Secure by Default: Sensitive Data on Consumer Platforms

As the threat from Cyber Space increases, the need to adopt the strategy of ‘Secure by Default’ becomes more urgent. Often in order to make today’s products and services secure, their usability has to be severely reduced. If an enterprise is to operate securely in a connected world, every product, system or service that is procured or deployed should be Secure by Default. It should actually be hard to make them insecure.

Security conscious enterprises (including Government departments) can help shape the marketplace in support of this strategy. We will initially focus on commercial/consumer computing platforms, including laptops, smartphones and tablet devices.

Managing the risks to modern platforms typically involves adding extra controls; requiring user interaction to access sensitive data, or monitoring/limiting use of some features. We reduce the likelihood or impact of a compromise, but in doing so we also reduce usability. Extra controls can also adversely impact application speed and/or device battery life.

An earlier white paper\(^1\) described the desired technical characteristics of secure platforms, and noted that many of those characteristics could be enabled at least to some extent on existing devices. Widespread adoption is not happening because the market demand is perceived to be low.

**How can we create demand for ‘Secure by Default’ technology?**

Simply ‘improving security’ is not sufficient to create commercial demand. We must enable capabilities which are compelling to users and to system managers.

- **Showcase Examples**

Where working examples exist, public demonstrations should be produced to show how real business problems can be solved with security technology. As the supporting software matures, trials can be conducted to ensure usability goals are satisfied.

- **Publish Requirements**

As showcases and trials build awareness, enterprises should be encouraged to publicly state their requirements and use cases for platform security technology.

- **Differentiate: Use Assurance to Show the Difference**

In order to deploy security technology with confidence, independent assurance in the robustness of critical functions is essential. Vendors and customers must collaborate to ensure that components can be certified to an appropriate level without significantly increasing production costs or timescales.

Appendix: Examples

Ideally, a secure platform should allow access to sensitive data/applications as required, but maintain separation between this and other capabilities required by the user. Equally the platform should deliver a user experience consistent with modern expectations of consumer devices. The cost to an enterprise of deploying and managing secure platforms should be minimised.

The following are some examples of where we can demonstrate the improvements described above.

Slick, Integrated Authentication

Users need to securely access a range of services; typically each requires its own authentication credential.

Large numbers of tokens or passwords are unwieldy for users; saving details on disk leaves credentials vulnerable to theft from malware.

We can use a secure key store such as a Trusted Platform Module (TPM) to enable the best of both worlds; authenticate once (e.g. when unlocking the device), and securely store credentials for a range of services.

There may be further opportunities to improve usability by building in physical tamper protection and resistance to brute force attacks in order to allow shorter user passwords. Technologies such as Near Field Communications (NFC) also potentially allow the use of separate physical tokens to exchange authentication data with a device with a single ‘tap’.

Flexible Use of Features and Applications

Users desire access to an increasing range of features and services; some of these present risks to sensitive data on their platforms. For example, social networking applications are designed to allow unconstrained sharing of user data including contact and location information as well as pictures taken on a built-in camera.

Platforms can connect to a variety of peripherals including external screens/projectors, which can themselves request access to data stored on the platform.

Heavily ‘locked down’ devices frustrate users, who subsequently look to work around the restrictions. Risks posed by some applications are difficult to manage.

Strong isolation of sensitive data (e.g. via bare-metal virtualisation, or a Trusted Execution Environment (TEE)) enables a wider range of applications to be used safely on a single device.
Managing Connections from Many Devices and Locations

Administrators of secure networks typically need to be able to control, or at least monitor which devices are connecting to the network. Unknown or unmanaged devices will typically not be granted access to sensitive data.

In addition to reliable identification, the cost and effort required to set up and manage such a system must be kept low.

MAC address-based access control is known to be weak, plus it is inflexible in managing connections from mobile devices. 802.1x-based solutions allow cryptographic authentication of devices, however currently private keys are usually stored on disk by software.

Automating Audit and Control

As well as identifying devices, administrators are also responsible for monitoring the status of devices connecting to the network. Reasons for doing this include the following:

- Monitoring for potential security issues arising from mis-configured or un-patched devices.
- Identifying compromised platforms, arising either from malicious attack or a user attempting to bypass security controls (for example, identifying that a device has been ‘jailbroken’ in order to install arbitrary software).
- Asset management

Clearly it is desirable to automate as much of the above as possible in order to reduce cost, as physical audits are expensive and unlikely to identify configuration issues.
There is value in using software agents to provide more detailed configuration information, however they should be underpinned by strong protection of the underlying environment.

Note also that combining these measures with the isolation mechanisms described above allows a reduction in the level of monitoring required. Applications which are securely isolated from the Secure Platform will not require monitoring.