Please comment on this simple software protection schema

Asked 16 years, 2 months ago Modified 1 year, 8 months ago

Viewed 813 times

2

I was asked implement a licensing schema for our product. They are very expensive products with few customers sparsely distributed around the world and basically every one of them has a design environment (a windows application installed on single windows machines, from 1 to 150 client machines per customer) and a web server that hosts production environment (1 to 8 machines per customer). Our product is licensed for server usage so customers can use any number of clients; we've decided not to license the server part (because it's subject to SLA agreements) but only the client, because, after some time without capability to use the client the system becomes basically useless.

Our basic assumption is that the customer is "honest enough" and only thing we would like to cover is stopping the client design environment if not properly licensed with a time expiration license.

I've evaluated different licensing product and they are or too expensive or too difficult to manage, so I've come up with this simple solution:

- The license will be a simple signed XML file, signed using the standard XML Signature feature of w3c, using a private key that will be given to the admin department on a USB key; if they lose of copy it then the licensing schema will fail but it will be their fault
- The client will open the license file on startup and check its validity using a public key embedded in the binaries
- If license XML is valid and the data in it (expiration date and product name) are correct than the designer work; if not, an appropriate message will be shown

Any ideas about possible problems or how to improve the scenario?

drm

Share

Improve this question

Follow

edited Apr 13, 2023 at 15:04

karel

5,852 ● 59 ● 56 ● 59

asked Oct 4, 2008 at 8:48

massimogentilini

4,162 ● 5 ● 31 ● 32

This question has nothing to do licensing directly, it's about software protection techniques. Please correct the title accordingly. Grazie :) – Sklivvz Oct 4, 2008 at 9:58

4 Answers

Sorted by: Highest score (default)

10

✓

I have yet to see a licensing scheme that wasn't broken in a few weeks provided there was sufficient interest. Your scheme looks very good (though be certain that if someone really wants to, they'll break it).

Whatever you do, you should follow Eric Sink's advice:

> The goal should simply be to "keep honest people honest". If we go further than this, only two things happen:
>
> 1. We fight a battle we cannot win. Those who want to cheat will succeed.
> 2. We hurt the honest users of our product by making it more difficult to use.

Since you're implementing a license scheme for a program designed for corporate use, you can go even simpler and just keep some kind of id and expiration date along with a simple signature on the client and refuse to start if the license expired or signature failed. It's not that hard to break it, but no licensing scheme is and if you consider your customers honest, this will be more than enough.

Share Improve this answer Follow

edited Oct 4, 2008 at 9:50

answered Oct 4, 2008 at 9:12

Jacek Szymański
2,664 ● 20 ● 15

1

It's not completely clear from your question how your scheme works. Does every instance of the client software have a different key? How long does the license last? Do you have a different key per customer? How is the license paid for? How is a license renewed?

If you are trying to control numbers of usages of the client code then only the first one above will do it.

At the end of the day, in the world you appear to inhabit, I suspect that you are going to have to live in trust that there are no blatant infringements of your license. Most decent sized organisations (which it sounds like your customers would be) have a responsibility not to infringe which can lead them to serious consequences if they break the license agreements. They will be audited on it periodically too and you probably have some statutory rights to go and check their usage (if not you should write it into your license agreement).

Where it becomes very dangerous for you is if the contents of the USB keys find their way onto the web. In that regard any scheme which uses a published key is vulnerable to a wilful disclosure of the secrets.

I'm certain there is a lot of literature on this subject, so it is probably worth you continuing your research.

BTW I'm not sure about your reference to SLAs in the middle part about your server licensing. Licensing and SLAs are very different. A license is the clients obligation an SLA is yours.

Share Improve this answer Follow

answered Oct 4, 2008 at 9:14

Simon
80.6k ● 26 ● 92 ● 119

SLA = Service Level Agreement. – massimogentilini Oct 7, 2008 at 7:11

1

if you give them the private key, what is to prevent them from creating more signed XML files instead of buying additional licenses from you? or is it a site-license? if the latter, what is to prevent them from creating licenses for other people/sites?

in general, development licensing schemes tie the license to a particular machine using the MAC address and/or hard drive serial number, or sometimes just with an activation key (which is usually just a hash of the hardware info)

and typically the encoding is done with a private key that you keep secret, and the license is verified with a public key; the client never has the private key, otherwise they can - if so inclined - generate their own licenses

Share Improve this answer

Follow

answered Oct 4, 2008 at 12:30

Steven A. Lowe

61.1k ● 19 ● 135 ● 204

1

I agree with Steven A. Lowe (I don't have 15 reputation, so I couldn't vote him up).

This also seems too complicated. Do you want it to be unbreakable? you can't. Any sufficiently motivated guru would find a way around it.

Sometimes a simple licensing scheme works best:

I suggest a simple encrypted file that the admin puts somewhere the client can access - it would contain the client name and expiry date. You use the client name from the file in all printed reports (that's what most PHBs care About, that way they would not use the license that prints somebody else's name).

Share Improve this answer

Follow

answered Oct 7, 2008 at 8:04

Osama Al-Maadeed

5,695 ● 5 ● 31 ● 48