 4, 2004).

All of a sudden, everyone and their brothers, best friends, and pets were posting messages to the site and arguing back and forth, debating the wisdom of what had just happened. The discussion eventually spilled out of Bugzilla and was shepherded over to the netscape.public.mozilla.crypto newsgroup.

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 start handing over big wads of cash to consulting firms.

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 and their private key is stored on a purple Hello Kitty diskette that sits atop Dad's Van de Graaff generator. They spend their free time issuing certificates to serial killers, zombies, and men who bite the heads off kittens.

That's right. Kittens.[15]

The original Bugzilla feature enhancement request was subsequently blocked/superseded by a directive that the Mozilla Foundation develop a formal certificate authority acceptance policy (presumably from scratch) 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 Project, and I can completely understand the fears voiced by those who preferred the status quo. Furthermore, I am certain everyone who participated in all the various debates had nothing but the best intentions, even though the discussion seemed a bit more like a filibuster with each passing day.

In some arguments, it was as if two or three people were simply yelling "NO" at the top of their lungs, arguing against everything, often not even taking the time to explain the basis underlying their concerns; nevertheless, these passionate appeals were frustratingly successful in their ability to steer the debate off-course, even when the overwhelming majority seemed on the verge of reaching some kind of compromise.

Though I may disagree with their views on the issue, I certainly can't fault the individuals involved for trying. After all, the minority opinion must be loud, lest it not being heard. 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

15. Actually, 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 co-location 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* (March 14, 2004).

when Network Solutions lost its monopoly on domain registration, things have changed significantly for the better. And there's no going 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 as you read this article, even if its root certificate still somehow remains excluded from the basic Mozilla install, CAcert 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 *http://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 and make suggestions and donations – contribute how you can, if you can. And see the notes in 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 organization may set for itself, whether you can spare some time to help with the project is beside 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.

And there's no time like the present. CAcert board members and developers were at CeBIT in Sydney earlier this year, it's only been a few weeks since the "PKI Roadshow" took your humble author halfway around Europe, and now (like many of you) we have our sights set on Boston in July. Along with several of our indefatigable developers, the entire CAcert Board of Directors will be at this year's USENIX conference. (Ironically, this will be the first time most of us will have ever set eyes upon one another!)

So, what does this mean for you? Well, if you hated this article, then just hold on to that anger – and soon you'll have a chance to actually smack me in person. For other, less violent attendees, we'll be available to answer questions about CAcert, demonstrate some of the less-appreciated uses for X.509, and help you sign up for your own free certificates.

Quick, get them before it's too late! I read that those things cost thousands of dollars apiece!