White Paper

General Public Use

G/On

Secure by Design

Version 6.0

Make Connectivity Easy

1. Scope

This document describes how security is implemented by design in the G/On solution based on our patented EMCADS™ technology.

2. Product Protection

2.1. Monolithic Programming

Monolithic programming is a style of programming where all the code ends up being one executable. This eliminates the need for DLL files or any other dependency on external files for the core functionality of the executable. Monolithic programming removes the need to have control of DLL's and other files, such as checksums or other means of authenticating the code to be real.

Many exploits are based on replacing DLL's with Trojans that seem to perform the correct actions, but also performs whatever the hidden intention the Trojan was designed for. Monolithic programming effectively removes the ability to replace a DLL or to hook into the dataflow between the executable and the DLL.

2.2. Windows Memory Manager

In order to eliminate the risk from the overwhelming amount of buffer overflow exploits targeted specifically at the Windows Operating System, EMCADS™ does NOT rely on the Windows Memory Manager. Instead, allocation of memory for stack and buffers is handled by Borland's memory manager ensuring complete control of memory management within the executable.

2.3. Encryption of Executables

The executables are bundled together with DLL and data files. The resulting executable is compressed and encrypted, protecting the code from being abused, reverse engineered, or tampered with in any other way. The encryption tools used are capable of detecting tampering from debuggers, and will exit upon such tampering.

3. Encryption Schemes

3.1. Elliptic Curve Cryptography (ECC)

EMCADS™ uses 163-bit ECC for the signing key-pair between the G/On Server and the G/On USB and G/On Desktop clients. 163-bit ECC is also used for the secure key exchange and for transferring the Client Identity Facility (CIF).

Once the session establishment is completed, the ECC keys are destroyed and never used again.

For more information on ECC, please see: http://en.wikipedia.org/wiki/Elliptic_curve_cryptography

3.2. Advanced Encryption Standard (AES)

G/On uses 256-bit AES for payload encryption. AES provides a fast symmetric encryption on even slow devices, enabling near bandwidth throughput. G/On uses separate AES keys for upstream and downstream data making it even harder to break the encryption. Once a session terminates the AES keys are destroyed and never used again.

For more information on AES, please see: http://en.wikipedia.org/wiki/AES

3.3. Hashing

After the datagram have been encrypted, it may be divided into smaller segments of up to 1300 bytes, in an attempt to eliminate packet fragmentation at the network layer and avoid the overhead

The data packets are hashed using SHA-1, ensuring that data is not tampered with during transmission.

For more information on SHA-1, please see: http://en.wikipedia.org/wiki/SHA-1

4. Two-factor authentication

4.1. The Identity File

When the G/On Server is installed and configured, a unique file, named the identity file, is created. This file contains information unique to the G/On installation, and the identity file is what gives the G/On USB and G/On Desktop clients the ability to connect to the G/On Server. The identity file is encrypted during creation, and can safely be distributed to the clients by electronic means.

The initial connection happens when the G/On USB or G/ON Desktop clients is first launched. The client decrypts the identity file to get the IP name/address of the G/On Server to contact. The client contacts the server on 3945/tcp (IANA default – can be reconfigured to the tcp port of your choice), the server responds with a greeting, and the secure key exchange (SKE) process starts.

4.2. Secure Key Exchange (SKE)

A greeting with a per-session public ECC key and a signature is sent from the server. Only a client with an identity file created by this server can validate the signature of the public key. This is the basis for the mutual authentication, ensuring the server and client is configured for each other. The client responds to the challenge with the client identity facility (CIF).

If the client is unable to present the correct response, the TCP connection is terminated immediately. This is also the response to connection attempt from anything that isn't a proper client, i.e. telnet to port 3945/tcp on the server.

4.3. Client Identity Facility (CIF)

The Client Identity Facility (CIF) contains the EMCADS™ Data Carrier (EDC) serial number which is either the unique serial number burned on the G/On USB key, or the unique hard disk firmware serial number of the device G/On Desktop was installed on. The CIF also contains a large number of identifiers from the device G/On is being executed on, such as:

- EDC Serial Number
- Device Volume Label
- Device Volume Serial
- EDC Manufacturer
- EDC Media Class
- EDC Interface
- EDC Class
- EDC Firmware
- Public IP Address
- Source Network
- Client Hash
- Client Version
- Machine Name
- Machine Domain
- Host Operating System (OS)
- OS Major Number
- OS Minor Number
- Host Class
- Primary MAC Address

All this information can be used to identify the device during adoption, to place the client in the correct global zone, and even match the device to a specific rule. This is the first part of the two-factor authentication.

The CIF also contains the chosen payload encryption method, which is currently 256-bit AES. As better encryption methods are developed, these can be included in the EMCADS™ technology.

4.4. Global Zones

Global Zones can be thought of in many different ways, depending on what your security policy states. G/On comes with three default zones, Inside, Outside and Unknown. These zones could also be called Trusted, Limited Trust, and Untrusted. The basic idea of the Global Zones is to allow you to decide what a user is allowed to access based on geographical location and the type of device used to connect.

4.5. Rules

Rules allow you to:

- permit a device
- deny a device
- assign a device to a Zone

based on the on what is know about the device from the CIF.

4.6. Login Dialog

The login dialog is the second part of the two-factor authentication. Once the device is authenticated, then the user must enter userid and password to be authenticated. The user can be locked to the device, the device can be locked to the user, or the user and device can be locked to each other.

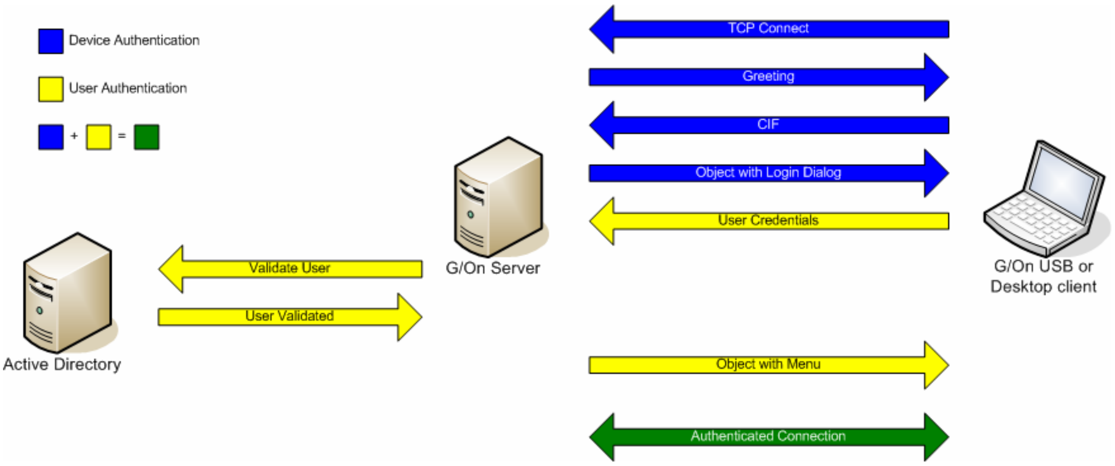
The user can be authenticated at the Active Directory (AD), eliminating the need to store password on the G/On Server. When the user is authenticated, and the user is matched to the EDC, the 2-factor authentication process is complete, and the user is presented a menu of applications based on zones, groups and userid.

The login dialog contains a number of features to prevent brute-force attacks.

- Failed Logins: 0 - 25, 0 = none, default = 5
- Display login dialog randomly on screen, default = off
- Prevent TAB navigation, default = on
- Make “Cancel” default button, default = on
- Allow users to use On-Screen-Keyboard (OSK) login, default = off
- Automatically invoke OSK, default = off, on = force OSK use
- Disconnect on Screen Saver Activation

What combination you chose to use, will be based on your security policy, and the level of hostility in the environment, in which you are deploying G/On.

4.7. Two-factor Authentication Process

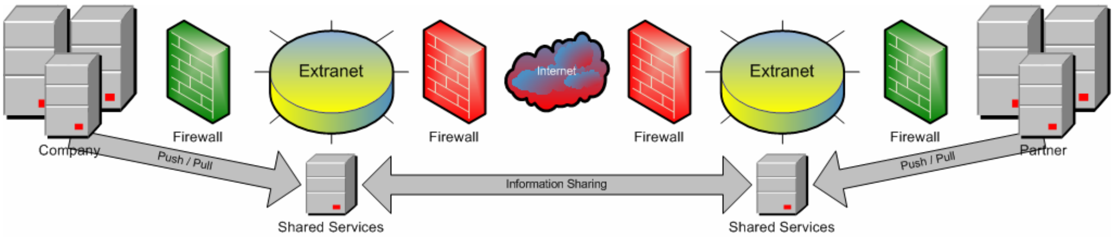


5. Application vs. Network Access

5.1. Network to Network Connectivity

Connecting two networks that are subject to the same security policy, under the administration of one IT department, using the same equipment, and funded by the same organization, is a business-as-usual process, and something that is a part of everyday business. Network to network connectivity is the normal way of attaching remote offices to headquarters, allowing the remote office access to applications and data at the central site.

The challenge arises with dislike networks need to be connected, like connecting a partner, vendor or customer to your network. Often security policies will be different, equipment will be incompatible, and the organizations will have different ways of handling IT in general. This causes the process of connecting the networks to be cumbersome, and will often result in a reduced functionality compared to the original intent of the connectivity venture.



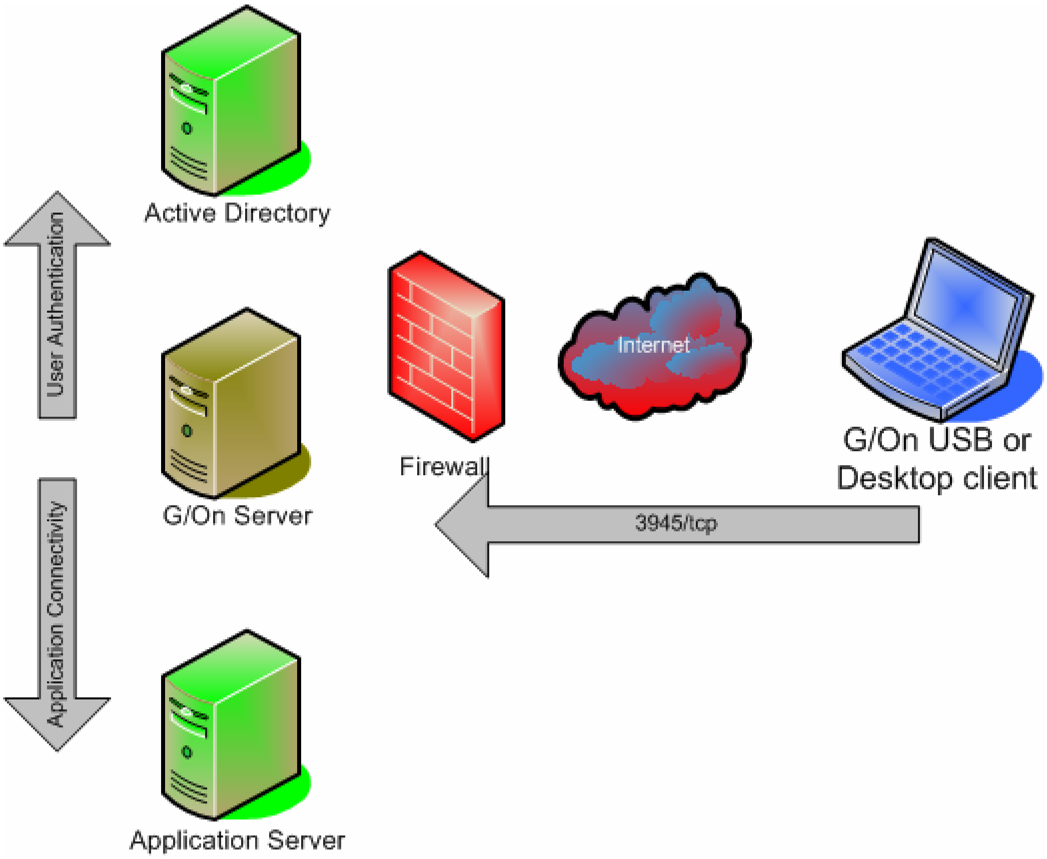
5.2. Application Connectivity

Application connectivity presents a whole new way of connecting partners, vendors, customers, or any other entity you wish to extend your business to. Application connectivity eliminates network to network connectivity, because the client PC connects to one server and this server provides the connectivity to the application servers. G/On is just such a solution, placing the G/On Server on the internal network, effectively eliminating the additional cost for VPN/SSL-VPN, tokens, certificates, extranets, portals, webifying applications, and all other technologies used today to give remote access. The client PC never becomes part of the internal network, and therefore reduces the ability of spreading virus, trojans, worms or other malware to a near impossibility.

G/On also reduces the amount of ports needed to be open in the firewall, to one single TCP port (default 3945/tcp, but can be configured to the tcp port of your choice). This is not only a factor in security, but also effectively reduces network traffic, by eliminating broadcast and network chatter between devices attached to the network.

Connecting to an application, instead of the network, effectively removes the need to negotiate security policies, equipment incompatibilities, and the splitting of cost. Instead you become a service provider, and your partner, vendor, or customer becomes a user of the service you provide.

With Global Zones, Group membership in the AD and UserID, you can tailor the applications presented to the user based on the level of trust you have for the user and the device the user is connecting from.



For more information on server placement, please refer to the Giritech Basic Best Practice Reference available in the G/On Admin Guide, and also available as a separate document.

5.3. Lock to Process

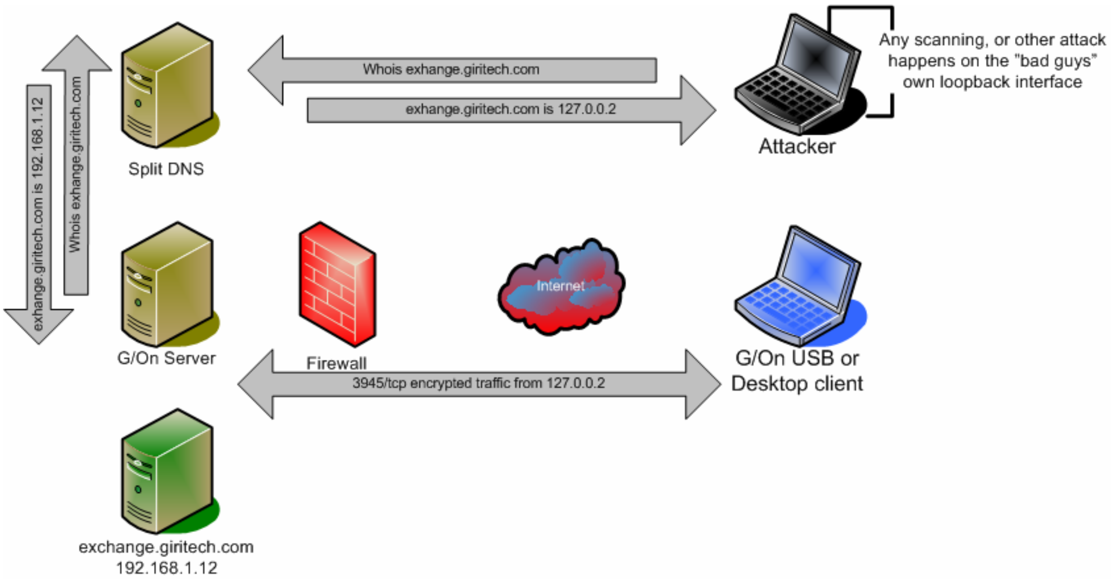
LockToProcess is the ability to only allow the application launched from the G/On menu, to send data through the Loopback interface. The way this works is when an application is launched, a web browser for instance, then the configuration contains information about what port and protocol the application uses. G/On opens a socket on Loopback interface which listens on the correct port, so for a web browser this would be TCP port 80 on IP address 127.0.0.2 (127.0.0.2:80). The process ID of the web browser is then locked to the socket and only this process ID will be capable of sending data to this socket. If another process tries to send data, like a virus or a trojan, the data is simply ignored by G/On.

5.4. The Loopback Interface & Split DNS

The port 3945/tcp connection between the G/On Server and G/On USB or Desktop client is linked to the loopback interface of the client, specifically 127.0.0.2. The Socket Gateway, which is part of the G/On clients, opens a socket for the used port, i.e. 127.0.0.2:80 for http traffic. All data sent to an established socket on 127.0.0.2 will be encrypted and sent through the port 3945/tcp to the server.

Split DNS is used in cases where the server sends a redirect from 127.0.0.2 to an actual hostname. On the inside, the hostname will resolve to the right IP address, but on the outside, the hostname must always resolve to 127.0.0.2.

Using a split DNS scenario with G/On has the added benefit of reducing attacks from the many worms, vira and backdoors roaming the internet, because all IP addresses of servers to access, will resolve to 127.0.0.2 on the external DNS, effectively causing an attacker his/her own loopback interface, instead of your server.


exhange.giritech.com is 192.168.1.12
Whois exhange.giritech.com
Split DNS
Whois exhange.giritech.com
exhange.giritech.com is 127.0.0.2
Attacker
Any scanning, or other attack happens on the "bad guys" own loopback interface
G/On Server
Firewall
Internet
G/On USB or Desktop client
3945/tcp encrypted traffic from 127.0.0.2
exchange.giritech.com
192.168.1.12

5.5. Man-in-the-Middle and Replay Attacks

The data sent through a G/On connection contains both a checksum and a SHA-1 hash. If these are not correct upon reception of data at either end, then the session will be terminated. This effectively prevents man-in-the-middle attacks.

Because G/On never uses the same set of ECC or AES keys twice, it becomes virtually impossible to perform replay attacks. A G/On client may respond to the first packet of a replay server's simulation of an initial packet, but the replay server will never be able to decrypt the response from the valid G/On Client. Equally, a replay client will never be able to answer a G/On Server, as it does not know what to include in the packet, and can therefore never satisfy the Rules and Zones engine of the G/On Server.

5.6. Virus, Spyware, Trojans, etc.

G/On is application based connectivity, not network based. This in itself makes it difficult for many forms of vira, spyware and Trojans to affect the corporate network. This does not mean the G/On is anti-viral, spyware proof, or safe from Trojans, backdoors and the like, but it does mean that G/On makes it very difficult for these types of parasites to spread into the corporate network.

With the right configuration of G/On and the applications connecting through G/On, it is possible to make it virtually impossible for parasites to infect the services provided from the corporate network. However, the client PC must still be protected by a firewall, anti-virus software and, in this day and age, even anti-spyware software.

For more information, please refer to the Giritech Basic Best Practice Reference available in the G/On Admin Guide, and also available as a separate document.

5.7. Phishing

If users are taught always to connect using G/On, and never follow links in e-mails regarding anything related to your business, banking, or other company activity, Phishing can be effectively be eliminated. Since the connectivity to applications flow through the loopback interface of the client PC, attempts to change out the URL will have no effect, as the clients connects at 127.0.0.2, and the full URL is only known at the G/On Server side.