

Technical field

The present invention regards a method for analyzing if data generated by an application has been tampered with before it is displayed to the user by securing that a dataset produced by an application and sent to the screen of an end users device actually is displayed and presented on screen.

Background of the invention

Tampering is the deliberate altering or adulteration of information, and today there is no single solution that can be considered as tamper proof.

Often several levels of security are needed to be addressed to reduce the risk of tampering. Usually the following considerations are taken in order to prevent tampering: Identify who a potential tampering attacker might be and what level of knowledge they might they have.

Identify all feasible methods of unauthorized access into a system. In addition to the primary means of entry, also consider back door methods.

Control or limit access to systems of interest.

Improve the tamper resistance by making tampering more difficult, time-consuming, etc.

Add tamper-evident features to help indicate the existence of tampering.

Educate people to watch for evidence of tampering.

A problem regarding tampering with displayed data is that it is usually hard to detect and check if data has been tampered with or not.

Summary of the invention

It is therefore an object of the invention, as it is stated in the set of claims, to solve the problems stated above. This is done by the application by adding randomly positioning pixels into the screen of the device in question, the application executes display operations and presents the display data to the end user, the application takes screen shots of what actually is displayed and compares the number and position of the pixels with that generated by the application.

If the comparison results in matched pixels in number, color and position the application has verified that data processes for display actually was displayed to the end user without any changes. But, if the comparison results in non-matching the application can, depending on the unmatched number and /or color that the display operation has been tampered with.

Detailed description

The application generates the data to be display on the screen of a device.

The application generates randomized addresses for positioning pixels on the screen of the device in question.

- 5 The application analyses the addressing and inserts the pixels in the blue channel (RGB) into the data that is going to be displayed in order to make the pixels as invisible for humans as possible.

The application executes display operations and presents the data to the end user.

The application takes screen shot of what actually is displayed to the end user

- 10 The application analyses the screen shot in order to detect the inserted pixels and compares the number and position of the pixels with the pixels that the application generated and processed for display to the end user.

If the comparison results in matched pixels in number, color and position the application has verified that data processes for display actually was displayed to the end user

- 15 without any changes. But, if the comparison results in non-matching the application can, depending on the unmatched number and /or color that the display operation has been tampered with.

An example of a scenario is a hacker interfering with a bank transaction between a user and a bank. When a user tries to pay a bill using net banking, the hacker intercepts the transaction and changes the amount to be paid and the account number it is to be paid to. The bank sees the information the hacker has entered and thinks it is from the user. The user only sees the information originally entered and approves the falsified transaction of the money.

- 25 With the present invention, a screenshot is taken of what is actually displayed at the other side. By checking if a set of marker pixels inserted into the picture at the user side corresponds with a set of marker pixels in the screen shot of what is displayed at the banking side it is possible to detect if the information in the picture has been tampered with, and hence stop the transaction.