G/On OS Security Model

Technical Whitepaper with Excitor comments on CESG Guidance

G/On OS 21

Document revision 1.1

2015-07-03

About this document

This document describes the security properties of G/On OS, which is a linux based, client side operating system designed specifically for running the G/On client

If you do not find the information you need in this document, you may want to look in the other documents in the G/On software documentation suite:

http://www.giritech.com/int/Support-Download/Product-Download/G-On-5.7-Product-Download

© Giritech A/S, 2015
Spotorno Allé 12
2630 Taastrup
Denmark

Legal Notice
Giritech reserves the right to change the information contained in this document without prior notice. Giritech® and G/On™ are trademarks and registered trademarks of Giritech A/S. Giritech A/S is a privately held company registered in Denmark. Giritech's core intellectual property currently includes the patented systems and methods known as EMCADS™. Other product names and brands used herein are the sole property of their owners. Unauthorized copying, editing, and distribution of this document is prohibited.

Contents

Introduction

G/On OS is a client-side operating system, which is tailored for one specific task: providing a secure environment in which to run the G/On client, thereby giving the user secure access to corporate, server side resources.

G/On OS can be placed on a G/On Token, and PCs and Macs can then be booted with G/On OS, from the G/On Token. Once booted, G/On OS will start the G/On client, which is included in G/On OS, and the client will then connect to the G/On Gateway Server that provides and controls access to the server side resources.

In the following three sections, we first describe the G/On client-server architecture and the most important security properties of this architecture. Then we describe G/On OS and its role and security properties. Finally, we provides a context for understanding and evaluating the risks mentioned in a separate security guidance document for G/On OS, published by the CESG, the National Technical Authority for Information Assurance within the UK.

The G/On Client-Server Architecture

In this section, a brief introduction to the G/On client-server architecture and security properties is presented, in order to provide a basis for understanding the role of G/On OS. G/On is a client-server system for secure access to central services provided by application servers, remote desktop servers (terminal servers), etc.

The G/On Gateway Server is placed in the security perimeter around the minimal, central set of servers and protects them by giving *the right users the right access to the right services under the right circumstances*. The most important features are:

- **Two factor authentication:** The G/On Gateway server authenticates users with two-factor authentication: memorized password and a physical token.
- **Strictly enforced access policies:** The G/On Gateway server enforces policies that define which server side services (applications) a user is authorized to use.
- **Server network isolation:** The G/On Gateway server separates the application client connection from the application server connection, so all communication between the

application client and application server is carried out by proxies with protocol validation capabilities. The G/On Gateway can only make connections, which have been explicitly permitted in its configuration.

The G/On Client runs on the client PC, in the G/On OS operating system booted from a G/On Token[1]. The client guides and helps the user to behave securely and follow policies. The most important features are:

- **Authentication of the server and setup of encrypted communication:** The client contacts the server and they perform a secure key exchange, in order to set up an encrypted G/On connection. As part of the key exchange, the client challenges the server to prove its identity by public key cryptography.
- **Limited client side access:** When the user requests access to a central application, which he/she has been granted access to, the G/On client and G/On gateway server collaborate to establish a connection from the PC to the central application server, through the encrypted channel. The G/On server then instructs the G/On client to start an appropriate application client (e.g. a remote desktop client), and the G/On client can also be instructed to only accept and forward communication from this client program through the established connection.

For details about the G/On Security Model, see separate white paper.

G/On OS

The purpose of G/On OS is to make it very easy for the user to stay secure while accessing corporate data with the G/On client – without having to use a corporately managed PC:

- G/On OS guides and helps the user to behave securely and follow policies
- G/On OS protects the user, and helps the user stay secure

Technically, G/On OS is a Linux based OS that can be placed on a G/On Token, and used for booting the client side PC. If an unmanaged PC was booted with an OS from the local hard disk, it

1 The G/On client also exists in versions that can run in the Windows and Mac OS X operating systems.

would get an unknown security posture. But when the PC is booted with G/On OS, it will use a known OS that the user can trust.

The most important security characteristics of G/On OS are:

- **Limited external attack surface**
  The firewall in G/On OS restricts outgoing connections to a bare minimum, and allows no incoming connections.
- **Limited internal complexity and attack surface**
  G/On OS is a minimal Linux OS with just a few applications installed, and with no mechanism for persisting changes to the Linux OS that might be made during its use, except a few selected configuration settings that may optionally be allowed to be stored.
- **Does not use the OS installed on the hard disk of the PC**
  Leaves no traces on the hard disk
  G/On OS runs in “diskless” mode: it has no access to the hard disk of the PC.

In the following two subsections, we present more details of the security features of G/On OS and discuss the security thinking around G/On OS, compared to the “standard” PC security thinking.

G/On OS Security Features

Firewall Locked Down

The firewall settings allow no incoming connections from the outside. And outgoing connections are only allowed to the G/On server – with the exception of the sandboxed Firefox browser mentioned in the following, which can optionally be allowed to access other sites, for signing in to Wi-Fi access points.

Sandboxed Firefox, for Logon to Access Points (Optional)

A special, sandboxed version of Firefox is included in G/On OS, and can optionally be made available for the user through an icon on the desktop. The outgoing firewall settings for the sandboxed Firefox are relaxed when the G/On client is not running, so the sandboxed Firefox can be used for logging in to WiFi hotspots and hotel access points that have web based login pages. The sandboxed Firefox runs in a process with SELinux restricted privileges, so it cannot access the USB drive or any data and also cannot access the local loopback network connector. When the

G/On client is running, the sandboxed Firefox is blocked from making outgoing connections, by the firewall.

Fixed, Minimal OS

G/On OS is a minimal Linux OS with just a few applications installed, including a Firefox browser, and clients for remote desktop, Citrix, and FTP. The Firefox browser is a separate instance, from the sandboxed Firefox mentioned above. There is no Linux GUI for starting these applications, but they may be started by menu items in the G/On Client, for which the user has been authorized. Also, there is no GUI for installing software, and no general mechanism for persisting changes to the Linux OS, that might be made during its use. The only exceptions regarding persistence of OS changes and data are:

1. G/On OS can be configured to allow storing of printer settings on the G/On token (optional)
2. G/On OS can be configured to allow storing of Wi-Fi passwords on the G/On token (optional)
3. G/On OS can be configured to store boot information in a text log for troubleshooting purposes (optional)

No Access to Hard Disks

G/On OS runs in RAM, without using the hard disks of the PC, and without making the hard disks accessible to the user or programs. This ensures that G/On OS cannot be affected by possible malware on the hard disks and it also ensures that no data can be written to the hard disks from G/On OS – neither application data nor system data (configurations, swap file, etc).

Automatic Shutdown on Token Removal

If you remove the G/On Token from which G/On OS was booted, G/On OS will automatically shut down and power off the PC

Automatic Shutdown when Inactive (Optional)

When the PC has not been used for a specified amount of time, the screen fades slowly over one minute before automatic shutting down and powering off the PC. This feature is configurable.

Automatic Disconnect and close Applications when Inactive (Optional)

When there has been no communication between the G/On Client and G/On gateway server for a specified amount of time, the G/On gateway server will terminate the connection. When the connection is terminated, the G/On client will close the application clients that it may have started during the session and then it will terminate. This feature is configurable.[2]

No tty Consoles

The usual linux text based consoles have been disabled.

OS Identification

The G/On OS includes an identification, which can be read by the G/On client, transmitted to the G/On Gateway Server, and used in authorization policies (zone rules). So it is possible to authorize access to an application, only if this identification code is present.

Standard PC Security Thinking and G/On OS

The standard way of thinking about PC security is very much influenced by the fact that PCs are mostly running Windows, allowing programs to be installed from arbitrary sources, allowing users to connect to arbitrary internet sites and allowing users to copy and store data any way they desire. As a consequence, these devices have huge attack surfaces, vulnerabilities are continuously being discovered and exploited and numerous possibilities for users to behave insecurely are prominently available in the user interface.

With this state of affairs, corporate IT security dogmas such as the following have evolved:

1. Include PCs inside the security perimeter and
2. Own and control the PCs and implement configurations and limitations and as many as possible of the security mechanisms that have evolved over the years for increasing the security of the Windows PC and
3. Do not trust users but treat them as adversaries in all matters of security

2 This is a general G/On feature, also available when using other client operating systems than G/On OS

In contrast to this, G/On OS is designed very differently from a standard PC operating system: G/On OS is a Linux based operating system with a fixed, minimum set of programs, with a very limited GUI, and by default with no options for persisting application data and no options for connecting to anything, except a G/On Gateway to the corporate servers. As a consequence, PCs running G/On OS have a very small attack surface, and no options for users to behave insecurely are prominent in the GUI. These properties motivate a quite different set of dogmas:

A. Put the PC outside the main security perimeter. Even if an attack on G/On OS should succeed, there is not much of value on a G/On OS PC and access to the services inside the perimeter is guarded by the G/On Gateway server.

B. Reconsider the cost/benefit of the security mechanisms, which are normally regarded as highly desirable, or even mandatory, in traditional PC deployments. The reduced attack surface of G/On OS and the fact that Linux is a much less frequent target of attacks than Windows changes the cost/benefit analysis. The improvement in security gained by implementing mechanisms such as anti-virus, frequent automatic security patching, and trusted booting may not be worth the cost of maintenance, operation and lost user productivity and the increased complexity of the software.

C. Most employees will not deliberately behave insecurely. With the help and guidance that G/On OS gives users, they can be trusted to not inadvertently behave in an insecure way.

Item C may prompt the question whether we could/should lock down the systems to also protect against possible employees with malicious intent. This question is discussed in the following.

”Locking Down” or ”Fencing Off”?

G/On OS is booted in a way, which is different from booting a traditional corporate PC. And this enables a deployment, which is a lot less expensive. However, this difference in the booting process makes it impossible to completely lock down the PC. This is explained more in detail in the following, and it is argued that operating systems like G/On OS therefore must be designed with the goal of guiding, helping and protecting the well intentioned user rather than aiming for the unattainable goal of preventing attacks from skilled, malicious, determined users.

With corporately owned and managed PCs, it is possible to effectively prevent even malicious users from making undesired modifications: the hardware can be protected with padlocks, the BIOS can be protected with passwords and configured to disallow booting from user controlled media and set up with keys for verifying the integrity of the OS. Also, the OS can be protected with

user access control, domain policies, etc. This is usually referred to as “Locking Down” the PC.

In the typical, low cost G/On OS usage scenario, the user controls the booting. So the user can in principle choose to boot any OS.[3] And since the G/On OS token must be readable by any PC even before it is booted or connected to any network, there is no way to prevent a skilled, malicious user from attempting to dissect it in a lab and making a modified copy, to be used for booting in order to try and circumvent the restrictions. Note, however, that even if a malicious user makes changes to G/On OS, there is little to be gained – he/she still has no better access to the central resources than before, because the central resources are protected by the G/On Gateway.

So, instead of focussing on the malicious user, it makes more sense to focus on guiding, helping and protecting the well intentioned user, for instance by removing unnecessary functionality from the graphical UI, and providing secure, predefined firewall settings and blocking the saving of user data and OS changes. This can be thought of as “Fencing off” unnecessary functionality so the well intentioned user is naturally helped and guided towards secure behavior.

With this description of the security features and security model of both G/On and G/On OS, we have provided a background for the last section in this document.

Comments on the CESG Security Guidance for G/On OS

CESG has issued an End User Security Guidance regarding G/On OS 19.3. In this document, the G/On OS platform has been assessed against each of the twelve CESG security recommendations, and for each recommendation, if there is something that the risk owners should be aware of, this is explained in a short note. Notes marked [!] represent a more significant risk.

3 With PC BIOSes that support trusted booting, it would in principle be possible to use pre-installed Microsoft keys, in order to verify the integrity of G/On OS. But this provides no real assurance, as any OS image can be signed so it is accepted by the Microsoft keys. Alternatively, it would be possible to install G/On specific keys. However, this would require manual configuration of the BIOS, which is impractical for a user to do, so it could only be done with corporately owned and configured PCs.

In the following, each of the notes from the CESG document is supplemented with Excitor comments that provides additional context for understanding and evaluating the risks mentioned in the CESG notes.

Recommendation 1 – Assured data-in-transit protection

CESG Note regarding Risks: [!] G/On uses a proprietary protocol for connectivity between G/On clients and the G/On gateway. This has not been independently assured to Foundation Grade.

Excitor Comment: The G/On protocol has been accepted for use by many government agencies, in European and North American countries. References can be provided.

Recommendation 2 – Assured data-at-rest protection

CESG Note regarding Risks: Nothing noted.

Recommendation 3 – Authentication

CESG Note regarding Risks: End users do not authenticate to the G/On client. G/On OS does not have a screen lock.

Excitor Comment: This is by design, because the use of G/On OS in itself does not give access to anything (no application programs, no persisted data). Access to applications is only possible after login to the G/On Client. In situations where the user would have activated a screen lock, we recommend that the user exits the G/On client. This will close the connection to the G/On server thereby preventing access to the application servers, and (with proper configuration) the G/On client will also close all the application windows displaying application data on the screen. When wanting to work with the applications again, the user can quickly start and log in to the G/On client, which can be configured to automatically launch e.g. a remote desktop, that has kept the state it was in when the G/On client was exited. The user experience is close to that of using a screen lock, and it can be argued that it is more secure than a screen lock, because the attack surface of the G/On Gateway server is smaller that the attack surface of a PC to which the attacker has physical access.

Recommendation 4 – Secure boot

CESG Note regarding Risks: Secure boot is not fully supported on this platform.

Excitor Comment: It would be possible for the G/On OS boot process to use Microsoft keys that are pre-installed in the BIOS of newer PCs, in order to verify the integrity of G/On OS. But the Microsoft keys provide no real assurance, as it is easy for any attacker to make an operating system image that will be accepted by the Microsoft keys. Alternatively, it would in principle be possible to install G/On specific keys in the BIOS that could enable a reliable verification of the integrity of G/On OS. However, this requires manual configuration of the BIOS, and it can be argued that the potential security gain is too small, compared with the cost.

Recommendation 5 – Platform integrity and application sandboxing

CESG Note regarding Risks: [!] There is no integrity protection of files on the USB token.

Excitor Comment: Procedural controls are recommended to protect USB tokens and prevent end users inserting them into untrusted or malicious devices.

Recommendation 6 – Application whitelisting

CESG Note regarding Risks: Users can run applications from unapproved sources.

Excitor Comment: With G/On OS, the main use case is access to internal systems and G/On OS will disallow browser access to all sites except the ones that are defined in whitelists when configuring the G/On system. We recommend that the whitelists only contain trusted sites. If general browsing on the internet is a requirement for a G/On OS user, we recommend that this is enabled by letting the user connect by remote desktop client to a fully patched remote desktop server, on which a browser can then be used.

Moreover, in G/On OS the user process cannot execute programs on the G/On OS USB token, and mounting of additional storage devices is disabled by default.

With this setup, it can be argued that there will not be any executable files from unapproved sources, accessible for the users to start from within G/On OS.

Recommendation 7 – Malicious code detection and prevention

CESG Note regarding Risks: There is no malicious code detection.

Excitor Comment: Use of antivirus programs has become the norm for Windows based PCs, where the user can browse to possibly malicious internet sites.

However, very little Linux malware exists in the wild.

Moreover, with G/On OS, the main use case is access to internal systems and G/On OS will disallow access to all sites except the ones that are defined in whitelists when configuring the G/On system. We recommend that the whitelists only contain trusted sites. If general browsing on the internet is a requirement for a G/On OS user, we recommend that this is enabled by letting the user connect by remote desktop client to a fully patched remote desktop server, on which a browser can then be used.

With this setup, it can be argued that the potential security improvement gained by installing and maintaining antivirus in G/On OS is too small, compared with the cost.

Recommendation 8 – Security policy enforcement

CESG Note regarding Risks: Users can bypass some locally-configured policies.

Excitor Comment: Procedural controls are recommended to prevent user modification of the firewall rules and security policies configured in the G/On OS configuration file.

Recommendation 9 – External interface protection

CESG Note regarding Risks: Nothing noted.

Recommendation 10 – Device update policy

CESG Note regarding Risks: [!] Patches and updates for G/On OS are not released regularly. Administrators need possession of USB tokens to apply these.

Excitor Comment: Regular patching of security vulnerabilities has become the norm for general purpose client side operating systems, where the user can browse to possibly malicious internet sites. However, with G/On OS, the main use case is access to internal systems and G/On OS will disallow access to all sites except the ones that are defined in whitelists when configuring the G/On system. We recommend that the whitelists only contain trusted sites. If general browsing on the

internet is a requirement for a G/On OS user, we recommend that this is enabled by letting the user connect by remote desktop client to a fully patched remote desktop server, on which a browser can then be used. In this setup, it can be argued that the potential security improvement gained by frequent patching is too small, compared with the cost in terms of the potential instability and loss of user productivity.

Recommendation 11 – Event collection for enterprise analysis

CESG Note regarding Risks: [!] There is no facility for collecting logs remotely from a device, forensic log information is not persistent.

Excitor Comment: There are no actions with potential security implications that can happen on the device, except when it is used for logging in to G/On, which is registered in an access log on the G/On Gateway server. More specifically: There are no data that can be accessed, and there are no settings that can be changed, and no programs that can be installed, so it can be argued that there is nothing interesting, which can be logged on the device.

Recommendation 12 – Incident response

CESG Note regarding Risks: Nothing noted.