

# Introduction – Project GRIPP

Prosectrim Trust, ©2006

As the price of computing technology is steadily decreasing, devices such as laptops and USB storage have become more commonly in use. Although these devices enhance business functionality, providing mobile access to information anytime and anywhere, they also pose a large threat to information security, mostly due to the sensitivity of data stored on these devices.

Many companies acknowledge the necessity of technology such as firewalls, intrusion detection, and advanced authentication systems, to secure their information. However, these technologies do not make them less vulnerable to a savvy social engineer or a dishonest employee. This may actually lead to a false sense of security, which might make them an even easier target.

This identifies the need for a platform to secure information against unauthorized distribution and/or scrutiny, even from persons authorized in the use of the protected data.

A project called GRIPP (Globally Regulated Information Protection Program) is currently in development to provide a solution to this lurking problem.

GRIPP provides protection by means of real-time encryption, but is vastly superior in the application thereof. While all data is encrypted, it is not decrypted by means of a password typed by a user. As a matter of fact, the user will never know the encryption password. Protected data is decrypted transparently as and when opened by specific applications, registered to use the data. As the application changes the data it will be re-encrypted on the fly and therefore will never be in a vulnerable state. The benefit of the system is that no person can take the information outside the protected environment, whether the internal corporate network, or even from a roaming users' laptop.

## **GRIPP Working**

Since the release of Microsofts' Windows NT, a strict set of rules were laid down and enforced, dictating the way applications interacts with hardware and resources. This gave the operating system better control resulting in a more stable system. The interface is called the API or Application Programming Interface.

This led the development of a technology, known as Supervised-processing. The idea is to monitor and influence the interaction between application and the resources, controlled by the operating system.

By using this technology to oversee the process of reading and writing data to permanent storage will take information security to a whole new level.

The following steps explain the inner workings of GRIPP: *(it is advised for non-technical users to skip to **Implementation Scenarios**)*

### STEP 1

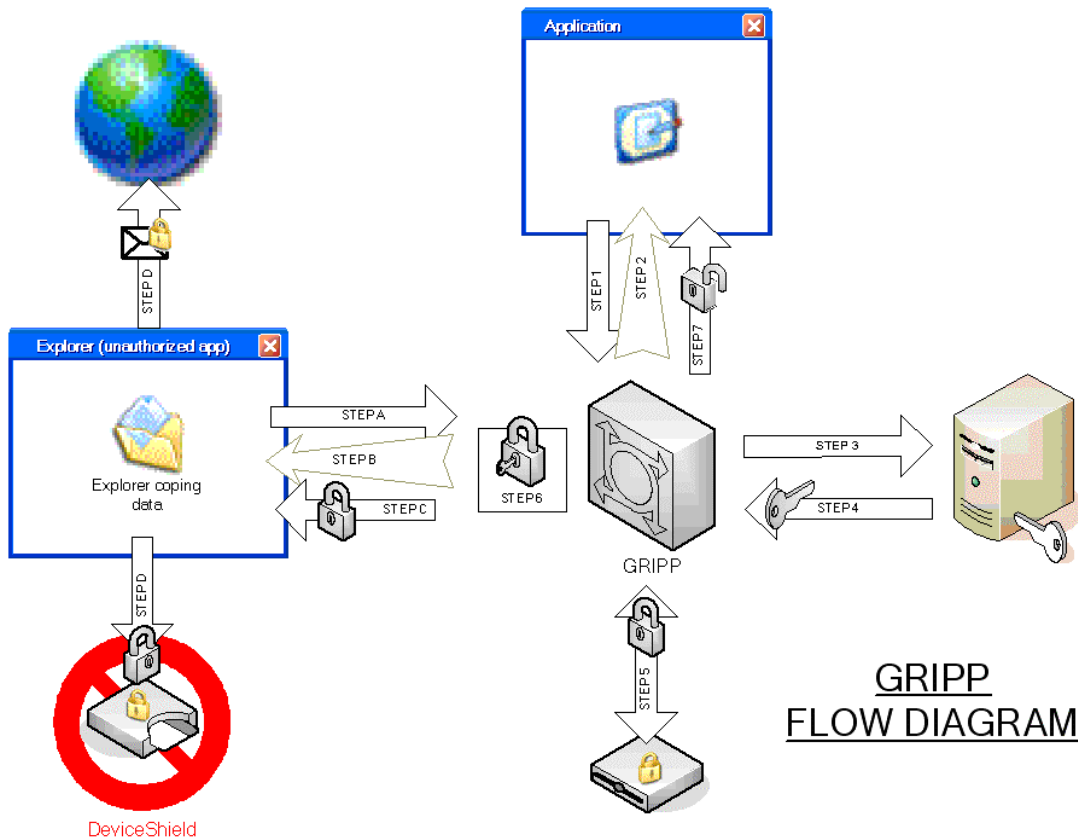
Application wants to open a file. GRIPP intercepts the request through the means of Supervised-processing.

### STEP 2

GRIPP runs a checksum to identify the application.

### STEP 3

The checksum together with computer identification is send to the Central Security Server requesting a decryption key.



### STEP 4

The Central Security Server verifies the request and if authorized, the decryption KEY is send back to the GRIPP module.

### STEP 5

GRIPP reads the requested data from disk into memory.

### STEP 6

GRIPP uses the KEY from the Security Server and decrypts the data.

### STEP 7

Decrypted data is passed to the application for processing.

When changes are made and data is saved it will be intercepted and re-encrypted before written to disk.

The following steps describe what happens when a user copies the data to a removable disk or wants to e-mail it outside the company:

**STEP A**

Explorer/Outlook wants to open the file in order to reproduce it onto removable media or email to data.

**STEP B**

GRIPP runs the checksum and request a KEY from the Central Security Server.

**STEP C**

Authentication fails (application is not authorized) and data is passed to Explorer/Outlook in encrypted format.

**STEP D**

Data written onto the removable disk or e-mailed stays encrypted and therefore useless to others.

## **Implementation Scenarios**

In order for one to better understand where GRIPP fits into the market, a diagram with a number of scenarios were set up. By describing the details of each scenario - user, risk, solution, shortcoming and GRIPPs' answer - will be highlighted.

### **Real-life Scenarios**

*(Please refer to Diagram 1)*

**Scenario i:**

*User A:* Software programmer – need access to the source code, e-mail, web, USB storage in order to perform his duties.

*Risk:* User has access to all source code within the company. User brings smart-phone with Bluetooth connectivity to the office and copy source code to use at home for private jobs.

*Solution:* Load device limiting software like DeviceWall or DeviceShield onto users PC.

*Shortcomings:* User decides to e-mail the source code to his external e-mail address and access it from his home PC.

*GRIPP:* Because the source code would be encrypted, e-mailing the data to a private mail account will not allow the user to utilize the data for private use. At the office, the GRIPP module will decrypt the data transparently when opened by Visual Basic / Delphi, resulting in the use of the source code to perform the task of programming.

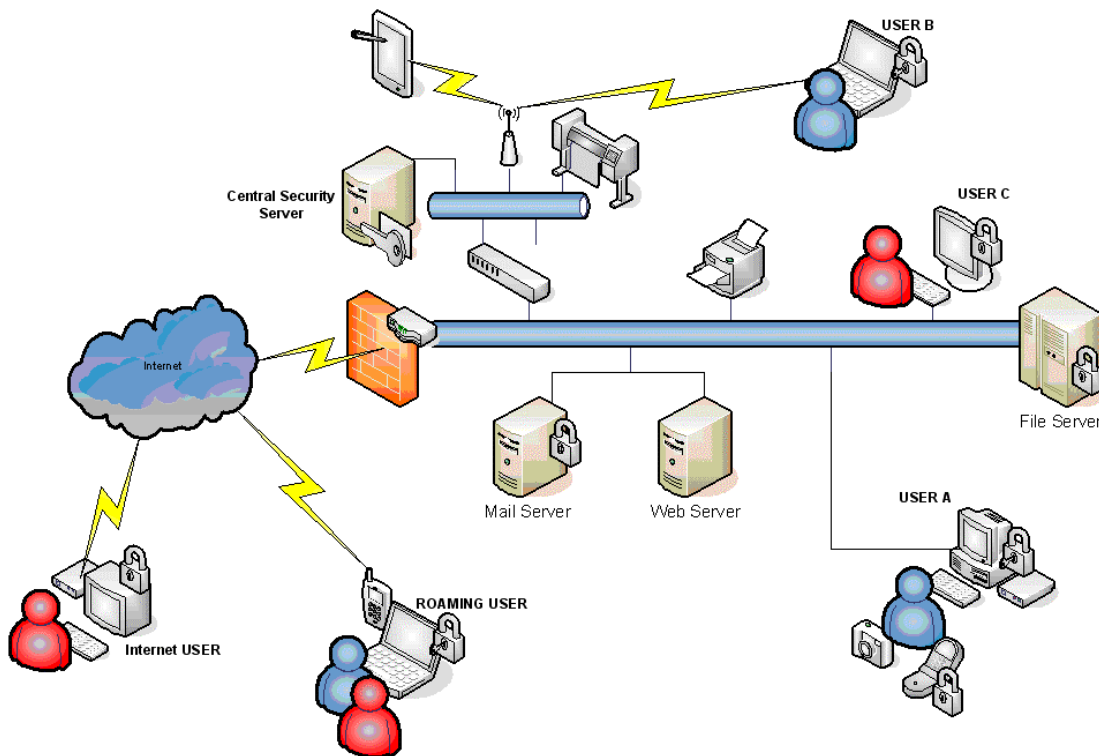


Diagram 1

**Scenario ii:**

*User B:* Manager – Use a notebook and have access to all data in the company. Also have e-mail and access to the Internet.

*Risk:* User takes notebook home and out of a controlled environment. This opens up the risk of theft as well as industrial espionage.

*Solution:* Load drive encryption software like DriveCrypt on the users computer. This will request a password on each start-up and protect data.

*Shortcomings:* Encrypting the data will protect against notebook theft. The problem is that the users usually pick easily to remember (and easy to crack) passwords.

*GRIPP:* With data encrypted by GRIPP there wouldn't be any user password requests; this eliminates the "weak password" syndrome.

**Scenario iii:**

*Roaming User:* Systems administrator – Takes his notebook home and need access to data offline. Occasionally access the companies' network through the Internet. User is highly technical.

*Risk:* The user gets motivated by money. In order for the user to perform his duties, access to the entire network is granted. When "head-hunted", this user comes with the competitions' corporate database.

*Solution:* Standard encryption software is useless in this case. Device limiting software like DeviceLock will provide some protection by stopping the user from just copying data to any removable storage.

*Shortcomings:* It takes only 5 “easy” steps for the user to get hold of the corporate database; (i) at the office - “detached” the database from SQL server and copy it to a notebook, (ii) re-attach the database as soon as a copy is made to avoid suspicion, (iii) at home – remove the hard disk from the notebook and install into home PC (this circumvents the DeviceLock software), (iv) copy data onto another hard disk drive, (v) “attached” the database onto another SQL server.

*GRIPP:* With the SQL server database encrypted and by using GRIPP for decryption at runtime, it doesn’t stop the theft of the database, but render it useless to any other.

***Scenario iv:***

*User C:* Admin – do managements’ typing and therefore accesses the CEOs’ hard drive through a shared folder.

*Risk:* Although the user has no access to important data, a network share provides access to information stored on the CEOs’ computer. A competitor hires the services of a social engineer in an attempt to get hold of important data files.

*Solution:* Applying data encryption together with removable device protection software will protect the data on the CEOs’ computer.

*Shortcomings:* The user is targeted by a social engineer and encouraged to open e-mail with an embedded Trojan. The anti-virus doesn’t detect the “home-made” Trojan and it is allowed to execute on the users computer. The Trojan uses the network share and waits for the data to be decrypted for use by the CEO and then copy data in order to upload it to the Internet.

*GRIPP:* With access granted to the CEOs’ computer to read the imported data, the data’s location is not important. Protected data files may be in the same directory as documents that needs to be accessed by admin. In this case the Trojan would have uploaded encrypted and therefore useless files.

***Scenario v:***

*Internet User:* Unknown – Trying to get into the network from the Internet.

*Risk:* The user wants to penetrate the network and deforms the website. This will reflect very poorly on the companies’ image.

*Solution:* Installing a firewall on the gateway router will protect against intrusion.

*Shortcomings:* The firewall must allow incoming connections to the web server. By exploiting vulnerabilities within the web server software, the Internet user manages to replace the default web page with offensive content.

*GRIPP:* By encrypting all the HTML documents and giving authorization to only IIS (the web server software) for decryption, the web server will not be able to serve the unencrypted offensive content.