UK Gov Security Assessment puts Ubuntu in First Place

CESG, the security arm of the UK government that assesses operating systems and software, has published its findings for all 'End User Device' operating systems (OSs). Based at GCHQ, they included OSs for laptops and mobile devices in their assessment, and for uses designated at "OFFICIAL" level in accordance with UK Government Security Classification Policy. This is roughly equivalent to a standard set of best practice security features. Any enterprise would be interested in implementing these to make sure that information is not leaked from their organisation.

The security assessment included the following categories:

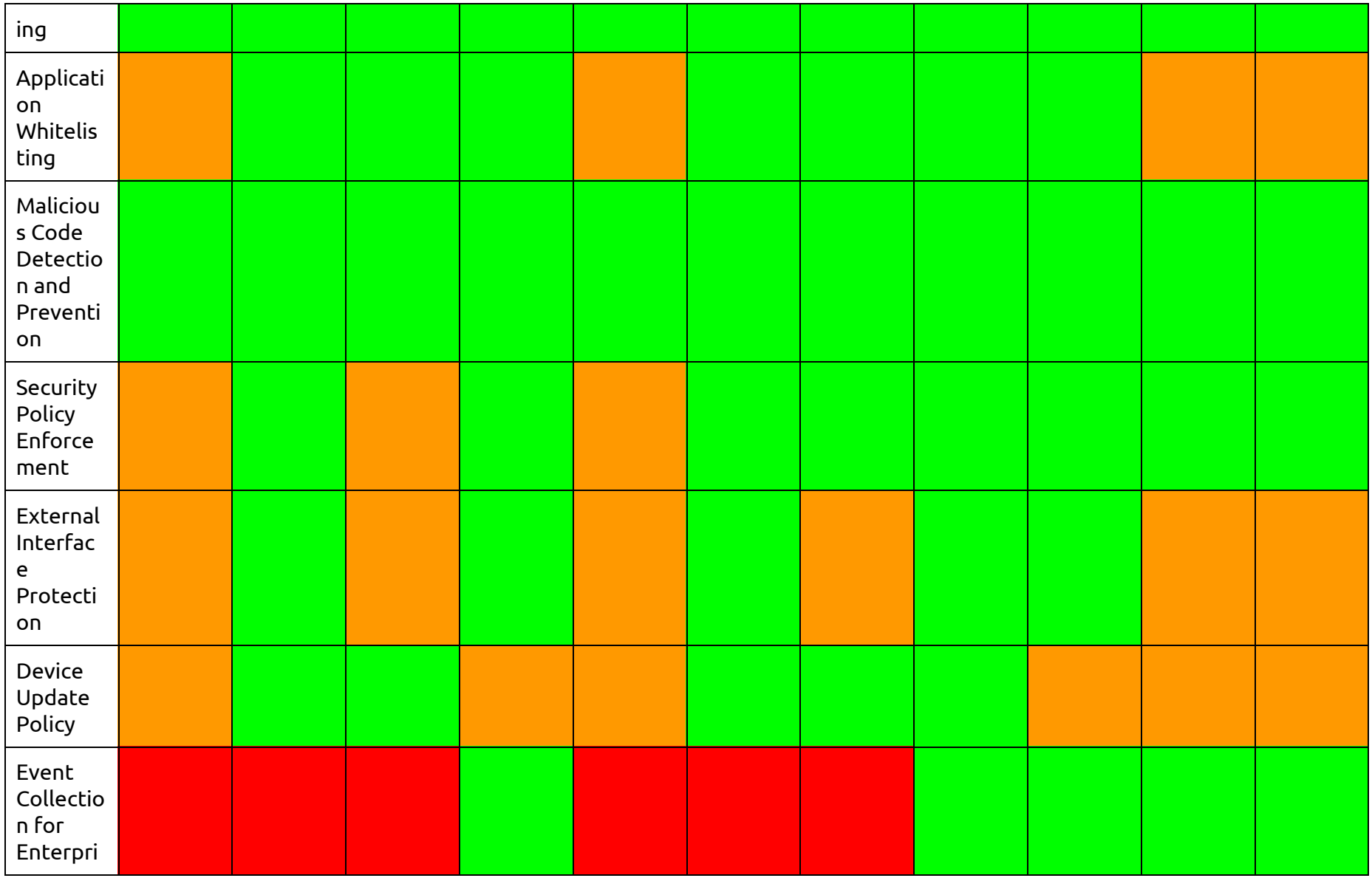
- VPN
- Disk Encryption
- Authentication
- Secure Boot
- Platform Integrity and Application Sandboxing
- Application Whitelisting
- Malicious Code Detection and Prevention
- Security Policy Enforcement
- External Interface Protection
- Device Update Policy
- Event Collection for Enterprise Analysis
- Incident Response

No currently available operating system can meet all of these requirements. Ubuntu however, scores the highest in a direct comparison.

A summary of the assessment is shown below:

Sections that were considered as having a “Significant Risk” are marked below as a red box; sections that have some notes about risks to be aware of are marked in orange; sections that passed the assessment are marked in green.

	Android 4.2 [1]	Samsung Devices with Android 4.2[2]	Apple iOS 6[3]	Apple OSX 10.8 [4]	Blackberry 10.1 (EMM Corporate) [5]	Blackberry 10.1 (EMM Regulated) [6]	Google Chrome OS 26 [7]	Ubuntu 12.04 [8]	Windows 7 and 8 [9]	Windows 8 RT [10]	Windows Phone 8 [11]
VPN											
Disk Encryption											
Authentication											
Secure Boot											
Platform Integrity & Application Sandbox											


ing
Application Whitelisting
Malicious Code Detection and Prevention
Security Policy Enforcement
External Interface Protection
Device Update Policy
Event Collection for Enterpri

-se Analysis											
Incident Response											
GREEN	5	9	7	8	5	9	8	9	8	7	7
ORANGE	6	2	4	4	6	2	3	3	4	4	3
RED	1	1	1	0	1	1	1	0	0	1	2

As you can see from the table the only OS that passes as many as 9 requirements without any “Significant Risks” as independently assessed by CESG is Ubuntu 12.04 LTS.

So, what about the 3 sections that have comments: VPN, Disk Encryption and Secure Boot?

VPN

The comments made by CESG were that “The built-in VPN has not been independently assured to Foundation Grade.” This means that the software *does* meet all the technical requirements of security to pass the assessment, but that the software itself has not been independently assessed to make sure that it hasn’t been tampered with during the development process.

You can also see from the comments made on each detailed assessment that nobody meets this requirement fully at this time. The best you can hope for is technical compliance with independent assessment pending, which is the case for Ubuntu 12.04 or independent assessment complete but missing technical features, like Windows 8, for example.

The independent assessment work for Ubuntu is being carried out by a partner and we expect CESG to provide additional guidance for meeting this requirement fully, in due course. We expect that this will be also available in time for the upcoming release of Ubuntu

14.04 LTS and if so we expect to fully meet this requirement in this release.

Disk Encryption

Disk encryption is a similar case to the VPN assessment.
For Ubuntu 12.04, CESG states:

“LUKS and dm-crypt have not been independently assured to Foundation Grade.”

LUKS and dm-crypt are used on Ubuntu to encrypt the data on the hard disk and to decrypt the data when starting up, by requesting a password from the user. Without the password, the computer cannot start the operating system or access any of the data.

The technical requirements are all met, but the software has not been through an independent assessment to prove that it has not been tampered with in development. So, the independent assessment still needs to be done for LUKS and dm-crypt on Ubuntu to pass this requirement.

However, every other operating system on the list has also yet to pass an independent assessment, but Ubuntu meets all the technical requirements already and we just need a sponsor to put the software through the assessment process.

Secure Boot

Secure boot is a Microsoft technology invented in co-operation with OEMs to ensure that software cannot be tampered with after the hardware has been shipped from the factory. It has provoked much debate in security circles, as the ability to install any software which you can control is desirable from a security perspective. The German government recently criticised secure boot [12] as preventing installation of specialised secure operating systems after sale of hardware.

Ubuntu’s response, from Ubuntu 12.10 onwards is to adopt Grub2 as the default bootloader, with support for Secure Boot, but with an ability to turn off secure boot to modify the OS, if required. This is explained in John Melamut’s blog post here [13]. We believe this

gives users and enterprises the best compromise between security and ability to customise after sale.

Summary

All in all Ubuntu 12.04 LTS stacks up as the most secure of the current desktop and mobile operating systems. Supported by Canonical with free security updates for 5 years, and without malware problems, it's hard to beat in official public sector applications.
We are working hard to close the gap and make Ubuntu clearly stand out as the most trustworthy operating system for the future and we hope to make excellent progress before our next LTS release in April 2014, 14.04 LTS, which will be even better.

Darryl Weaver
Sales Engineer, EMEA,
Canonical

Further Reading

The original CESG guidance is available to read here:
https://www.gov.uk/government/collections/end-user-devices-security-guidance--2

References

[1] https://www.gov.uk/government/publications/end-user-devices-security-guidance-android-42
[2] https://www.gov.uk/government/publications/end-user-devices-security-guidance-samsung-devices-with-android-42
[3] https://www.gov.uk/government/publications/end-user-devices-security-guidance-apple-ios-6
[4] https://www.gov.uk/government/publications/end-user-devices-security-guidance-apple-os-x-108
[5] https://www.gov.uk/government/publications/end-user-devices-security-guidance-blackberry-101-emm-corporate
[6] https://www.gov.uk/government/publications/end-user-devices-security-guidance-blackberry-101-emm-regulated
[7] https://www.gov.uk/government/publications/end-user-devices-security-guidance-google-chrome-os-26
[8] https://www.gov.uk/government/publications/end-user-devices-security-guidance-ubuntu-1204
[9] https://www.gov.uk/government/publications/end-user-devices-security-guidance-windows-7-and-windows-8
[10] https://www.gov.uk/government/publications/end-user-devices-security-guidance-windows-8-rt
[11] https://www.gov.uk/government/publications/end-user-devices-security-guidance-windows-phone-8
[12] http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/trusted_computing_eng.html

[13] http://blog.canonical.com/2012/09/20/quetzal-is-taking-flight-update-on-ubuntu-secure-boot-plans/