# Core - Feature # 22245

| | | | |
|---|---|---|---|
| **Status:** | Resolved | **Priority:** | Should have |
| **Author:** | Bernhard Kraft | **Category:** | Install Tool |
| **Created:** | 2010-03-06 | **Assigned To:** | Nicole Cordes |
| **Updated:** | 2013-10-22 | **Due date:** | |
| **PHP Version:** | 5.4 | | |
| **Complexity:** | | | |
| **Sprint Focus:** | | | |
| **Subject:** | Secure Install Tool Login | | |

**Description**

As we have an rsaauth library now and a service for salted passwords it would make sense to:

1. store the install tool password as salted password instead of md5
this makes it harder for people having read access to localconf.php to use md5 digest for password cracking

2. use RSA for login and password changes so the password or it's md5 sum never gets transmitted directly over the line

3. Add a way to set a new install password without transmitting its md5 value in any direction over the line (so not even display the md5 sum to the admin user going to set the install tool password)

All those issues get solved by the attached patch.
It is hard to separate password salting and RSA from each other, so theres no way to have two patches for each feature ...

greets,
Bernhard

(issue imported from #M13754)

**Related issues:**

| | | |
|---|---|---|
| related to Core - Feature # 50613: Use salted Install Tool password | **Resolved** | **2013-08-01** |
| related to Core - Feature # 21423: Install Tool Password gets transmitted pla... | **Rejected** | **2009-11-02** |

## History

**#1 - 2010-05-07 15:32 - Chris topher**

From Core List:

- Transferring the password using RSA is a good idea, if there is a fallback if RSA does not work.
=> Everyone on Core List considers this the way to go.

- To improve security maybe it is a good idea to store the password SHA-256 encrypted or maybe using saltedpw.
=> There are some concerns. This maybe should be discussed seperately (so it would no longer block the integration of RSA here).

**#2 - 2013-05-18 13:51 - Alexander Opitz**

*- Status changed from New to Needs Feedback*

*- Target version deleted (0)*

The issue is very old, does this issue exists in newer versions of TYPO3 CMS (4.5 or 6.1)?

RSA is integrated, so the point "store the password SHA-256" is open?

**#3 - 2013-05-18 16:21 - Chris topher**

*- Status changed from Needs Feedback to New*

*- Target version set to 6.2.0*

*- TYPO3 Version changed from 4.4 to 6.1*

*- PHP Version changed from 4.3 to 5.4*

Alexander Opitz wrote:

> *RSA is integrated, so the point "store the password SHA-256" is open?*

All the other points are open as well; the Install Tool in fact *still* uses md5 hashes. RSA is *not* used there yet.

**#4 - 2013-05-19 11:04 - Alexander Opitz**

Oh yes right.

**#5 - 2013-07-25 01:38 - Ernesto Baschny**

The patch has to be probably completely rewritten for 6.2 now (due to the new Install Tool), but the main idea is still very much valid and meaninful. I'm adding our security specialist Helmut Hummel as a watcher, maybe he finds some time to work on that?  Or maybe Berhard is still "active" and is willing to contribute a new patch?

Thanks!

**#6 - 2013-07-25 01:38 - Ernesto Baschny**

*- Category set to Install Tool*

**#7 - 2013-08-01 12:04 - Bernhard Kraft**

My schedule is rather full currently. I don't think I can allocate some spare time soon.

The patch is not that complicated. I think the parts which changed in the services class can get applied almost without change. I didn't have a look at the new install tool login mechanism until now.

The trick with this patch is not only that the password gets transfered via RSA encryption but also how someone can set the install tool password: When logging in with a wrong password not an MD5 is shown to the user but rather a "hash-key:REMOTE_IP" value. This value has to get filled into the "ENABLE_INSTALL_TOOL" file. If someone logs into the install tool with the shown hash from the shown REMOTE_IP the RSA transmitted password is accepted and written into localconf.php ...

The only attack vector I know of (except writing localconf.php directly on the server) is to intercept the transmission using a man-in-the-middle attack either over the network or via a trojan horse on the admins client PC. The first case can only get solved by using SSL or similar technology and trusted certificates, for the second case (trojan horse on admin client PC) there is not really a countermeasure except appropriate anti virus software.

**#8 - 2013-09-12 23:26 - Christian Kuhn**

Install tool now uses salted passwords for its password, existing passwords are automatically updated.
Still open is the rsaauth issue. Problems:

- rsaauth relies on database connectivity for key storage and this is not wanted for install tool, key should be stored in install tool session, so rsaauth needs a factory and implementation for different key storage backends.
- rsaauth needs working openssl to be successful
- rsaauth is not a "required" extension and it probably never should be (saltedpasswords is required extension since 6.2 now)

Nicole Cordes is currently working on rsaauth to use it in the install tool ... maybe contact her to get a better feeling on what should / needs to be done?

**#9 - 2013-09-17 23:46 - Nicole Cordes**

*- Assigned To set to Nicole Cordes*
*- TYPO3 Version changed from 6.1 to 6.2*

**#10 - 2013-09-17 23:47 - Nicole Cordes**

*- Status changed from New to Accepted*

**#11 - 2013-10-22 10:32 - Nicole Cordes**

*- Status changed from Accepted to Resolved*

As the install tool now supports salted passwords this issue can be closed. The encryption of the submitted password is not as easy and covered by other tickets.

## Files

| | | | |
|---|---|---|---|
| installToolPassword_secure__v0.diff | 20.7 kB | 2010-03-06 | Administrator Admin |
| installToolPassword_secure__v1.diff | 22.7 kB | 2010-03-06 | Administrator Admin |