

RE: [Full-Disclosure] Cryptome Hacked!

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-02/0383.html>

From: Sung J. Choe (schoe@oicinc.com)

Date: 02/27/03

From: "Sung J. Choe" <schoe@oicinc.com>

To: "'yossarian'" <yossarian@planet.nl>, "'full-disclosure@lists.netsys.com'" <full-disclosure@lists.netsys.com>

Date: Wed, 26 Feb 2003 15:04:27 -1000

> *Let me turn around the issue a bit – any crypto software distributed with the blessing or very active support in development of the Powers That Are in No Such Agency*

That is my point exactly. Anybody foolish enough to think that the US govt would allow unbreakable crypto to be loose in the public domain is insane. Just imagine an international financial network with transactions conducted in total secrecy: the govt would and should never allow that.

> *can we stay clear of political statements on this forum*

I apologize for some of the political statements in my post. However, please take seriously my questions as they are valid for this forum given TIA (Total Information Awareness) and the current state of global security. I appreciate any creative insight anybody may have regarding my question. Please feel free to disregard the other statements.

Sung J. Choe <[SChoe\[at\]oicinc.com](mailto:SChoe[at]oicinc.com) <<mailto:SChoe@oicinc.com>>>, TICSA Systems Administrator, Facility Security Officer

Oceanic Imaging Consultants, Inc. / www.oicinc.com
<<http://www.oicinc.com>> Ph #: (808) 539-3634

-----Original Message-----

From: yossarian [<mailto:yossarian@planet.nl>]

Sent: Wednesday, February 26, 2003 2:17 PM

To: full-disclosure@lists.netsys.com

Subject: Re: [Full-Disclosure] Cryptome Hacked!

Well, the mirror on lessgov is gone too. But <http://cryptome.sabotage.org/> <<http://cryptome.sabotage.org/>> is still up, anyway. So you can see for yourself that they have PGP as the only crypto product they offer. If they have altered it, anyone can see by comparing the source, which they also provide (both stored offsite, and also unavailable right now)

I can believe that you are almost sure, but since this is a fact you can

RE: [Full-Disclosure] Cryptome Hacked!

Full-Disclosure: RE: [Full-Disclosure] Cryptome Hacked!

verify, why assume, why not prove it?

Let me give you a hint: Look at the paper from Claude Crepeau and Alain Slakmon on Simple Backdoors to RSA key generation. If you want to alter PGP in a way difficult to detect, this would be the way. Any other way would be too obvious. If you see how feasible this is, rethink your position. Any keyscheme you use may be backdoored, so generating your own keypairs might just not suffice.

Let me turn around the issue a bit – any crypto software distributed with the blessing or very active support in development of the Powers That Are in No Such Agency, would you assume that there is no backdoor? Just google on Key Recovery features, in P1363 or any other mainstream PKI – search on project Krisis by the EU, or look at the archived site kra.org (on archive.org), look at the discussions related to the wassenaar agreements. See the continuing story from clipper chip via Key Escrow to CKI on certain if not all governments wanting access to your keys for policing? What if the company you serve has offices all over the world? Will you give the cryptkeys to all the countries where you have offices? Remember that ex-CIA boss Wooley admitted 'checking' on European companies, whether they violated trade embargoes? How? As security professionals we need to be aware on who might be reading our confidential information – and then decide whether this is acceptable to the company whose data you must secure. Don't forget that maybe some gov. agencies might lose the keys to the data you should be protecting. What a nice liability case it would be, heh!. Say I open an office in Australia – and the gov there wants root to my systems, for policing. Should I give them access to the corporate network or just the Australian office? But will my network zoning suffice, to keep them off, say, my Miami office's network? Is it legal in Florida giving access to unspecified police or intelligence communities in other countries to data, maybe even sensitive to national security? This will be a definite No, so in order not to break the law in one country, I must break it in another country. How to risk manage this?

On a personal note: I am almost sure that the risk to my personal well-being by the American/Government, albeit small, is bigger than that posed by extremists as John Young, who do not have much means, budget or interest in bothering me. Taking on the US govt, as they do, they'll have their hands full.

And Plz. can we stay clear of political statements on this forum, this is one of the few places I can hang around and not be bothered by political statements, not linked at all to the subjectmatter of the list?

Yossarian

----- Original Message -----

From: Sung J. Choe <<mailto:schoe@oicinc.com>>

To: 'full-disclosure@lists.netsys.com'

<<mailto:full-disclosure@lists.netsys.com>>

Sent: Thursday, February 27, 2003 12:10 AM

RE: [Full-Disclosure] Cryptome Hacked!

Full-Disclosure: RE: [Full-Disclosure] Cryptome Hacked!

Subject: [Full-Disclosure] Cryptome Hacked!

Cryptome.org, a site for privacy enthusiasts and leftists alike, was apparently hacked today. Their server is up but "all files were deleted". Besides the usual anti-American/anti-government vitriol that is usually found at Cryptome.org, they also distribute crypto software. This brings up the following question: What is the best method for ensuring the integrity of software which require a high level of trust? I am almost sure that any crypto software distributed by such extremists as John Young (operator of cryptome.org) has been tampered with in some way. Does anybody else share this opinion?

| Sung J. Choe <schoe[at]joicinc.com>, TICSAs |
Systems Administrator, Facility Security Officer

| Oceanic Imaging Consultants, Inc. |
Phone #: (808) 539-3634 x3634

568D CAD6 53A0 92E6 4A2A 4E87 3BA0 5F90 37BB 8EE7

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/octet-stream attachment: [schoe.vcf](#)

RE: [Full-Disclosure] Cryptome Hacked!