Perspectives on the current dilemma for balancing national security and civil ethics

- There is an active debate about the need to find a balance between guaranteeing individual privacy and meeting the demands of national security.
- A novel architecture developed by a UK company enables an innovative and creative solution that addresses both issues.

Cyber security – the need for solutions

Cyber security solutions are required to ensure protection of data against snooping and misuse, whilst also retaining simple and safe access and simultaneously providing support for national security. It is widely accepted that the current infrastructure of the internet does not meet these objectives, in large part because the internet was not designed with security in mind.

A pivotal problem that underpins these difficulties is that of cryptographic key management; how to put the right keys in the hands of the right people in a seamless and yet secure manner. The server-centric approach championed by Scentrics, protected by its patent and implemented in its product portfolio, provides a solution that delivers seamless cross-platform cyber security.

The purpose of this brief document is to provide a description of the motivating problem and to discuss the core ideas behind the Scentrics product portfolio.

Context

This section examines the context within which the Scentrics key management service operates, and establishes the terminology we use throughout this document.

The protocol used to access the Scentrics key management service is designed to enable *users* to make use of cryptographic services on a smart phone, tablet or PC. That is, users wish to be able to make use of cryptographic services on any suitable device (the device currently employed by a user is referred to as the *client*). The main obstacle to achieving such universal access to cryptographic services is ensuring that the user-specific cryptographic keys necessary for performing cryptographic functions are available at every platform.

In the Scentrics system, this is achieved with the aid of a trusted *server*. This server stores a *profile* for each user which it supports, where this profile contains all the security context information for the user (including cryptographic keys, certificates, and any other necessary user-specific information). The server is trusted to maintain the integrity and confidentiality of the profile. Part or all of the profile is transferred to a platform employed by the user, on request by the user (this transfer must take place in such a way that the confidentiality and integrity of the profile is preserved). The recipient platform can then use the profile to perform cryptographic functions for the user.

This profile transfer must take place in such a way that both passive and active interceptors are prevented from learning anything about the profile contents, and/or modifying the profile. This includes interceptors capable of performing so called *man-in-the-middle attacks*, in which an interceptor masquerades as the client to the server and the server to the client.

Of course, the server will need to have some means of authenticating the user before downloading the profile. For the purposes of this system, it is assumed that this will be performed using a secret password shared by the user and the server. However, the system is inherently flexible and can readily be adapted to support a range of means for user authentication.

In the remainder of this document a *session* means a specific period of time while a user is employing a particular client device. That is, the download of profile data will be required to support a session, and, even if a user has a number of sessions using the same client device, a profile download will be required on every occasion.

The client device is not necessarily completely trustworthy. Of course, if the software implementing the protocol has been manipulated then an attacker may be able to obtain a copy of the profile data downloaded to a client. This is a problem inherent to any application performing cryptographic processing on a client device. The likelihood of compromise is minimised in the Scentrics architecture by minimising the time during which keys are held on the client device; moreover, the impact of such a compromise could further be minimised by limiting the lifetime of the secret data that is downloaded to the client (including private and secret keys)[1]. The latter possibility is an inherent advantage of the cloud-based approach to key management. A further protection envisaged in the Scentrics patent portfolio is the use of a trusted execution environment at the client, where available, to perform critical security processing.

[1] The lifetime of a downloaded private key could be limited by requiring the server to generate a new key pair for every session, and choosing a very short validity period (e.g. some small number of hours) for the key pair.

Rationale – the key management problem

A fundamental objective for cyber security is to protect the confidentiality and/or integrity of information, both when it is stored and when it is in transit. The information to be protected could include government or commercial secrets, health records for individuals, financial instruments, e.g. credit card numbers, and a host of types of personal information. The risks associated with a lack of appropriate protection are huge. For example:

- if an unencrypted commercially sensitive email is intercepted, then the potential consequences to the companies involved could be very significant, including potentially serious impacts on share price;
- users often store very sensitive personal information on social networking sites in unprotected form; these sites routinely mine user personal data for purposes which may be damaging to the end user; moreover, such sites do not always delete data promptly, if ever;
- mobile devices are increasingly used for making payments and conducting m-commerce – if the integrity of individual transactions can be attacked then both individuals and payment organisations stand to lose very large sums of money.

Today, the means of communication in widespread use are often inherently insecure (e.g. the public Internet), and data is stored in the cloud on servers located around the world – often we are completely unaware of where our data is located. Routine data collection, generation, processing and management is performed on a wide range of platforms, many of which are inherently mobile (e.g. tablets and smart phones) and hence which can be easily lost or stolen. Against this background, the use of cryptographic techniques, such as encryption and digital signatures, to protect information is absolutely vital. Cryptography can be used to guarantee confidentiality, to enable detection of unauthorised changes, and to guarantee the origin of data. Indeed, cryptography is very widely used today in a huge range of applications, and is fundamental to the correct operation of computers and the Internet.

However, despite its success, there are major impediments to the full deployment of cryptography, especially to protect information managed by individuals. For example, whilst it is in theory possible for users cryptographically to protect sensitive emails so that they can only be read by their intended recipients, in practice this only happens in a small minority of cases. Similarly, whilst it is theoretically possible to use cryptography to protect stored data, the vast majority of individuals store data in the cloud, including on social media sites, completely unprotected.

The obvious question is ‘Why?’ That is, why don’t users avail themselves of the many cryptographic products that exist to protect their data? The reason is clear – it is simply too difficult. The underlying problem is known as key management. Essentially, in order to use cryptography, users must generate secret keys, i.e. secret values (a little like passwords) which must be stored somewhere securely, since if the key is compromised then so is the data.

Ensuring appropriate management and storage of these keys is intrinsically difficult. Firstly, most user computers and phones do not have a secure place to store sensitive data, so that if the device is lost or stolen then the stored keys can be compromised. Secondly, to enable a protected message to be accessed, the appropriate keys somehow need to be transmitted to the recipients in a way that preserves their secrecy and integrity – this is highly problematic. Thirdly, the keys must be stored long term, since if a key is used to encrypt stored data and the key is lost, then the data cannot be decrypted, i.e. it is essentially gone forever. Fourthly, most users employ a

variety of computers, including smart phones, tablets, notebooks and desktops, and if the key is stored on one device then it is typically not possible to access any protected data from another device.

The increasing use of mobile platforms means that any underlying security infrastructure must be lightweight, easily installed, and inherently flexible. Users expect to switch seamlessly between platforms, so, as noted above, solutions involving long-term storage of keys on user devices are almost bound to fail.

These are just some of the many practical barriers to the effective use of cryptography for the individual.

Support for lawful interception

The fact that the Scentrics service is cloud-based enables simple and secure management of keys in accordance with the prevailing legal framework, including lawful access to data. Depending on the laws applying within the jurisdiction in which the service operates, lawful access can be given on a highly granular level to individual keys, e.g. enabling the decryption of individual protected data items or emails sent to or from a specified individual.

That is, the Scentrics technology offers a simple and compelling solution to the lawful key recovery problem, in a way which does not damage user trust. In other solutions in which keys are stored long term on user devices, no such simple solution is available, requiring complex and error-prone key escrow capabilities or building backdoors into cryptographic applications.

About Scentrics

Scentrics is a UK company supported by an academic Technical Innovation Board (TIB) including scientists from leading UK universities in the field who have defined the architecture and deployment strategy for the Scentrics 'core API' and its dependent applications. Scentrics is a cloud-based cryptographic key management system upon which a range of different security applications can be built.

Scentrics currently offers both key management and secure messaging as services via the Cloud. All keys are generated, distributed, revoked and managed at a central server, and not at the client. The client is responsible for use of the keys, e.g. for encryption of messages, so although key management is cloud-based, messaging security is end-to-end. That is, the server does not see and is not required to process individual messages; the solution thus scales because complex computations, such as encryption of individual messages, is distributed to the clients.

The fact that the Scentrics service is cloud-based enables simple and secure management of keys in accordance with the prevailing legal framework, including lawful access to data. Depending on the laws applying within the jurisdiction in which the service operates, lawful access can be given on a highly granular level to individual keys, e.g. enabling the decryption of individual protected data items or emails sent to or from a specified individual.

The server-centric approach championed by Scentrics, protected by its patent and implemented in its product portfolio, provides a solution that delivers seamless cross-platform cyber security.