(12) **PATENT**

(19) NO (11) **339312** (13) **B1**

NORWAY (51) Int Cl.
G06F 3/00 (2006.01)
G06F 3/048 (2013.01)
G06F 3/06 (2006.01)
G06F 3/14 (2006.01)
G06F 21/36 (2013.01)

Norwegian Industrial Property Office

(21)	Application nr.	20150255	(86)	International Filing Date and Application Number
(22)	Date of Filing	2015.02.24	(85)	Date of Entry into National Phase
(24)	Date of Effect	2015.02.24	(30)	Priority
(41)	Publicly Available	2016.08.25		
(45)	Granted	2016.11.21		

(73)	Applicant	PROTECTORIA AS, Klingenberggata 7 B, 0161 OSLO, Norge
(72)	Inventor	Trond Lemberg, Skotbuveien 81, 1409 SKOTBU, Norge
(74)	Agent or Attorney	Oslo Patentkontor AS, Postboks 7007 Majorstua, 0306 OSLO, Norge

(54) Title **Secure data for display**

(56) References Cited:

Display security for online transactions: SMS-based authentication scheme.Internet Technology and Secured Transactions (ICITST), 2010 International Conference for, 20101108IEEE, Piscataway, NJ, USA
US 2014201527 A1
GB 2512140

(57) Abstract

A method for analyzing if data generated by an application has been trampered with, comprising an application and a device with a screen and a channel of communication, wherein said application generates data to be displayed on the screen of a device, pixels is insered into the data that is going to be displayed, said application generates randomzied addresses for positioning pixels on the screenof the device in question, the display operations are excuted and data presented to the end user, ascrren shot of that is displayed is taken, and said screen short is analyzed, and the number and position of the pixels compares with the pixels that the application generated and processed for display to the end user.

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.

From Alzomai, M. et al: "Display security for online transactions: SMS-based authentication scheme", 2010 International Conference for Internet Technology and Secured Transactions (ICITST), 20101108 IEEE, Piscataway, NJ, USA there is known a method for secure online transactions. Among other, the method includes to verify and authenticate transactions by comparing image information, the images being captured from a display screen.

US 2014/201527 describes a system and method for secure delivery of information between a sender and receiver via a network. The method includes entering additional information preventing displayed information from being retransmitted or copied.

GB 2512140 describes a system and method for handling the display of messages. The system includes an image memory for storing images and metadata associated

with the images, the metadata including a time stamp showing when the image was captured, and a device taking a screen shot of an image displayed on a screen, wherein the screen shot and the time stamp is stored in the image memory, and a device for comparing image data taken from the screen shot.

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.

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

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 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.

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.

Claims

1. A method for analyzing if display data generated by an application has been tampered with, comprising an application and a device with a screen and a channel of communication, c h a r a c t e r i z e d i n t h a t :
   - said application generates data to be displayed on the screen of a device,
   - said application generates randomized addresses for positioning pixels on the screen of the device in question,
   - pixels is according to the pixel addressing information inserted into the data that is going to be displayed,
   - the display operations are executed and the data presented to the end user,
   - a screen shot of what is displayed is taken, and
   - said screen shot is analyzed by the application, and the number and position of the pixels are compared with the pixels that the application generated and processed for display to the end user.

2. A method according to claim 1, wherein the inserted pixels is in the blue channel in the RGB color model.

P a t e n t k r a v

1. Fremgangsmåte for å analysere om fremvisningsdata generert av en applikasjon har blitt tuklet med, omfattende en applikasjon og en innretning med en skjerm og en kommunikasjonskanal,

   k a r a k t e r i s e r t v e d a t :

   - nevnte applikasjon genererer data for fremvisning på skjermen til en innretning,
   - nevnte applikasjon genererer tilfeldige adresser for posisjonering av piksler på skjermen til den aktuelle innretningen,
   - piksler settes inn i dataene som skal fremvises ifølge pikseladresseinformasjonen,
   - fremvisningsoperasjonene utføres og dataene presenteres for sluttbrukeren,
   - det tas en skjermdump av det som fremvises, og
   - nevnte skjermdump analyseres av applikasjonen, og antallet og posisjonen av pikslene sammenlignes med piksler generert av applikasjonen for fremvisning for sluttbrukeren.

2. Fremgangsmåte ifølge krav 1, hvor de innsatte piksler er i den blå kanalen i RGB fargemodellen.