Encryption: transparent AND secure?

How transparent is secure encryption allowed to be – which kind of transparency do users require for safely utilizing it?

Hilde v. Waldenfels,
Sales Manager, itWatch GmbH

Nowadays the notion of transparency is used in two ways: On the one hand it denotes "without any input from a user", meaning invisible in the background. On the other hand it implies "with all details laid completely open", in order to make everything visible and foreclose backdoors or concealed channels. Thus, when it comes to the encryption of sensitive data, the question to ask is not only how transparent the encryption should be, but also which group of users need which kind of the above defined transparency, so that the overall procedure leads to the desired level of security.

Examples of prevalent systems for the encryption may serve as an illustration for the importance of the discussion on common available base technologies.

Example 1: The Encryption of Mobile Devices

Let's say, a user puts a presentation on a memory stick – the encryption takes place completely transparent in the background. Now, the user must at least know enough about it, to be able to estimate, if the presentation can be decrypted on the target system, without putting at risk the privacy of other data, especially of those on the same media. We're not talking about a trivial matter, that is shown by potential attacks over USB dumpers, by the requirements for the infrastructure of the third party system when using a PKI, as well as by the understanding of the required privileges for the use of a application or of a driver for the decryption.

Example 2: The Encryption of Hard Disks

Systems for the hard disk encryption differ in many aspects.

A pre-boot authentication procedure with strong authentication can guarantee in the event of an attack – like theft or loss of notebooks -- the security of all those data, that are "unused" in that instance. But after the user's authentication all data on the hard disk and in each started application are available in plain text. That's because the decryption is performed "transparently" in the background. According to Microsoft's estimation more than 50 % of all the threats for PCs and Notebooks stem from running applications, which are infected by malware or have been changed by infected files or through the internet, without somebody noticing anything. So, as soon as the operating system is running, the sensitive data on the disk are not protected anymore.

Then again, there are security solutions available, which encrypt all the data on the hard disk, but all the keys and procedures for the decryption are kept on the disk as well, which in turn makes attacks of the "system at rest" easier. The owner of a notebook should at least know enough about it, to be able to decide, which class of sensitive data can be stored on the device and what kind of physical protection the notebook needs in certain situations.

Moreover the security officer and the system provider have to reach an agreement on the question, if they should leave open backdoors for software distribution and patch management, which in turn would put the complete system at risk. But otherwise would complicate or even get in the way of systems management procedures.

Two issues are obvious: On the one hand the aim "to hide all technology from the user" leads to too big deficiencies in the overall security process. On the other hand, a user, assuming that encryption delivers complete protection, thinks he/she can do without additional security measures. The following example may serve as an illustration for this scenario:

Example 3: Self Encrypting Hardware

Assuming a user stores the most confidential data like information on company acquisitions or HR decisions, on a self encrypting memory stick. In this case, the media with a provable high security level (i.e. CC EAL 4+) holds data for different purposes of use and of different sensitivity. Now, the data decryption is performed "transparently in the background", that is immediately after inserting the media on any system and providing the correct PIN or after authenticating with the fingerprint – also without taking into account which program tries to access the data. While the user assumes, he/she is opening only his/her own files, a background program could be copying all the data from the stick. This can happen because of the transparency of the decryption in plain text without the user being aware of. That kind of malware is called "USB-Dumper, but the principle behind it is to be found in many different patterns of attacks.

Another double-edged challenge regarding the encryption of data is presented during a secure transmission of data into the internet.

Example 4: Encrypted Upload into the Internet

Any user can rent for little money his/her own storage in the internet and use automatic encryption for the access to it. The user now is (mistakenly) assuming the data was safely stored because of the encrypted upload. From a company's perspective encrypted data upload is presenting another challenge: The encrypted data upload can be technically "broken open" in the company's firewall, but in many cases this is illegal, at least in Germany. Hence insider threat or infiltrated malware have the chance to withdraw data, without being found out. Maybe the statistics on the exchanged data volume arouse some suspicion, but they are not enough prove.

Thus, as a protection against industrial espionage in DLP projects, it is recommended to

perform the data check with unencrypted access – that is on the client – and block the upload of encrypted files.
Placing strong authentication at the users free disposal, could turn out to be a bad idea as the next audit shows.

Example 5: Encryption and Long-Term Archiving

Certain kind of data, like those for financial accounting, are subject to mandatory archiving according to GoBS, GoS, FAIT and many more regulations and standards. Compliance to the retention regulations is met, if the archived data over the whole retention period is available in plain text. If data under regulatory retention compliance is stored encrypted, then the information is archived but the legal compliance is not met. Only an appropriate key escrow can offer a solution for this challenge. So, the duty of safeguarding the keys involved AND of the entire decryption process are also part of the regulatory requirements.

In order for the auditor to approve the process, the procedure not only has to be "transparent", but also any use of optional encryption has to be checked for data under regulatory retention duty, so that appropriate action can be initiated.
If a company has invested in licenses, hardware or internal resources for raising the security level, some best practices should be considered:

1. The technical possibilities for using encryption can be provided either
   a. optional or
   b. mandatory – depending on the degree of confidentiality of the content and the storage location (mobile ...).
   c. In some cases they have to be prohibited.
2. The security functionality is to be organized in a way that it is
   a. always available when needed and
   b. the user
      i. not only knows, how to use the encryption but
      ii. it has to be guaranteed, that he/she understands when, where and under which circumstances he/she can decrypt the data.
   c. cancelled when required by legal necessity.
3. The process' security meets in all real usage scenarios the defined security objectives.
4. The possibility of choosing personal keys is not to put additional strain on the help desk.

When talking about the transparency of encryption it should also be mentioned, that the encryption procedure itself has to be disclosed, that is, made transparent, to the IT security officers or executives, and the key usage has to be comprehensible and protected.

Best Practice and Check Lists

Some best practices can make dealing with "transparency" easier, when setting up a project and choosing a solution. Besides, they can provide instructions for secure actions and in setting limits for use cases.

Optional or Mandatory Encryption During Data Transport

Mobile data can present a high risk, because memory sticks easily get lost. In such an event the amended data protection act demands for certain data, stored as plain text on a lost stick, very unpleasant action involving the duty of public information. KonTraG imposes legal liability directly on the board of directors or the executive management.

In most cases users don't keep in mind, that sensitive data need a special treatment. Therefore processes, which in fact hide the optional encryption by providing another button (i.e. secure storing) or a special menu (i.e. context menu with encryption) for optional encryption, are less suitable. A better alternative offer solutions, where the security policy sets encryption as an administrative option to "optional" or "mandatory", depending on the used media and the content to be stored. Given the fact, that there are privileged users,

who can export data as plain text, here the presence of an electronic declaration of intent for the documentation of the liability transfer in real time is recommended.

Several incidents of data loss, like those in call centers, have drawn much attention to the matter. Whenever a company uses termporary staff for operating on the “expensive” company data or on those of customers, the appropriate "scope definition" for the keys can provide the required security for the process. The enterprise keys are not known neither to users nor to administrators, thus offering protection against taking out or selling data. However the keys allow for the exchange of sensitive data in the company or with defined partners and customers.

If a user takes out data, which is encrypted with a personal key or with a PKI, all the required applications should be stored on the data media. In addition the user has to be informed, what a system has to offer and comply to, to be able to safely copy the data on the machine. However, this procedure has some drawbacks: The security awareness activity has to be initiated simultaneously with the use case, should not be repeated too often and the content is not be too complex. Therefore we recommend procedures instead, which don’t place requirements on systems outside the organization.

There are a number of questions to be answered, depending on the trustability of the user groups, the used data and the mobile media, of the communication applications (browser, ftp, mail etc.) as well as of the desired degree of liability:

- How can you keep security awareness in realtime up to date, with respect to the supported usage scenarios and the current legal compliance?
- Should an electronic audit-proof declaration of intent in certain cases overwrite the liability of the executive board according to KonTraG?
- Against what kind of attacks should protection be provided and who could be the attackers?
- How can confidential information, when transparently decrypted, be protected against the access of unentitled applications?
- How can you support the goals of DLP-projects with different key systems? And, if required multi-tenancy enabled for different departments like HR, employee organization or executive level ...
- How can legal and in-house requirements (also cost reduction for the help desk) for archiving and backup/ recovery be implemented by key escrow and availability of the procedures?
- How can you implement the complexity requirement for personal keys in a user friendly manner and without the implication of the help desk?
- How can trivial data, like directions, be excluded from a mandatory encryption, and at the same time be stored alongside the encrypted data for instance on mobile media?
- How can you guarantee, that on the black market a stolen hard disk obtains only the hardware price and no information value is left?
- What is necessary to guarantee, that a user under time pressure doesn’t have to perform extra actions, which he/she possibly forgets about.
- How can backup/recovery for the field service be performed, maybe even decentralized, without putting the confidentiality at risk?
- How can self encrypting techniques be excluded from a mandatory encryption?
- How can special procedures, which don’t accept encrypted content, work together with the encryption process?
- Are the used algorithms, the key escrow and the overall procedure consistent with the intended security level?